デベロッパーガイド

Amazon Route 53



API バージョン 2013-04-01

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon Route 53: デベロッパーガイド

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon の商標およびトレードドレスは、Amazon のものではない製品またはサービスにも関連して、お客様に混乱を招いたり Amazon の信用を傷つけたり失わせたりするいかなる形においても使用することはできません。Amazon が所有しない商標はすべてそれぞれの所有者に所属します。所有者は必ずしも Amazon と提携していたり、関連しているわけではありません。また、Amazon 後援を受けているとはかぎりません。

Table of Contents

Amazon Route 53 とは？ 1
ドメイン登録の仕組み 3
ウェブサイトやウェブアプリケーションへのインターネットトラフィックのルーティング 4
ドメインのインターネットトラフィックをルーティングするように Amazon Route 53 を設定する方法の概要 5
Amazon Route 53 によりドメインのトラフィックをルーティングする方法 6
Amazon Route 53 がリソースの正常性をチェックする方法 8
Amazon Route 53 の概念 10
ドメイン登録の概念 11
ドメインネームシステム (DNS) の概念 12
コントロールプレーンとデータプレーンの概念 17
ヘルスチェックの概念 18
Amazon Route 53 の開始方法 19
Amazon Route 53 へのアクセス 20
AWS Identity and Access Management 20
Amazon Route 53 の料金と請求 21
AWS SDKs の使用 21
開始方法 23
セットアップする 23
にサインアップする AWS アカウント 24
ツールをダウンロード 24
DNS トラフィックを Amazon S3 静的ウェブサイトにルーティングする 25
前提条件 25
ステップ 1: ドメインの DNS トラフィックをウェブサイトバケットにルーティングする 26
ステップ 2: ウェブサイトをテストする 28
CloudFront ディストリビューションに DNS トラフィックをルーティングする 29
前提条件 29
ステップ 1: ドメインの DNS トラフィックを CloudFront ディストリビューションにルーティングする 30
の他のサービスとの統合 33
ログ記録、モニタリング、タグ付け 33
他の AWS リソースへのトラフィックのルーティング 34
DNS ドメイン名の形式 37
ドメイン名登録用のドメイン名の形式 37

ホストゾーンとレコード用のドメイン名の形式 37
ホストゾーンおよびレコード名のアスタリスク (*) を使用する 38
国際化ドメイン名の形式 39
ドメインの登録と管理 42
新しいドメインの登録 43
新しいドメインの登録 43
ドメインを登録または移管するときに指定する値 51
ドメインの登録時に Amazon Route 53 が返す値 57
ドメイン登録のステータスの表示 58
ドメインの設定の更新 59
ドメインの連絡先情報と所有者の更新 60
ドメインの連絡先情報のプライバシー保護の有効化/無効化 69
ドメインの自動更新の有効化/無効化 73
別のレジストラへの許可のない移管を防ぐためのドメインのロック 74
ドメインの登録期間の延長 75
ネームサーバーを更新して別のレジストラを使用する 77
ドメインのネームサーバーおよびグルーレコードの追加あるいは変更 77
ドメインの登録の更新 82
失効した、または削除されたドメインの復元 85
ドメインのホストゾーンの置き換え 87
ドメインの移管 88
移管タイプを選択する 89
移管前チェックリスト 91
Route 53 への移管 94
一般的な移管の問題 113
Route 53 からの移管 116
別の AWS アカウントへの移管 122
移管ステータス 126
ドメインの有効期限日に対する移管の影響 128
承認および確認メールの再送信 130
E メールアドレスの更新 131
E メールの再送信 131
ドメインの DNSSEC の設定 136
DNSSEC がドメインを保護する方法の概要 137
ドメインに DNSSEC を設定する際の前提条件と最大数 139
ドメインへのパブリックキーの追加 139

ドメインのパブリックキーの削除 141
レジストラの検索 142
ドメインに関する情報の表示 142
ドメイン名登録の削除 144
ドメイン登録の問題に関する AWS サポートへのお問い合わせ 147
AWS アカウントにサインインできる AWS 場合のサポートへのお問い合わせ 148
AWS アカウントにサインインできない場合の AWS サポートへのお問い合わせ 149
ドメイン請求レポートのダウンロード 149
Amazon Route 53 に登録できる最上位ドメイン 150
サポートされている最上位ドメインのインデックス 152
汎用最上位ドメイン 155
地理的最上位ドメイン 465
DNS サービスとしての Amazon Route 53 の設定 530
Route 53 を既存ドメインの DNS サービスにする 531
Route 53 を使用中のドメインの DNS サービスにする 531
Route 53 を非アクティブドメインの DNS サービスにする 540
新しいドメインの DNS ルーティングの設定 545
Route 53 から購入したドメインの DNS を設定する 545
別のレジストラから購入したドメインの DNS を設定する 545
リソースへのトラフィックのルーティング 547
サブドメインのトラフィックのルーティング 547
ホストゾーンの使用 554
「パブリックホストゾーンの操作」 555
プライベートホストゾーンの使用 585
ホストゾーンを別の AWS アカウントに移行する 599
レコードを使用する 610
ルーティングポリシーの選択 611
エイリアスレコードと非エイリアスレコードの選択 637
サポートされる DNS レコードタイプ 642
Amazon Route 53 コンソールを使用したレコードの作成 663
リソースレコードセットのアクセス許可 665
指定値 666
ゾーンファイルをインポートしてレコードを作成する 757
レコードの編集 761
レコードの削除 762
レコードの一覧表示 763

DNSSEC 署名の設定 765
DNSSEC 署名を有効にし、信頼チェーンを確立します。 767
DNSSEC 署名の無効化 777
カスタマー管理キーの使用 782
キー署名キー (KSK) の使用 783
Route 53 での KMS キーと ZSK 管理 786
Route 53 での DNSSEC の非存在証明 787
DNSSEC 署名のトラブルシューティング 788
AWS Cloud Map を使用してレコードとヘルスチェックを作成する 789
DNS の制約と動作 790
最大レスポンスサイズ 790
Authority セクションの処理 790
Additional セクションの処理 790
関連トピック 790
トラフィックフロー 791
トラフィックフローの利点 791
トラフィックポリシーの作成と管理 793
トラフィックポリシーの作成 793
トラフィックポリシーを作成するときに指定する値 796
地理的近接性の設定の効果を示す地図の表示 806
トラフィックポリシーの追加のバージョンの作成 810
JSON ドキュメントを使用してトラフィックポリシーを作成する 813
トラフィックポリシーバージョンおよび関連するポリシーレコードの表示 816
トラフィックポリシーバージョンとトラフィックポリシーの削除 820
ポリシーレコードの作成および管理 822
ポリシーレコードの作成 824
ポリシーレコードを作成または更新する場合に指定する値 826
ポリシーレコードの更新 827
ポリシーレコードの削除 829
トラフィックポリシードキュメントの形式 830
基本構文 831
エンドポイント定義の構文 832
ルール定義の構文 835
例 846
VPC Resolver とは 855
VPC とネットワークの間における DNS クエリの解決 857

ネットワークからの DNS クエリを VPC Resolver に転送する方法 861
Resolver エンドポイントが VPCs からネットワークに DNS クエリを転送する方法 864
インバウンドエンドポイントとアウトバウンドエンドポイントを作成する際の考慮事項 871
Route 53 VPC Resolver の可用性とスケーリング 875
Route 53 VPC Resolver の開始方法 877
VPC へのインバウンド DNS クエリの転送 879
インバウンド転送の設定 879
インバウンドエンドポイントを作成または編集するときに指定する値 880
インバウンドエンドポイントの管理 884
ネットワークへのアウトバウンド DNS クエリの転送 887
アウトバウンド転送の設定 888
アウトバウンドエンドポイントを作成または編集するときに指定する値 889
ルールを作成または編集するときに指定する値 893
アウトバウンドエンドポイントの管理 895
転送ルールの管理 898
リゾルバーの委任ルールのチュートリアル 906
アウトバウンド委任のステップ 906
委任タイプ 907
DNSSEC 検証の有効化 912
AWS リソースへのインターネットトラフィックのルーティング 914
Amazon API Gateway API 914
前提条件 915
トラフィックを API Gateway エンドポイントにルーティングするための Route 53 の設定 916
Amazon CloudFront ディストリビューション 919
前提条件 921
Amazon Route 53 を設定して、CloudFront ディストリビューションにトラフィックをルーティング 922
Amazon EC2 インスタンス 924
前提条件 925
トラフィックを Amazon EC2 インスタンスにルーティングする Amazon Route 53 の設定 925
App Runner サービス 927
前提条件 928
Amazon Route 53 での App Runner サービスに対するトラフィックのルーティングの設定 928

Global Accelerator ... 930
前提条件 ... 930
トラフィックがアクセラレーターにルーティングされるように Amazon Route 53 を設定 .. 931
AWS Elastic Beanstalk 環境 ... 932
Elastic Beanstalk 環境へのアプリケーションのデプロイ ... 932
Elastic Beanstalk 環境のドメイン名の取得 ... 933
Route 53 レコードの作成 ... 933
ELB ロードバランサー ... 936
前提条件 ... 937
トラフィックが ELB ロードバランサーにルーティングされるように Amazon Route 53 を設定 ... 938
Amazon S3 バケット ... 940
前提条件 ... 940
トラフィックが S3 バケットにルーティングされるように Amazon Route 53 を設定 ... 941
Amazon Virtual Private Cloud インターフェイスエンドポイント ... 943
前提条件 ... 944
Amazon VPC インターフェイスのエンドポイント ... 944
Amazon WorkMail ... 946
Amazon OpenSearch Service ... 949
前提条件 ... 949
Amazon Route 53 を Amazon OpenSearch Service ドメインエンドポイントにルーティングする Amazon Route 53 の設定 ... 949
VPC Lattice ... 951
前提条件 ... 951
VPC Lattice サービスドメインエンドポイントにトラフィックをルーティングするように Amazon Route 53 を設定する ... 951
その他の AWS リソース ... 953
ヘルスチェックの作成 ... 954
ヘルスチェックの種類 ... 955
Route 53 でヘルスチェックの正常性を判断する方法 ... 956
Route 53 がエンドポイントをモニタリングするヘルスチェックのステータスを決定する方法 ... 956
Route 53 が他のヘルスチェックをモニタリングするヘルスチェックのステータスを決定する方法 ... 958
Route 53 が CloudWatch アラームをモニタリングするヘルスチェックのステータスを決定する方法 ... 959

ヘルスチェックの作成、更新、削除 960
ヘルスチェックの作成と更新 961
ヘルスチェックを作成または更新するときに指定する値 963
ヘルスチェックを作成すると Route 53 が表示する値 989
CloudWatch アラーム設定を変更する場合のヘルスチェックの更新 989
ヘルスチェックの無効化または有効化 991
ヘルスチェックの反転 992
ヘルスチェックの削除 992
DNS フェイルオーバーが設定されている場合のヘルスチェックの更新または削除 994
のヘルスチェックができるようにルーターとファイアウォールのルールを設定する 995
DNS フェイルオーバーの設定 996
DNS フェイルオーバーを設定するためのタスクリスト 997
の単純構成におけるヘルスチェックの動作 999
複雑な構成におけるヘルスチェックの動作 1003
ヘルスチェックが設定されている場合に Route 53 がレコードを選択する方法 1011
フェイルオーバー (アクティブ/アクティブとアクティブ/パッシブ) の設定 1014
プライベートホストゾーンのフェイルオーバーの設定 1017
Route 53 でフェイルオーバーの問題を回避する方法 1018
ヘルスチェックの名前付けとタグ付け 1019
タグの制限 1020
ヘルスチェックに対するタグの追加、編集、削除 1020
API バージョン 2012-12-12 未満の使用 1023
ヘルスチェックのステータス監視と通知の受信 1025
ヘルスチェックのステータスと失敗理由を表示する 1025
ヘルスチェッカーとエンドポイント間のレイテンシーのモニタリング 1027
CloudWatch を使用したヘルスチェックのモニタリング 1032
ヘルスチェックのステータスを表示する 1032
ヘルスチェックアラームを表示する 1035
CloudWatch コンソールでヘルスチェックメトリクスを表示する 1038
SNS 通知を使用してアラームを作成する 1038
リゾルバー DNS ファイアウォール 1043
Resolver DNS Firewall の仕組み 1044
DNS Firewall のコンポーネントと設定 1044
Resolver DNS Firewall が DNS クエリをフィルタリングする方法 1048
DNS Firewall を使用するための手順の概要 1049
複数のリージョンで DNS Firewall ルールグループを使用する 1050

DNS Firewall のリージョンの可用性 1050
Resolver DNS Firewall の開始方法 1051
Resolver DNS Firewall ウォールドガーデンの例 1052
Resolver DNS Firewall ブロックリストの例 1054
DNS Firewall のルールグループとルール 1056
DNS Firewall のルールグループ設定 1057
DNS Firewall のルール設定 1057
DNS Firewall でのルールアクション 1060
DNS Firewall でのルールグループおよびルールの管理 1061
DNS ファイアウォールの基本ルール 1065
マネージドドメインリスト 1065
独自のドメインリストの管理 1071
DNS ファイアウォールの詳細ルール 1073
高度な DNS 保護 1074
高度なマネージドドメインリスト 1075
Palo Alto Networks によるパートナーマネージド DNS 脅威保護 1078
DNS Firewall でクエリログ記録を設定する 1085
アカウント間での ルールグループの共有 1088
VPC 向けの DNS Firewall による保護の有効化 1090
VPC とファイアウォールのルールグループ間の関連付けの管理 1091
DNS Firewall での VPC の設定 1092
Amazon Route 53 プロファイルとは 1094
プロファイルの優先順位付け 1095
プロファイルの可用性 1095
プロファイルの使用 1095
プロファイルを作成する 1096
DNS ファイアウォールルールグループを関連付ける 1098
プライベートホストゾーンを関連付ける 1100
リゾルバールールを関連付ける 1100
VPC エンドポイントを関連付ける 1101
クエリログ記録設定を関連付ける 1102
プロファイル設定を編集する 1103
VPC を関連付ける 1105
プロファイルの表示と更新 1106
プロファイルの削除 1108
プロファイルに関連付けられたリソースの表示と更新 1109

リソースの関連付け解除 1112
プロファイルに関連付けられた VPC の表示 1112
VPC の関連付け解除 1114
共有 Route 53 プロファイルの使用 1116
Route 53 プロファイルを共有するためのアクセス許可の付与 1117
Route 53 プロファイルを共有するための前提条件 1117
Route 53 プロファイルの共有 1117
共有 Route 53 プロファイルの共有解除 1118
共有 Route 53 プロファイルの特定 1119
共有 Route 53 プロファイルの責任とアクセス許可 1120
請求と使用量測定 1120
インスタンスクォータ 1120
Amazon Route 53 on Outposts とは 1121
アーキテクチャの概要 1121
Route 53 on Outposts の機能 1122
AWS Outposts が VPC から切断された場合の VPC リゾルバーの動作 1123
での VPC Resolver の開始方法 AWS Outposts 1123
第 2 世代 AWS Outposts 1123
第 1 世代 AWS Outposts 1123
インバウンドエンドポイントの作成 (第 1 世代 AWS Outposts のみ) 1125
Outpost のインバウンドエンドポイントを作成または編集するときに指定する値 1125
アウトバウンドエンドポイントの作成 (第 1 世代 AWS Outposts のみ) 1127
でアウトバウンドエンドポイントを作成または編集するときに指定する値 AWS Outposts 1128
アウトバウンドエンドポイントの転送ルールの作成 1130
Resolver on Outpost の管理 1130
Outpost でのリゾルバーの編集 (第 1 世代 AWS Outposts のみ) 1131
Resolver on Outpost ステータスの表示 1131
Outpost でのリゾルバーの削除 (第 1 世代 AWS Outposts のみ) 1132
Resolver on Outpost でのインバウンドエンドポイントの管理 (第 1 世代 AWS Outposts のみ) 1133
インバウンドエンドポイントの表示と編集 1133
インバウンドエンドポイントのステータスの表示 1134
インバウンドエンドポイントの削除 1135
Resolver on Outpost でのアウトバウンドエンドポイントの管理 (第 1 世代 AWS Outposts のみ) 1136
アウトバウンドエンドポイントの表示と編集 1137

アウトバウンドエンドポイントのステータスの表示 1137
アウトバウンドエンドポイントの削除 1139
Route 53 Global Resolver とは 1140
Route 53 Global Resolver を使用する理由 1141
概念と用語 1141
オンプレミスおよびリモートロケーションのクライアント用の DNS リゾルバー 1142
DNS クライアント認証 1142
トラフィック分割 DNS 解決 1143
高可用性とグローバルプレゼンス 1144
DNS 解決と転送 1144
DNS フィルタリングとドメインリスト 1145
高度な DNS 脅威検出 1146
モニタリングとログ記録 1147
仕組み 1147
クライアントが DNS クエリを実行するとどうなるか 1148
グローバルエニーキャストアーキテクチャ 1148
DNS フィルタリングとセキュリティ 1149
ユースケース 1149
関連サービス 1151
グローバルリゾルバーへのアクセス 1152
サポートされている AWS リージョン 1152
オプトインリージョンに関する考慮事項 1153
アカウントアクセスの設定 1155
ポリシーとロールの作成 1155
ネットワークに関する考慮事項 1156
チュートリアル: 最初の Route 53 Global Resolver を作成する 1157
前提条件 1157
ステップ 1: グローバルリゾルバーを作成する 1157
ステップ 2: DNS ビューを作成して認証を設定する 1158
ステップ 3: DNS フィルタリングルールを設定する (オプション) 1158
ステップ 4: 設定をテストする 1159
ステップ 5: DNS アクティビティのモニタリング 1159
ステップ 6: クリーンアップする (オプション) 1159
次の手順 1160
DNS ビューの管理 1161
DNS ビューの管理 1161

プライベートホストゾーンの関連付けの管理 1163
DNS ビューの設定を構成する 1163
アクセスコントロールの管理 1166
アクセスコントロール方法 1166
アクセスソースの設定 1167
アクセストークンの管理 1168
ベストプラクティス 1172
DNS の保護 1173
DNS Firewall ルールの設定と管理 1173
マネージドドメインリスト 1177
ビルドドメインリスト 1181
DNS Firewall Advanced 保護 1182
セキュリティポリシーの管理 1183
プライベートホスト関連付けの設定 1184
プライベートホストゾーンの関連付けを管理する 1185
アカウント間の DNS ビューの共有 1186
DNS ビューの共有 1188
共有 DNS ビューの使用 1189
DNS アクティビティのモニタリング 1190
DNS の可視性を取得する 1191
DNS モニタリングの設定 1196
CloudWatch によるモニタリング 1197
DNS 問題のトラブルシューティング 1205
接続の問題の診断 1206
パフォーマンスの問題を解決する 1208
設定のトラブルシューティング 1209
内部リソースアクセスのトラブルシューティング 1211
クォータ 1211
ソフトクォータ 1212
AWS CloudFormation リソースの作成 1214
Route 53、VPC Resolver、および CloudFormation テンプレート 1214
Route 53 と のベストプラクティス CloudFormation 1215
結果整合性について理解する 1215
DNS レコードの順序付けと論理 ID 1216
ロールバック失敗の処理 1217
の詳細 CloudFormation 1217

コードの例 1218
Route 53 1219
基本 1219
Route 53 ドメイン登録 1248
基本 1249
セキュリティ 1333
データ保護 1334
ダングリング委任レコードからの保護 1335
Identity and access management 1337
アイデンティティを使用した認証 1338
アクセスコントロール 1339
サービスリンクロールの使用 1359
AWS 管理ポリシー 1364
条件の使用 1379
Route 53 API のアクセス許可リファレンス 1397
ログ記録とモニタリング 1398
コンプライアンス検証 1399
耐障害性 1400
インフラストラクチャセキュリティ 1401
の検出結果を Security Hub CSPM に送信する 1402
Security Hub CSPM での検出結果の仕組み 1402
DNS Firewall が送信する検出結果のタイプ 1403
Security Hub CSPM が使用できない場合の再試行 1403
Security Hub CSPM の既存の検出結果を更新する 1403
DNS Firewall からの一般的な検出結果 1404
統合の有効化と構成 1406
Security Hub CSPM への検出結果の配信の停止 1406
モニタリング 1407
パブリック DNS クエリのログ記録 1407
DNS クエリのログ記録の設定 1408
Amazon CloudWatch を使用して DNS クエリログにアクセスする 1410
ログの保持期間の変更と Amazon S3 へのログのエクスポート 1411
クエリログ記録の停止 1411
DNS クエリログに表示される値 1412
クエリログの例 1413
リゾルバーでのクエリのログ記録 1413

Resolver のクエリログの送信先となるリソース 1415
設定の管理 1417
ドメイン登録のモニタリング 1426
Amazon Route 53 のヘルスチェックと Amazon CloudWatch を使用したリソースのモニタリング 1426
ヘルスチェックのメトリクスとディメンション 1427
Amazon CloudWatch を使用したホストゾーンのモニタリング 1429
Route 53 パブリックホストゾーンの CloudWatch メトリクス 1430
Route 53 パブリックホストゾーンメトリクスの CloudWatch ディメンション 1431
Amazon CloudWatch による Route 53 VPC Resolver エンドポイントのモニタリング 1431
VPC Resolver のメトリクスとディメンション 1432
Amazon CloudWatch を使用した Resolver DNS Firewall ルールグループのモニタリング 1440
DNS Firewall のメトリクスとディメンション 1440
DNS Firewall データでの Amazon CloudWatch Contributor Insights の使用 1443
Amazon CloudWatch Logs Insights を使用した DNS Firewall ログの分析 1444
を使用した DNS Firewall イベントの管理 EventBridge 1444
リゾルバー DNS ファイアウォールイベント 1445
DNS ファイアウォールイベントの送信 1446
アクセス許可 1449
その他のリソース 1449
イベント DNS ファイアウォールの詳細リファレンス 1449
を使用した Amazon Route 53 API コールのログ記録 AWS CloudTrail 1457
CloudTrail での Route 53 の情報 1457
イベント履歴での Route 53 イベントの表示 1458
Route 53 のログファイルエントリを理解する 1459
トラブルシューティング 1467
マイドメインはインターネットで使用できません 1468
新しいドメインを登録しましたが、確認メールのリンクが選択されていません 1468
Amazon Route 53 にドメイン登録を移管したが、DNS サービスを移管しなかった 1469
ドメイン登録を移管し、ドメイン設定で誤ったネームサーバーを指定した 1470
DNS サービスをまず移管したが、ドメイン登録を移管する前に十分に時間を置かなかった 1472
Route 53 がドメインのインターネットトラフィックをルーティングするために使用しているホストゾーンを削除した 1472
ドメインは停止しています 1473
マイドメインは停止しています (ステータスは ClientHold です) 1473

新しいドメインを登録しましたが、確認メールのリンクが選択されていません 1474
ドメインの自動更新を無効にしていてドメインの有効期限が切れた 1475
登録者の連絡先の E メールアドレスを変更しましたが、新しい E メールアドレスが有効であることを確認しませんでした 1475
AWS 適正使用ポリシーの違反によりドメインが停止されました 1476
裁判所命令によってドメインを停止しました 1476
マイドメインオペレーションの失敗 1476
連絡先情報が無効であるため、ドメインオペレーションが失敗しました 1476
マイドメインを Amazon Route 53 に移管できませんでした 1477
認可 E メールのリンクが選択されていません 1477
現在のレジストラから取得した認可コードが無効である 1477
.es ドメインを Amazon Route 53 に移管する際に「Parameters in request are not valid」エラーを受信する 1478
Amazon Route 53 に移管する国際化ドメイン名の、Punycode で記述されたリストはありますか? 1478
一般的な移管エラーメッセージ 1478
DNS 設定を変更したが、変更が適用されていない 1481
過去 48 時間以内に DNS サービスを Amazon Route 53 に移管したため、DNS はまだ前の DNS サービスを使用している 1481
DNS サービスを Amazon Route 53 に移管したが、ドメインレジストラでネームサーバーを更新しなかった 1482
DNS リゾルバーがまだレコードの古い設定を使用している 1483
同じ名前のホストゾーンが複数あり、ドメインに関連付けられていないホストゾーンを更新しました 1484
ブラウザに「Server not found」エラーが表示されます 1486
ドメインまたはサブドメインの名前にレコードを作成しなかった 1486
レコードを作成したが、誤った値を指定した 1486
トラフィックをルーティングしているリソースが使用できない 1486
ウェブサイトホスティングのために設定された Amazon S3 バケットにトラフィックをルーティングすることができません 1487
同じホストゾーンで 2 回請求がありました 1487
ドメインに対して複数の請求書を受け取った 1487
AWS アカウントが閉鎖または完全に閉鎖され、ドメインが Route 53 に登録されている 1488
IP アドレスの範囲 1490
Route 53 ネームサーバーの IP アドレス範囲 1490
Route 53 ヘルスチェックの IP アドレス範囲 1490

プレフィックスリストの参照 1491
Route 53 ヘルスチェックの内部 IP アドレス範囲 1491
リソースのタグ付け 1492
チュートリアル 1494
親ドメインを移行しないで Amazon Route 53 をサブドメインの DNS サービスとして使用する 1495
親ドメインを移行しないで Amazon Route 53 を DNS サービスとして使用するサブドメインを作成する 1496
親ドメインを移行しないでサブドメインの DNS サービスを Amazon Route 53 に移行 1499
Amazon Route 53 でレイテンシーベースルーティングへ移行する 1503
Amazon Route 53 のレイテンシーベースルーティングに別のリージョンを追加する 1506
Amazon Route 53 でレイテンシーおよび加重レコードを使用して、リージョン内の複数の Amazon EC2 インスタンスにトラフィックをルーティングする 1507
Amazon Route 53 で 100 を超える加重レコードを管理する 1509
Amazon Route 53 での重み付けを利用した、耐障害性のある複数のレコードでの応答 1510
ベストプラクティス 1512
Amazon Route 53 DNS のベストプラクティス 1513
VPC Resolver のベストプラクティス 1516
Resolver エンドポイントとのループ構成を防ぐ 1517
Resolver エンドポイントのスケーリング 1517
Resolver エンドポイントの高可用性 1519
DNS ゾーンウォーキング 1520
Resolver エンドポイントのサブネット互換性 1520
Amazon Route 53 ヘルスチェックのベストプラクティス 1521
Amazon Route 53 ドメイン登録のベストプラクティス 1522
API リクエストを行う 1524
ホストゾーン、リソースレコードセット、ヘルスチェックの API リクエストの実行 1524
REST リクエスト 1525
REST レスポンス 1526
ドメイン登録と Route 53 Resolver の API リクエストの作成 1528
RPC リクエスト 1528
RPC レスポンス 1530
Amazon Route 53 API リクエストの署名 1531
関数別の Amazon Route 53 API アクション 1531
関数のタイプ 1531
関数別のアクション 1533

API スロットリング 1541
スロットリングの適用方法 1541
リクエストレートトークンバケットサイズとリフィルレート 1542
スループット制限の変更 1543
API スロットリングをモニタリングする 1544
再試行とエクスポネンシャルバックオフ 1544
制限の引き上げのリクエスト 1545
API スロットリングのベストプラクティス 1545
クォータ 1547
Service Quotas を使用したクォータの表示と管理 1547
エンティティのクォータ 1547
ドメインのクォータ 1548
ホストゾーンのクォータ 1548
レコードのクォータ 1550
Route 53 VPC リゾルバーのクォータ 1550
ヘルスチェックのクォータ 1558
クエリログの設定のクォータ 1559
トラフィックフローポリシーおよびポリシーレコードのクォータ 1559
再利用可能な委任セットのクォータ 1559
Route 53 プロファイルのクォータ 1560
API リクエストの最大数 1561
ChangeResourceRecordSets リクエストの要素数と文字数 1561
Amazon Route 53 API リクエストの頻度 1561
Route 53 VPC Resolver API リクエストの頻度 1562
関連情報 1563
AWS のリソース 1563
サードパーティ製ツールとライブラリ 1564
グラフィカルユーザーインターフェイス 1565
ドキュメント履歴 1566
2025 年のリリース 1566
2024 年のリリース 1568
2023 年のリリース 1570
2022 年のリリース 1571
2021 年のリリース 1572
2020 年のリリース 1572
2018 年のリリース 1573

2017 年のリリース 1574
2016 年のリリース 1576
2015 年のリリース 1580
2014 年のリリース 1583
2013 年のリリース 1586
2012 年のリリース 1587
2011 年のリリース 1588
2010 年のリリース 1588
..... mdlxxxix

Amazon Route 53 とは？

Amazon Route 53 は、可用性と拡張性に優れたドメインネームシステム (DNS) ウェブサービスです。Route 53 を使用すると、ドメイン登録、DNS ルーティング、ヘルスチェックの 3 つの主要な機能を任意の組み合わせで実行できます。

3 つの関数すべてに Route 53 を使用する場合は、次の順序に従います。

1. ドメイン名の登録

   ウェブサイトには example.com などの名前が必要です。Route 53 では、ドメイン名と呼ばれるウェブサイトまたはウェブアプリケーションの名前を登録できます。

   - 概要については、「ドメイン登録の仕組み」を参照してください。
   - 手順については、「新しいドメインの登録」を参照してください。
   - ドメインの登録と、Amazon S3 バケットでの簡単なウェブサイトの作成方法のチュートリアルについては、「Amazon Route 53 の開始方法」を参照してください。

2. ドメインのリソースへのインターネットトラフィックのルーティング

   ユーザーがウェブブラウザを開き、ドメイン名 (example.com) またはサブドメイン名 (acme.example.com) を入力すると、Route 53 はブラウザをウェブサイトまたはウェブアプリケーションに接続します。

   - 概要については、「ウェブサイトやウェブアプリケーションへのインターネットトラフィックのルーティング」を参照してください。
   - 手順については、「DNS サービスとしての Amazon Route 53 の設定」を参照してください。
   - Amazon WorkMail にメールをルーティングする手順については、Amazon WorkMail へのトラフィックのルーティング を参照してください。

3. リソースの正常性のチェック

   Route 53 は、自動リクエストをインターネット経由でウェブサーバーなどのリソースに送信して、そのリソースが到達可能、使用可能、機能中であることを確認します。リソースが使用できなくなったときに通知を受け取ることができます。インターネットトラフィックを異常なリソースから遠ざけることもできます。

   - 概要については、「Amazon Route 53 がリソースの正常性をチェックする方法」を参照してください。

- 手順については、「Amazon Route 53 ヘルスチェックの作成」を参照してください。

Route 53 の他の機能

ドメインネームシステム (DNS) ウェブサービスであることに加えて、Route 53 は次の機能を提供します。

VPC リゾルバー

の Amazon VPCs AWS リージョン、 AWS Outposts ラックVPCs、またはその他のオンプレミスネットワークの再帰的な DNS を取得します。条件付き転送ルールと Route 53 エンドポイントを作成して、Route 53 プライベートホストゾーンまたはオンプレミス DNS サーバーでカスタム名を解決します。

詳細については、「Route 53 VPC Resolver とは」を参照してください。

Amazon Route 53 Resolver on Outposts

VPC Resolver on Outpost ラックを、Resolver エンドポイントを介してオンプレミスデータセンターの DNS サーバーに接続します。これにより、Outposts ラックと他のオンプレミスリソース間の DNS クエリが解決されます。

詳細については、「Amazon Route 53 on Outposts とは」を参照してください。

リゾルバー DNS ファイアウォール

VPC リゾルバー内で再帰的な DNS クエリを保護します。ドメインリストを作成して、これらのルールに対してアウトバウンド DNS トラフィックをフィルタリングするファイアウォールルールを構築します。

詳細については、「DNS ファイアウォールを使用してアウトバウンド DNS トラフィックをフィルタリングする」を参照してください。

トラフィックフロー

使いやすくコスト効率の高いグローバルトラフィック管理: 地理的近接性、レイテンシー、ヘルス、およびその他の考慮事項に基づいて、アプリケーションに最適なエンドポイントにエンドユーザーをルーティングします。

詳細については、「DNS トラフィックのルーティングにトラフィックフローを使用する」を参照してください。

Amazon Route 53 プロファイル

Route 53 プロファイルを使用すると、DNS 関連の Route 53 設定を多くの VPCs と異なる に適用および管理できます AWS アカウント。

詳細については、「Amazon Route 53 プロファイルとは」を参照してください。

トピック

- ドメイン登録の仕組み
- ウェブサイトやウェブアプリケーションへのインターネットトラフィックのルーティング
- Amazon Route 53 がリソースの正常性をチェックする方法
- Amazon Route 53 の概念
- Amazon Route 53 の開始方法
- Amazon Route 53 へのアクセス
- AWS Identity and Access Management
- Amazon Route 53 の料金と請求
- AWS SDK での Route 53 の使用

ドメイン登録の仕組み

ウェブサイトやウェブアプリケーションを作成する場合は、まずウェブサイトの名前 (domain name) を登録します。ドメイン名は、お客様のウェブサイトをユーザーが表示するためにブラウザーに入力する名前 (example.com など) です。

ここでは、Amazon Route 53 を使用してドメイン名を登録する方法の概要を示します。

1. ドメイン名を選択し、希望するドメイン名が使用可能であること、つまり、他の誰もが登録していないことを確認します。

   使用するドメイン名がすでに使用されている場合は、他の名前を試すか、.com などの最上位ドメインのみを .ninja や .hockey などの別の最上位ドメインに変更することができます。Route 53 でサポートされている最上位ドメインの一覧については、「Amazon Route 53 に登録できる最上位ドメイン」を参照してください。
2. Route 53 を使用してドメイン名を登録します。ドメインを登録するときは、ドメインの所有者の名前と連絡先情報、その他の連絡先の名前とその情報を提供します。

Route 53 にドメインを登録すると、サービスは自動的にドメインの DNS サービスになります。以下が実行されます。

- ドメインと同じ名前の hosted zone を作成します。
- 4 つの一連のネームサーバーをホストゾーンに割り当てます。誰かがブラウザを使用して www.example.com などのウェブサイトにアクセスすると、これらのネームサーバーはウェブサーバーや Amazon S3 バケットなどのリソースを探す場所をブラウザに指示します。(Amazon S3 は、ウェブ上の任意の場所から任意の量のデータを保存および取得するためのオブジェクトストレージです。A バケットは、S3 に保存するオブジェクトのコンテナです。)
- ホストゾーンからネームサーバーを取得し、ドメインに追加します。

詳細については、「ウェブサイトやウェブアプリケーションへのインターネットトラフィックのルーティング」を参照してください。

3. 登録プロセスの終了時に、Route 53 はドメインのレジストラに情報を送信します。domain registrar は、Amazon Registrar, Inc. か、当社のレジストラ関連会社である Gandi のいずれかです。ドメインのレジストラを見つける方法については、「レジストラの検索」を参照してください。
4. レジストラはお客様の情報をドメインのレジストリに送信します。レジストリとは、.com などの 1 つまたは複数の最上位ドメインのドメイン登録を販売する会社です。
5. レジストリは、お客様のドメインに関する情報を自社のデータベースに保存し、その情報の一部をパブリック WHOIS データベースにも保存します。

ドメイン名を登録する方法の詳細については、「新しいドメインの登録」を参照してください。

別のレジストラにドメイン名を既に登録している場合は、ドメイン登録を Route 53 に移管できます。この操作は、Route 53 の他の機能を使用する場合は不要です。詳細については、「ドメイン登録の Amazon Route 53 への移管」を参照してください。

ウェブサイトやウェブアプリケーションへのインターネットトラフィックのルーティング

インターネット上のすべてのコンピューターは、スマートフォンやラップトップから、大規模な小売サイトのコンテンツに対応するサーバーに至るまで、番号を使用して相互に通信します。これらの番号は、IP アドレスと呼ばれ、以下のいずれかの形式になります。

- インターネットプロトコルバージョン 4 (IPv4) 形式 (192.0.2.44 など)

- インターネットプロトコルバージョン 6 (IPv6) 形式 (2001:0db8:85a3:0000:0000:abcd:0001:2345 など)

ブラウザを開いてウェブサイトにアクセスするときは、このような長い文字列を覚えて入力する必要はありません。代わりに、example.com のようなドメイン名を入力しても、正しい場所に移動できます。Amazon Route 53 などの DNS サービスは、ドメイン名と IP アドレス間の接続を行います。

トピック

- ドメインのインターネットトラフィックをルーティングするように Amazon Route 53 を設定する方法の概要
- Amazon Route 53 によりドメインのトラフィックをルーティングする方法

ドメインのインターネットトラフィックをルーティングするように Amazon Route 53 を設定する方法の概要

ここでは、Amazon Route 53 コンソールを使用してドメイン名を登録し、ウェブサイトやウェブアプリケーションにインターネットトラフィックをルーティングするように Route 53 を設定する方法の概要を示します。

1. お客様のユーザーがコンテンツへのアクセスに使用するドメイン名を登録します。概要については、「ドメイン登録の仕組み」を参照してください。
2. ドメイン名を登録した後、Route 53 はドメインと同じ名前のパブリックホストゾーンを自動的に作成します。詳細については、「「パブリックホストゾーンの操作」」を参照してください。
3. リソースにトラフィックをルーティングするには、レコード (リソースレコードセット) をホストゾーンに作成します。各レコードには、次のようなドメインのトラフィックをルーティングする方法に関する情報が含まれています。

   名前

   レコードの名前は、Route 53 でトラフィックをルーティングするドメイン名 (example.com) またはサブドメイン名 (www.example.com、retail.example.com) に対応します。

   ホストゾーン内の各レコードの名前は、ホストゾーンの名前で終わる必要があります。例えば、ホストゾーンの名前が example.com の場合、すべてのレコード名は example.com で終わる必要があります。Route 53 コンソールはこの処理を自動的に行います。

タイプ

レコードタイプによって通常、トラフィックをルーティングする先のリソースのタイプが決まります。例えば、トラフィックを E メールサーバーにルーティングするには、[Type] で [MX] を指定します。IPv4 IP アドレスが割り当てられたウェブサーバーにトラフィックをルーティングするには、[Type] で [A] を指定します。

値

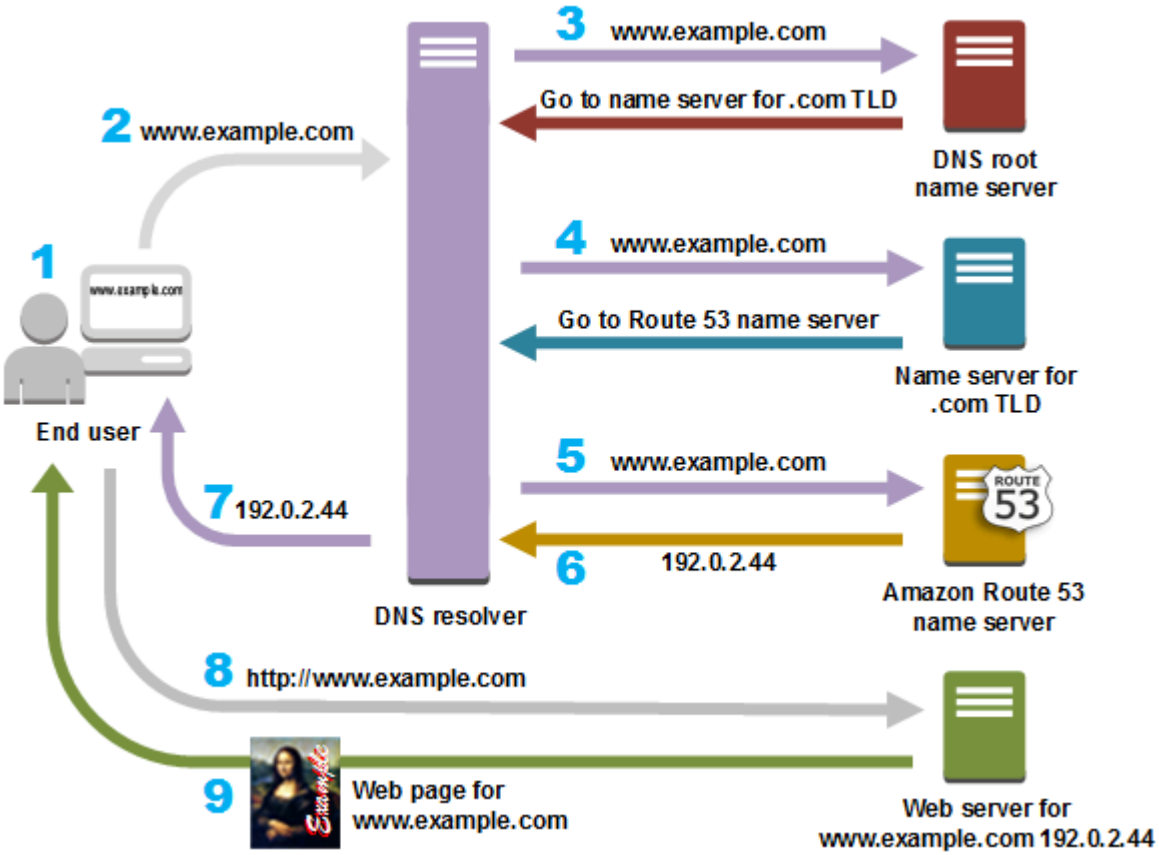
値は [Type] と密接に関連します。[Type] で [MX] を指定する場合は、[Value] で 1 つ以上の E メールサーバーの名前を指定します。[Type] で [A] を指定する場合は、IP アドレスを IPv4 形式 (192.0.2.136 など) で指定します。

レコードの詳細については、「レコードを使用する」を参照してください。

エイリアスレコードと呼ばれる特殊な Route 53 レコードを作成して、トラフィックを Amazon S3 バケット、Amazon CloudFront ディストリビューション、およびその他の AWS リソースにルーティングすることもできます。詳細については、「エイリアスレコードと非エイリアスレコードの選択」および「AWS リソースへのインターネットトラフィックのルーティング」を参照してください。

Amazon Route 53 によりドメインのトラフィックをルーティングする方法

インターネットトラフィックをウェブサーバーや Amazon S3 バケットなどのリソースにルーティングするように Amazon Route 53 を設定した後、www.example.com のコンテンツをリクエストすると、数ミリ秒で次のようになります。 Amazon S3



1. ユーザーがウェブブラウザを開き、アドレスバーに www.example.com を入力して、Enter キーを押します。
2. www.example.com のリクエストは DNS リゾルバーにルーティングされます。DNS リゾルバーは通常、ケーブルインターネットプロバイダー、DSL ブロードバンドプロバイダー、企業ネットワークなど、ユーザーのインターネットサービスプロバイダー (ISP) によって管理されます。
3. ISP の DNS リゾルバーは、www.example.com のリクエストを DNS ルートネームサーバーに転送します。
4. DNS リゾルバーは www.example.com のリクエストが再びあると、今度は .com ドメインのいずれかの TLD ネームサーバーに転送します。.com ドメインのネームサーバーは、example.com ドメインに関連付けられた 4 つの Route 53 ネームサーバーの名前で応答します。

   DNS リソルバーは、4 つの Route 53 ネームサーバーをキャッシュ (保存) します。次回に誰かが example.com を参照すると、すでに example.com のネームサーバーがあるため、ステップ 3 および 4 はスキップされます。通常、ネームサーバーは 2 日間キャッシュされます。
5. DNS リゾルバーは、Route 53 ネームサーバーを選択し、www.example.com のリクエストをそのネームサーバーに転送します。

6. Route 53 ネームサーバーは、example.com ホストゾーンで www.example.com レコードを検索し、関連付けられた値 (ウェブサーバーの IP アドレス 192.0.2.44 など) を取得して、IP アドレスを DNS リゾルバーに返します。
7. DNS リゾルバーに、ユーザーが必要とする IP アドレスが追加されました。リゾルバーは、その値をウェブブラウザに返します。

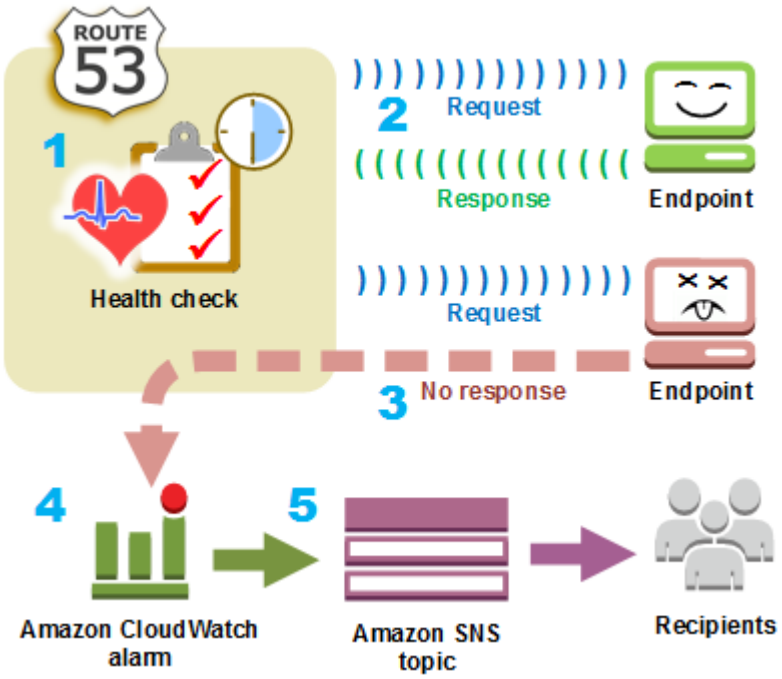
> **Note**
>
> DNS リゾルバーは、指定された期間、example.com の IP アドレスをキャッシュして、次回に誰かが example.com を参照すると、より高速に応答できるようにもします。詳細については、「time to live (TTL)」を参照してください。

8. ウェブブラウザは、DNS リゾルバーから取得した IP アドレスに www.example.com のリクエストを送信します。これは、Amazon EC2 インスタンスで実行されているウェブサーバー、ウェブサイトエンドポイントとして設定されている Amazon S3 バケットなど、お客様のコンテンツが置かれている場所です。
9. 192.0.2.44 にあるウェブサーバーなどのリソースは、www.example.com のウェブページをウェブブラウザに返し、ウェブブラウザはそのページを表示します。

Amazon Route 53 がリソースの正常性をチェックする方法

Amazon Route 53 ヘルスチェックでは、ウェブサーバーや E メールサーバーなどのリソースの正常性を監視します。ヘルスチェックの Amazon CloudWatch アラームを設定して、リソースが使用できなくなったときに通知を受け取ることができます。

ここでは、リソースが使用不可になったら通知を受け取る場合のヘルスチェックのしくみの概要を示します。



1. ヘルスチェックを作成し、ヘルスチェックの実行方法を定義する以下の値を指定します。
   - Route 53 でモニタリングするウェブサーバーなどのエンドポイントの IP アドレスまたはドメイン名 (他のヘルスチェックのステータス、または CloudWatch アラームの状態をモニタリングすることもできます)。
   - Amazon Route 53 がチェックの実行に使用するプロトコル (HTTP、HTTPS、または TCP)。
   - Route 53 がエンドポイントにリクエストを送信する頻度。これはリクエスト間隔です。
   - Route 53 が異常と判断するまでにエンドポイントが応答に失敗しなければならない連続回数。これは失敗しきい値です。
   - 必要に応じて、Route 53 がエンドポイントを異常とみなしたときの通知方法。通知を設定すると、Route 53 は CloudWatch アラームを設定します。CloudWatch は Amazon SNS を使用して、エンドポイントが異常であることをユーザーに通知します。
2. Route 53 は、ヘルスチェックで指定した間隔でエンドポイントにリクエストを送信し始めます。

   エンドポイントがリクエストに応答した場合、Route 53 はエンドポイントを正常とみなし、何も処理を実行しません。
3. エンドポイントがリクエストに応答しない場合、Route 53 は、エンドポイントがリクエストに応答しない連続回数のカウントを開始します。
   - 指定した失敗しきい値にカウントが達すると、Route 53 はそのエンドポイントを異常とみなします。

- カウントが失敗しきい値に達するまでにエンドポイントが再び応答を開始すると、Route 53 はカウントを 0 にリセットし、CloudWatch はお客様に通知しません。

4. Route 53 がエンドポイントを異常とみなし、ヘルスチェックの通知を設定している場合、Route 53 は CloudWatch に通知します。

   通知を設定していない場合でも、Route 53 ヘルスチェックのステータスは Route 53 コンソールで確認できます。詳細については、「ヘルスチェックのステータス監視と通知の受信」を参照してください。

5. ヘルスチェックの通知を設定している場合、CloudWatch はアラームをトリガーし、指定した受取人に Amazon SNS を使用して通知を送信します。

指定したエンドポイントの正常性をチェックするだけでなく、1 つ以上の他のヘルスチェックの正常性をチェックするようにヘルスチェックを設定できます。これにより、5 つのうち 2 つのウェブサーバーなど、指定された数のリソースがいつ使用できないかがわかります。CloudWatch アラームのステータスをチェックするようにヘルスチェックを設定して、リソースがリクエストに応答しているかどうかだけでなく、幅広い基準に基づいて通知を受け取ることもできます。

ウェブサーバーやデータベースサーバーなど、同じ機能を実行する複数のリソースがある場合は、DNS フェイルオーバーを設定できます。ヘルスチェックをそのリソースの各レコードに関連付けます。基盤となるリソースが正常でないとヘルスチェックでわかった場合、Route 53 は関連付けられているレコードにトラフィックをルーティングしないようにします。

Route 53 を使用してリソースの正常性を監視する方法の詳細については、「Amazon Route 53 ヘルスチェックの作成」を参照してください。

Amazon Route 53 の概念

ここでは、Amazon Route 53 デベロッパーガイド 全体で説明されている概念の概要を示します。

トピック

- ドメイン登録の概念
- ドメインネームシステム (DNS) の概念
- コントロールプレーンとデータプレーンの概念
- ヘルスチェックの概念

ドメイン登録の概念

ここでは、ドメイン登録に関連する概念の概要を示します。

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

ドメイン名

ユーザーがウェブブラウザのアドレスバーに入力してウェブサイトやウェブアプリケーションにアクセスするための名前 (example.com など)。ウェブサイトやウェブアプリケーションをインターネットで使用できるようにするには、まずドメイン名を登録します。詳細については、「ドメイン登録の仕組み」を参照してください。

ドメインレジストラ

特定の最上位ドメイン (TLD) のドメイン登録を処理する ICANN (Internet Assigned Names and Numbers) から認定を受けている会社。ドメインのレジストラを見つける方法については、「レジストラの検索」を参照してください。

ドメインレジストリ

特定の最上位ドメインを含むドメインを販売する権利を有する会社。たとえば、VeriSign は、.com TLD を含むドメインを販売する権利を有するレジストリです。ドメインレジストリは、地理的 TLD に関する居住者要件など、ドメインを登録するためのルールを定義します。また、ドメインレジストリは、同じ TLD を含むすべてのドメイン名に対する信頼できるデータベースを維持しています。レジストリのデータベースには、各ドメインの連絡先情報やネームサーバーなどの情報が保存されています。

ドメインリセラー

Amazon Registrar などのレジストラのドメイン名を販売する会社。Amazon Route 53 は、Amazon Registrar と当社のレジストラ関連会社である Gandi のドメインリセラーです。

最上位ドメイン (TLD)

.com、.org、.ninja などのドメイン名の末尾の部分。最上位ドメインには 2 つのタイプがあります。

汎用最上位ドメイン

これらの TLD は通常、ユーザーにウェブサイトで見つかるものを連想させます。たとえば、TLD が .bike のドメイン名は、オートバイや自転車のビジネスや組織のウェブサイトに関連付けられていることがよくあります。いくつかの例外を除き、お客様は任意の一般的な TLD を使用できるため、自転車のクラブがドメイン名に .hockey TLD を使用しても構いません。

地理的最上位ドメイン

これらの TLD は国や都市などの地理的地域に関連付けられています。地理的 TLD の一部のレジストリは居住者要件を設けており、the section called “.io (英領インド洋地域)” などの他のレジストリは汎用 TLD の使用を許可または推奨しています。

Route 53 でドメイン名を登録する際に使用できる TLD の一覧については、「Amazon Route 53 に登録できる最上位ドメイン」を参照してください。

ドメインネームシステム (DNS) の概念

ここでは、ドメインネームシステム (DNS) に関連する概念の概要を示します。

- 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)

エイリアスレコード

Amazon CloudFront ディストリビューションや Amazon S3 バケットなどの AWS リソースにトラフィックをルーティングするために Amazon Route 53 で作成できるレコードのタイプ。Amazon S3 詳細については、「エイリアスレコードと非エイリアスレコードの選択」を参照してください。

権威ネームサーバー

ドメインネームシステム (DNS) の一部に関する決定的な情報を持つネームサーバー。該当する情報を返すことで、DNS リゾルバーからのリクエストに応答します。例えば、.com 最上位ドメイン (TLD) の権威ネームサーバーは、登録されたすべての .com ドメインのネームサーバーの名前を認識しています。.com 権威ネームサーバーが example.com の DNS リゾルバーからリクエストを受信すると、example.com ドメインの DNS サービスのネームサーバーの名前で応答します。

Route 53 ネームサーバーは、Route 53 を DNS サービスとして使用するすべてに対するドメインの権威ネームサーバーです。ネームサーバーは、お客様がドメインのホストゾーンで作成したレコードに基づいて、ドメインおよびサブドメインのトラフィックをどのようにルーティングするかを認識しています (Route 53 ネームサーバーは、Route 53 を DNS サービスとして使用するドメインのホストゾーンを保存しています)。

例えば、Route 53 ネームサーバーが www.example.com のリクエストを受信すると、そのレコードを検索し、レコードに指定されている 192.0.2.33 などの IP アドレスを返します。

CIDR ブロック

CIDR ブロックは IP の範囲であり、IP ベースルーティングで使用されます。Route 53 では、IPv4 の場合は IPv4IPv6 の場合は /0 ~ /48 の CIDR ブロックを指定できます。例えば、/24 IPv4 の CIDR ブロックには、256 個の連続した IP アドレスが含まれます。CIDR ブロック (または IP 範囲) を CIDR ロケーションにグループ化し、再利用可能な CIDR コレクションにグループ化できます。

DNS クエリ

コンピュータやスマートフォンなどのデバイスがドメイン名に関連付けられたリソースのドメインネームシステム (DNS) に送信するリクエスト。DNS クエリの最も一般的な例は、ユーザーがブラウザを開いてアドレスバーにドメイン名を入力するときです。DNS クエリへの応答は通常、ウェブサーバーなどのリソースに関連付けられた IP アドレスです。リクエストを開始したデバイ

スは、IP アドレスを使用してリソースと通信します。例えば、ブラウザは IP アドレスを使用してウェブサーバーからウェブページを取得できます。

DNS リゾルバー

インターネットサービスプロバイダー (ISP) によって管理される DNS サーバー。ユーザーのリクエストと DNS ネームサーバーの仲介役を果たします。ブラウザを開いてアドレスバーにドメイン名を入力すると、クエリはまず DNS リゾルバーに送信されます。リゾルバーは DNS ネームサーバーと通信して、ウェブサーバーなどのリソースの IP アドレスを取得します。DNS リゾルバーは再帰的なネームサーバーとも呼ばれます。これは、ラップトップ上のウェブブラウザなど、ユーザーのデバイスに返されるレスポンス (通常は IP アドレス) を取得するまで、一連の信頼できる DNS ネームサーバーにリクエストを送信するためです。

ドメインネームシステム (DNS)

コンピューター、スマートフォン、タブレット、その他の IP 対応デバイスの相互通信を支援する世界規模のサーバーネットワーク。ドメインネームシステムは、example.com など簡単に理解できる名前を IP アドレスと呼ばれる番号に変換して、インターネットでコンピューター同士がそれらの番号を使用して相互に検索できるようにします。

「IP address」も参照してください。

ホストゾーン

ドメイン (example.com など) とそのすべてのサブドメイン (www.example.com、retail.example.com、seattle.accounting.example.com など) のトラフィックをルーティングする方法に関する情報を含むレコードのコンテナ。ホストゾーンの名前はドメインと同じです。

例えば、example.com のホストゾーンには、www.example.com のトラフィックを IP アドレス 192.0.2.243 のウェブサーバーにルーティングするための情報から成るレコードと、example.com の E メールを mail1.example.com と mail2.example.com の 2 つの E メールサーバーにルーティングするための情報から成るレコードを含めることができます。各 E メールサーバーにもそれぞれに固有のレコードが必要です。

「record (DNS record)」も参照してください。

IP アドレス

インターネット上のデバイス (ラップトップ、スマートフォン、Web サーバなど) に割り当てられる番号。デバイスがインターネット上の他のデバイスと通信できるようにします。IP アドレスは以下のいずれかの形式になります。

- インターネットプロトコルバージョン 4 (IPv4) 形式 (192.0.2.44 など)
- インターネットプロトコルバージョン 6 (IPv6) 形式 (2001:0db8:85a3:0000:0000:abcd:0001:2345 など)

Route 53 は、以下の目的で IPv4 アドレスと IPv6 アドレスの両方をサポートしています。

- IPv4 アドレスの場合は A タイプ、IPv6 アドレスの場合は AAAA タイプのレコードを作成できる
- リクエストを IPv4 または IPv6 アドレスに送信するヘルスチェックを作成できる
- DNS リゾルバーが IPv6 ネットワークにある場合は、IPv4 または IPv6 のいずれかを使用して、Route 53 にリクエストを送信できる

ネームサーバー

コンピューターが相互に通信するために使用する IP アドレスにドメイン名を変換するためのドメインネームシステム (DNS) のサーバー。ネームサーバーは再帰ネームサーバー (DNS resolver) または authoritative name server のいずれかになります。

DNS がトラフィックをリソースにどのようにルーティングするか (そのプロセスでの Route 53 の役割も含む) の概要については、「Amazon Route 53 によりドメインのトラフィックをルーティングする方法」を参照してください。

プライベート DNS

ドメインとそのサブドメインのトラフィックを 1 つ以上の Amazon Virtual Private Cloud (VPC) 内の Amazon EC2 インスタンスにルーティングできるドメインネームシステム (DNS) のローカルバージョン。 VPCs 詳細については、「プライベートホストゾーンの使用」を参照してください。

レコード (DNS レコード)

ドメインまたはサブドメインのトラフィックをどのようにルーティングするかを定義するために使用する、ホストゾーン内のオブジェクト。例えば、IP アドレスが 192.0.2.234 のウェブサーバーにトラフィックをルーティングする example.com と www.example.com のレコードを作成できます。

Route 53 固有のレコードによって提供される機能に関する情報を含め、レコードの詳細については、「DNS サービスとしての Amazon Route 53 の設定」を参照してください。

再帰ネームサーバー

「DNS resolver」を参照してください。

再利用可能な委託セット

複数のホストゾーンで使用できる 4 つの一連の権威ネームサーバー。デフォルトでは、Route 53 はランダムに選択されたネームサーバーを新しいホストゾーンごとに割り当てます。多数のドメインの DNS サービスを Route 53 に移行しやすくするために、再利用可能な委任セットを作成できます。次に、再利用可能な委任セットを新しいホストゾーンに関連付けます。(既存のホストゾーンに関連付けられているネームサーバーを変更することはできません)。

再利用可能な委任セットを作成し、ホストゾーンにプログラムで関連付けます。Route 53 コンソールの使用はサポートされていません。詳細については、Amazon Route 53 API リファレンスの「CreateHostedZone」と「CreateReusableDelegationSet」を参照してください。AWS SDK、AWS Command Line Interface、および AWS Tools for Windows PowerShell でも同じ機能を利用できます。

ルーティングポリシー

Route 53 が DNS クエリに応答する方法を決定するレコードの設定。Route 53 は、次のルーティングポリシーをサポートしています。

- シンプルルーティングポリシー – ドメインで特定の機能を実行する単一のリソース (example.com ウェブサイトにコンテンツを提供するウェブサーバーなど) にインターネットトラフィックをルーティングするために使用します。
- フェイルオーバールーティングポリシー – アクティブ/パッシブフェイルオーバーを構成する場合に使用します。
- 位置情報ルーティングポリシー– ユーザーの場所に基づいてインターネットトラフィックをリソースにルーティングする場合に使用します。
- 地理的近接性ルーティングポリシー – リソースの場所に基づいてトラフィックをルーティングし、必要に応じてトラフィックをある場所のリソースから別の場所のリソースに移動する場合に使用します。
- レイテンシールーティングポリシー– 複数の場所にリソースがあり、レイテンシーが最も小さいリソースにトラフィックをルーティングする場合に使用します。
- IP ベースのルーティングポリシー – トラフィックの送信元の IP アドレスがわかっており、ユーザーの位置に基づいてトラフィックをルーティングする際に使用します。
- 複数値回答ルーティングポリシー – ランダムに選ばれた最大 8 つの正常なレコードを使用して Route 53 が DNS クエリに応答する場合に使用します。
- 加重ルーティングポリシー– 指定した比率で複数のリソースにトラフィックをルーティングする場合に使用します。

詳細については、「ルーティングポリシーの選択」を参照してください。

サブドメイン

登録されたドメイン名の前に 1 つ以上のラベルが付いたドメイン名。例えば、example.com というドメイン名を登録している場合、www.example.com はサブドメインになります。example.com ドメインのホストゾーン accounting.example.com を作成している場合、seattle.accounting.example.com はサブドメインになります。

サブドメインのトラフィックをルーティングするには、必要な名前 (www.example.com など) でレコードを作成し、ウェブサーバーの IP アドレスなどの適切な値を指定します。

TTL (有効期限)

DNS リゾルバーが、レコードの現在の値を取得するために Route 53 に別のリクエストを送信するまで、レコードの値をキャッシュ (保存) する必要のある期間 (秒単位)。TTL が期限切れになる前に DNS リゾルバーが同じドメインに対する別のリクエストを受信すると、リゾルバーはキャッシュされた値を返します。

Route 53 の料金は Route 53 が応答する DNS クエリの数に一部基づいているため、TTL を長くすると料金を減らすことができます。TTL を短くすると、www.example.com のウェブサーバーの IP アドレスを変更するなどして、レコードの値を変更した後に DNS リゾルバーが古いリソースにトラフィックをルーティングする時間を短縮できます。

コントロールプレーンとデータプレーンの概念

ここでは、Amazon Route 53 がその機能をコントロールとデータプレーンに分割する方法に関連する概念の概要を示します。ほとんどの と同様に AWS のサービス、Route 53 にはコントロールプレーンとデータプレーンが含まれています。コントロールプレーンを使用すると、リソースの作成、更新、削除などの管理オペレーションを実行できます。データプレーンは、サービスのコア機能を提供します。どちらも信頼性が高いように構築されています。コントロールプレーンはデータ整合性のために最適化されていますが、データプレーンは可用性のために最適化されています。データプレーンの耐障害性設計により、コントロールプレーンが使用できなくなる可能性のあるまれな破壊イベントでも可用性を維持できます。このため、可用性が重要なデータプレーン関数を使用します。

Route 53 パブリックおよびプライベート DNS とヘルスチェックの場合、コントロールプレーンは us-east-1 にあり AWS リージョン 、データプレーンはグローバルに分散されます。

Amazon Route 53 は、次のようにコントロールプレーンとデータプレーンに分けられます。

- Route 53 パブリックおよびプライベート DNS の場合、コントロールプレーンは Route 53 APIs で構成され、DNS エントリを管理できます。これには、Route 53 と Traffic Flow APIs の両方が含ま

れます。Route 53 コンソールは us-east-1 にありますが AWS リージョン、 がそのリージョンに障害がある AWS と判断した場合、Route 53 コンソールは us-west-2 によって提供されます AWS リージョン。データプレーンは、信頼できる DNS サービスです。200 を超えるポイントオブプレゼンス (PoP) ロケーションで実行され、ホストゾーンとヘルスチェックデータに基づいて DNS クエリに応答します。

- Route 53 ヘルスチェックの場合、コントロールプレーンは Route 53 API で構成され、ヘルスチェックの作成、更新、削除に使用できます。Route 53 ヘルスチェックコンソールは us-east-1 にありますが AWS リージョン、 がそのリージョンに障害がある AWS と判断した場合、Route 53 ヘルスチェックコンソールは us-west-2 によって提供されます AWS リージョン。データプレーンは、ヘルスチェックを実行し、結果を集約して、Route 53 パブリックおよびプライベート DNS とのデータプレーンに配信するグローバル分散サービスですAWS Global Accelerator。
- Route 53 VPC Resolver の場合、コントロールプレーンは、Amazon VPC 設定、Resolver ルール、クエリログ記録ポリシー、DNS Firewall ポリシーを管理できる VPC Resolver APIs で構成されます。データプレーンは DNS リゾルバーサービスです。VPC 内の DNS クエリに応答し、エンドポイントを介してクエリを他のリゾルバーに転送し、DNS ファイアウォールポリシーを適用して DNS クエリをフィルタリングします。VPC Resolver はリージョナルサービスです。コントロールプレーンとデータプレーンはそれぞれ独立して実行されます AWS リージョン。
- Route 53 ドメイン登録は、us-east-1 のコントロールプレーンでのみ管理されます。 AWS リージョン。

データプレーン、コントロールプレーン、および が高可用性目標を達成するためのサービス AWS を構築する方法の詳細については、Amazon Builders' Library の「アベイラビリティーゾーンを使用した静的安定性」を参照してください。

ヘルスチェックの概念

ここでは、Amazon Route 53 ヘルスチェックに関連する概念の概要を示します。

- DNS failover
- endpoint
- health check

DNS フェイルオーバー

異常なリソースから正常なリソースにトラフィックをルーティングするための手法。複数のウェブサーバーやメールサーバーなど、同じ機能を実行するリソースが複数ある場合は、Route 53

ヘルスチェックを設定してリソースの正常性を確認できます。次に、正常なリソースにのみトラフィックをルーティングするようにホストゾーンのレコードを設定します。

詳細については、「DNS フェイルオーバーの設定」を参照してください。

エンドポイント

ヘルスチェックで正常性のモニタリング対象として設定しているリソース (ウェブサーバーや E メールサーバーなど)。IPv4 アドレス (192.0.2.243)、IPv6 アドレス (2001:0db8:85a3:0000:0000:abcd:0001:2345)、またはドメイン名 (example.com) によりエンドポイントを指定できます。

> **Note**
>
> 他のヘルスチェックのステータスや CloudWatch アラームのステータスをモニタリングするヘルスチェックを作成することもできます。

ヘルスチェック

以下を実行するために使用できる Route 53 コンポーネント。

- ウェブサーバーなどの指定したエンドポイントが正常であるかどうかをモニタリングする
- 必要に応じて、エンドポイントが異常になったら通知を受け取る
- 必要に応じて、DNS フェイルオーバーを設定し、インターネットトラフィックを異常なリソースから正常なリソースに再ルーティングできるようにします。

ヘルスチェックの作成および使用方法の詳細については、「Amazon Route 53 ヘルスチェックの作成」を参照してください。

Amazon Route 53 の開始方法

Amazon Route 53 の開始方法については、このガイドの以下のトピックを参照してください。

- Amazon Route 53 を設定する: にサインアップする方法 AWS、 AWS アカウントへのアクセスを保護する方法、Route 53 へのプログラムによるアクセスを設定する方法について説明します。
- Amazon Route 53 の開始方法。ドメイン名を登録し、静的ウェブサイトをホストするように設定された Amazon S3 バケットを作成し、インターネットトラフィックをウェブサイトにルーティングする方法について説明します。

Amazon Route 53 へのアクセス

Amazon Route 53 には、以下の方法でアクセスできます。

- AWS マネジメントコンソール – このガイドの手順では、 を使用してタスク AWS マネジメントコンソール を実行する方法について説明します。
- AWS SDKs – SDK を提供する AWS プログラミング言語を使用している場合は、 SDK を使用して Route 53 にアクセスできます。SDKs認証を簡素化し、開発環境と統合して、Route 53 コマンドへのアクセスを提供します。詳細については、Tools for Amazon Web Services を参照してください。
- Route 53 API – SDK が提供されていないプログラミング言語を使用している場合、API アクションと API リクエストの作成方法の情報については、Amazon Route 53 API リファレンスを参照してください。
- AWS Command Line Interface - 詳細については、 AWS Command Line Interface ユーザーガイドのAWS Command Line Interfaceのセットアップを始めるを参照してください。
- AWS Tools for Windows PowerShell - 詳細については、 AWS Tools for PowerShell ユーザーガイドの AWS Tools for Windows PowerShellのセットアップを参照してください。

AWS Identity and Access Management

Amazon Route 53 は、組織が以下を行うために使用できるサービスである AWS Identity and Access Management (IAM) と統合されています。

- 組織の AWS アカウントでユーザーとグループを作成する
- AWS アカウントのユーザー間でアカウントリソースを簡単に共有する
- 各ユーザーに一意のセキュリティ認証情報を割り当てる
- サービスやリソースに対するユーザーのアクセス権を細分化して制御する

例えば、Route 53 で IAM を使用して、 AWS アカウント内のどのユーザーが新しいホストゾーンを作成またはレコードを変更できるかを制御できます。

IAM の一般的な情報については、以下を参照してください。

- Amazon Route 53 での Identity and Access Management
- Identity and Access Management (IAM)

- IAM ユーザーガイド

Amazon Route 53 の料金と請求

他の AWS 製品と同様に、Amazon Route 53 を使用するための契約や最低契約金はありません。設定したホストゾーンと、Route 53 が応答する DNS クエリの数に対してのみお支払いいただきます。詳細については、「Amazon Route 53 料金表」を参照してください。

請求の表示方法、アカウントと支払いの管理方法など、 AWS サービスの請求については、AWS Billing 「 ユーザーガイド」を参照してください。

AWS SDK での Route 53 の使用

AWS Software Development Kit (SDKsは、多くの一般的なプログラミング言語で使用できます。各 SDK には、デベロッパーが好みの言語でアプリケーションを簡単に構築できるようになる API、コード例、およびドキュメントが提供されています。

SDK ドキュメント	コード例
AWS SDK for C++	AWS SDK for C++ コード例
AWS CLI	AWS CLI コード例
AWS SDK for Go	AWS SDK for Go コード例
AWS SDK for Java	AWS SDK for Java コード例
AWS SDK for JavaScript	AWS SDK for JavaScript コード例
AWS SDK for Kotlin	AWS SDK for Kotlin コード例
AWS SDK for .NET	AWS SDK for .NET コード例
AWS SDK for PHP	AWS SDK for PHP コード例
AWS Tools for PowerShell	AWS Tools for PowerShell コード例
AWS SDK for Python v4	AWS SDK for Python v4 のコード例
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto3) コード例

SDK ドキュメント	コード例
AWS SDK for Ruby	AWS SDK for Ruby コード例
AWS SDK for Rust	AWS SDK for Rust コード例
AWS SDK for SAP ABAP	AWS SDK for SAP ABAP コード例
AWS SDK for Swift	AWS SDK for Swift コード例

Route 53 に固有の例については、「AWS SDK を使用した Route 53 のコード例」を参照してください。

> **可用性の例**
>
> 必要なものが見つからなかった場合。このページの下側にある [Provide feedback] リンクから、コードの例をリクエストしてください。

Amazon Route 53 の開始方法

Amazon Route 53 にドメインを登録し、静的ウェブサイトの DNS クエリに応答するように Route 53 を設定して開始します。最初のトピックでは、開いている Amazon S3 バケットに静的ウェブサイトをホストします。2 番目のトピックでは、Amazon CloudFront ディストリビューションを使用してウェブサイトに SSL/TLS を提供します。

推定コスト

- ドメインの登録には年額料金がかかります。料金の範囲は、.com などの最上位ドメインに応じて 9 USD から数百 USD です。詳細については、Route 53 のドメイン登録価格を参照してください。この料金は返金の対象外です。
- ドメインを登録すると、同じ名前のホストゾーンが作成されます。ホストゾーンを使用して、Route 53 がドメインのトラフィックをルーティングする場所を指定します。
- この設定の一環として、Amazon S3 バケットを作成し、サンプルウェブページをアップロードします。 AWS の新規のお客様の場合、Amazon S3 は無料で使い始めることができます。既存の AWS 顧客の場合、料金は、保存するデータの量、データに対するリクエストの数、転送されるデータの量に基づきます。詳細については、Amazon S3 の料金 を参照してください。
- CloudFront の料金は、データに対するリクエストの数、使用するエッジロケーションの数、および転送されたデータの量に基づきます。詳細については、「CloudFront 料金表」を参照してください。

トピック

- Amazon Route 53 を設定する
- Amazon S3 バケットの静的なウェブサイトにドメインを使用する
- Amazon CloudFront ディストリビューションを使用して静的なウェブサイトを提供する

Amazon Route 53 を設定する

トピック

- にサインアップする AWS アカウント
- ツールをダウンロード

にサインアップする AWS アカウント

の使用を開始するには AWS、 が必要です AWS アカウント。の作成の詳細については AWS アカウント、「 AWS アカウント管理 リファレンスガイド」の「 の開始方法 AWS アカウント」を参照してください。

ツールをダウンロード

には Amazon Route 53 用のコンソール AWS マネジメントコンソール が含まれていますが、プログラムでサービスにアクセスする場合は、以下を参照してください。

- API ガイドには、サービスがサポートする操作が記載されており、関連する SDK および CLI ドキュメントへのリンクを提供します。
  - Amazon Route 53 API Reference (Amazon Route 53 API リファレンス)
- raw HTTP リクエストの組み立てなどの低レベルの詳細を処理せずに API を呼び出すには、 AWS SDK を使用できます。 AWS SDKs は、 AWS サービスの機能をカプセル化する関数とデータ型を提供します。 AWS SDK をダウンロードしてインストール手順にアクセスするには、該当するページを参照してください。
  - Java
  - JavaScript
  - .NET
  - Node.js
  - PHP
  - Python
  - Ruby

  AWS SDKs「Amazon Web Services のツール」を参照してください。
- AWS Command Line Interface (AWS CLI) を使用して、コマンドラインから複数の AWS サービスを制御できます。スクリプトを使用してコマンドを自動化することもできます。詳細については、「AWS Command Line Interface」を参照してください。
- AWS Tools for Windows PowerShell は、これらの AWS サービスをサポートしています。詳細については、「AWS Tools for PowerShell コマンドレットリファレンス」(Cmdlet リファレンス) を参照してください。

Amazon S3 バケットの静的なウェブサイトにドメインを使用する

このトピックでは、Amazon Route 53 を使用してドメインの DNS トラフィックを静的ウェブサイトをホストする Amazon Simple Storage Service バケットにルーティングする方法について説明します。ドメインを S3 ウェブサイトエンドポイントにポイントするエイリアスレコードを作成します。

このトピックは、完全な静的ウェブサイト設定ワークフローの一部です。任意の S3 バケットへのトラフィックのルーティングに関する一般的な情報については、「Amazon S3 バケットでホストされているウェブサイトへのトラフィックのルーティング」を参照してください。

これらのステップを完了すると、次のリソースが設定されます。

- ウェブサイトホスティングおよびリダイレクト用に設定された Amazon S3 バケット (www サブドメインを使用している場合)
- バケットにアップロードされたウェブサイトコンテンツ
- ウェブサイトバケット用に設定されたパブリックアクセス

訪問者は、カスタムドメイン名を使用して静的ウェブサイトにアクセスできます。

> **Note**
>
> 既存のドメインを Route 53 に移管することも可能ですが、その処理は複雑であり、新しいドメインを登録する場合に比べて時間がかかります。詳細については、「ドメイン登録の Amazon Route 53 への移管」を参照してください。

前提条件

開始する前に、以下のステップを完了します。

- 「Amazon Route 53 を設定する」のステップを完了します。
- Amazon Route 53 を使用してドメイン名を登録します。詳細については、「新しいドメインの登録」を参照してください。
- 静的ウェブサイトホスティング用に Amazon Simple Storage Service バケットを設定します。完全な手順については、「Amazon Simple Storage Service ユーザーガイド」の「チュートリアル: Route 53 に登録されたカスタムドメインを使用した静的ウェブサイトの設定」を参照してください。

ステップ 1: ドメインの DNS トラフィックをウェブサイトバケットにルーティングする

静的ウェブサイトホスティング用に Amazon Simple Storage Service バケットが設定されたので、Amazon Route 53 を使用してドメインの DNS トラフィックをバケットにルーティングします。これにより、訪問者はカスタムドメイン名を使用してウェブサイトにアクセスできます。

トラフィックをウェブサイトにルーティングするには

1. Route 53 コンソール (https://console.aws.amazon.com/route53/) を開きます。
2. ナビゲーションペインで [Hosted zones] を選択します。

   > **Note**
   >
   > ドメインを登録すると、同名のホストゾーンが、Amazon Route 53 によって自動的に作成されます。ホストゾーンには、ドメインのトラフィックを Route 53 がどのようにルーティングするかに関する情報が含まれています。

3. ホストゾーンリストから、ドメインの名前を選択します。
4. [Create record (レコードを作成)] を選択します。
5. 次の値を指定します。

   レコード名

   ルートドメインのレコードを作成するには、空白のままにします。

   レコードタイプ

   A を選択 - トラフィックを IPv4 アドレスと一部の AWS リソースにルーティングします。

   エイリアス

   エイリアスをオンにします。

   トラフィックのルーティング先

   [Alias to S3 website endpoint] (S3 ウェブサイトエンドポイントのエイリアス) を選択します。

   S3 バケットを作成したリージョンを選択します。

S3 バケットを選択します。バケット名はドメインの名前と一致する必要があります。このリストに、バケットが作成されたリージョンの Amazon S3 ウェブサイトエンドポイントとともにバケット名が表示されます (例: `s3-website-us-west-1.amazonaws.com (example.com)`)。

バケットがこのリストに表示されない場合は、バケットが作成されたリージョンの Amazon S3 ウェブサイトエンドポイント (例: **`s3-website-us-west-2.amazonaws.com`**) を入力します。Amazon S3 ウェブサイトエンドポイントの完全なリストについては、「Amazon S3 ウェブサイトエンドポイント」を参照してください。

ターゲットの正常性の評価

デフォルト値の [No] をそのまま使用します。

6. [レコードを作成] を選択します。

(オプション) サブドメイン (**`www.example.com`**) のエイリアスレコードを追加するには

サブドメインのバケットを作成した場合は、そのバケットのエイリアスレコードも追加します。

1. [Create record (レコードを作成)] を選択します。
2. 次の値を指定します。

レコード名

`www` と入力します。

レコードタイプ

A を選択 - トラフィックを IPv4 アドレスと一部の AWS リソースにルーティングします。

エイリアス

エイリアスをオンにします。

トラフィックのルーティング先

[Alias to S3 website endpoint] (S3 ウェブサイトエンドポイントのエイリアス) を選択します。

S3 バケットを作成したリージョンを選択します。

サブドメインの S3 バケットを選択します (例: s3-website-us-west-2.amazonaws.com (www.example.com))。

ターゲットの正常性の評価

デフォルト値の [No] をそのまま使用します。

3. [レコードを作成] を選択します。

ステップ 2: ウェブサイトをテストする

ウェブサイトが正常に動作していることを確認するには、ウェブブラウザを開いて以下の URL を入力します。

- http://######## (example.com など) に、########のバケットにある、インデックスドキュメントが表示されます
- http://www.######## (www.example.com など) – リクエストが########のバケットにリダイレクトされます

状況によっては、期待される動作を実現するために、キャッシュの消去が必要になる場合があります。

インターネットトラフィックのルーティングの詳細については、「DNS サービスとしての Amazon Route 53 の設定」を参照してください。インターネットトラフィックを AWS リソースにルーティングする方法については、「」を参照してくださいAWS リソースへのインターネットトラフィックのルーティング。

> **Note**
>
> Amazon S3 は、ウェブサイトへの HTTPS アクセスをサポートしていません。HTTPS を使用する場合は、Amazon CloudFront を使用して Amazon S3 でホストされている静的ウェブサイトを提供できます。詳細については、「Amazon CloudFront ディストリビューションを使用して静的なウェブサイトを提供する」を参照してください。

Amazon CloudFront ディストリビューションを使用して静的なウェブサイトを提供する

このトピックでは、ドメインの DNS トラフィックを、静的ウェブサイトを提供する Amazon CloudFront ディストリビューションにルーティングする方法について説明します。ドメインとサブドメインを CloudFront ディストリビューションにポイントするエイリアスレコードを作成します。

このトピックは、静的ウェブサイトのセットアップワークフローの一部です。CloudFront ディストリビューションへのトラフィックのルーティングに関する一般的な情報については、「」を参照してくださいドメイン名を使用したトラフィックの Amazon CloudFront ディストリビューションへのルーティング。

これらのステップを完了すると、次のリソースが設定されます。

- のドメインの SSL/TLS 証明書 AWS Certificate Manager
- ウェブサイトホスティングおよびリダイレクト用に設定された Amazon S3 バケット
- ルートドメインとサブドメインの両方の CloudFront ディストリビューション

その後、訪問者は CloudFront から HTTPS セキュリティを使用してカスタムドメイン名のウェブサイトにアクセスできます。

前提条件

開始する前に、以下のステップを完了します。

- 「Amazon Route 53 を設定する」のステップを完了します。
- Amazon Route 53 を使用してドメイン名を登録します。詳細については、「新しいドメインの登録」を参照してください。
- Amazon CloudFront と Amazon Simple Storage Service を使用して、安全な静的ウェブサイトを作成します。手順については、Amazon CloudFront デベロッパーガイド」の「安全な静的ウェブサイトの開始方法」を参照してください。

ステップ 1: ドメインの DNS トラフィックを CloudFront ディストリビューションにルーティングする

ウェブサイトの Amazon CloudFront ディストリビューションを作成したので、ドメインの DNS トラフィックをそれらのディストリビューションにルーティングします。これにより、訪問者はカスタムドメイン名でウェブサイトにアクセスできます。

CloudFront ディストリビューションへのトラフィックのルーティングの詳細については、「ドメイン名を使用したトラフィックの Amazon CloudFront ディストリビューションへのルーティング」を参照してください。

トラフィックをウェブサイトにルーティングするには

1. Route 53 コンソール (https://console.aws.amazon.com/route53/) を開きます。
2. ナビゲーションペインで [Hosted zones] を選択します。

   > **Note**
   >
   > ドメインを登録すると、Amazon Route 53 は同じ名前のホストゾーンを作成しました。このホストゾーンには、Route 53 がドメインのトラフィックをルーティングする方法に関する情報が保存されます。

3. ホストゾーンリストから、ドメインの名前を選択します。
4. [Create record (レコードを作成)] を選択します。
5. 次の値を指定します。

   レコード名

   サブドメインレコードには、「`www`」と入力します。

   レコードタイプ

   A を選択 - トラフィックを IPv4 アドレスと一部の AWS リソースにルーティングします。

   エイリアス

   エイリアスをオンにします。

トラフィックのルーティング先

[Alias to CloudFront distribution] (CloudFront ディストリビューションへのエイリアス) を選択します。

[us-east-1 Region] (us-east-1 リージョン) を選択します。

CloudFront ディストリビューションを選択します。ディストリビューション名は、CloudFront コンソールのドメイン名列の値と一致します (例: `d111111abcdef8.cloudfront.net`)。

ターゲットの正常性の評価

デフォルト値の [No] をそのまま使用します。

6. [レコードを作成] を選択します。

ルートドメインのエイリアスレコードを追加するには (**`example.com`**)

ルートドメインのエイリアスレコードも追加します。トラフィックを にリダイレクトする CloudFront ディストリビューションにポイントします`www.example.com`。

1. [Create record (レコードを作成)] を選択します。
2. 次の値を指定します。

レコード名

ルートドメインのレコードを作成するには、空白のままにします。

レコードタイプ

A を選択 - トラフィックを IPv4 アドレスと一部の AWS リソースにルーティングします。

エイリアス

エイリアスをオンにします。

トラフィックのルーティング先

[Alias to CloudFront distribution] (CloudFront ディストリビューションへのエイリアス) を選択します。

[us-east-1 Region] (us-east-1 リージョン) を選択します。

ルートドメイン CloudFront ディストリビューションを選択します。

ターゲットの正常性の評価

デフォルト値の [No] をそのまま使用します。

3. [レコードを作成] を選択します。

ステップ 2: ウェブサイトをテストする

ウェブサイトが機能していることを確認するには、ウェブブラウザを開き、次の URLsに移動します。

- https://www. ##### (www.example.com など) – *www. #####* のバケットにあるインデックスドキュメントが表示されます
- https:// ##### (example.com など) – リクエストが *www.#####* のバケットにリダイレクトされます

状況によっては、期待される動作を実現するために、キャッシュの消去が必要になる場合があります。

インターネットトラフィックのルーティングの詳細については、「」を参照してくださいDNS サービスとしての Amazon Route 53 の設定。 AWS リソースにトラフィックをルーティングするには、「」を参照してくださいAWS リソースへのインターネットトラフィックのルーティング。

の他のサービスとの統合

Amazon Route 53 を他の AWS サービスと統合して、Route 53 API に送信されたリクエストのログ記録、リソースのステータスのモニタリング、リソースへのタグの割り当てを行うことができます。Route 53 を使用して、インターネットトラフィックを AWS リソースにルーティングすることもできます。

トピック

- ログ記録、モニタリング、タグ付け
- 他の AWS リソースへのトラフィックのルーティング

ログ記録、モニタリング、タグ付け

AWS CloudTrail

Amazon Route 53 は AWS CloudTrail、 AWS アカウントによって Route 53 API に送信されたすべてのリクエストに関する情報をキャプチャするサービスである と統合されています。CloudTrail ログファイルを使用して、Route 53 に対してどのようなリクエストが行われたか、送信元 IP アドレス、リクエスト者、およびリクエスト日時を確認できます。

詳細については、「を使用した Amazon Route 53 API コールのログ記録 AWS CloudTrail」を参照してください。

Amazon CloudWatch

Amazon CloudWatch を使用して、Route 53 ヘルスチェックの状態 (正常または異常) を監視できます。ヘルスチェックでは、ウェブアプリケーション、ウェブサーバー、その他のリソースの正常性とパフォーマンスがモニタリングされます。指定した一定の間隔で、Route 53 はインターネット経由でリソースにリクエストを送信し、アクセス可能で機能していることを確認します。

詳細については、「CloudWatch を使用したヘルスチェックのモニタリング」を参照してください。

タグエディター

タグは、Route 53 ドメイン、ホストゾーン、ヘルスチェックなど、 AWS リソースに割り当てるラベルです。タグはそれぞれ、1 つのキーと 1 つの値で構成されており、どちらもユーザーが定義します。例えば、キーが "Customer" で値が "Example Corp" であるドメイン登録にタグを割り

当てることができます。タグには多くの目的があります。一般的な用途の 1 つは、 AWS コストを分類して追跡することです。

詳細については、「Amazon Route 53 リソースのタグ付け」を参照してください。

他の AWS リソースへのトラフィックのルーティング

Amazon Route 53 を使用して、さまざまな AWS リソースにトラフィックをルーティングできます。

Amazon API Gateway

Amazon API Gateway を使用すると、いずれの規模でも API を作成、発行、保守、モニタリング、保護できます。または他のウェブサービス、および AWS クラウドに保存されているデータにアクセスする AWS APIs を作成できます。

Route 53 を使用してトラフィックを API Gateway API にルーティングします。詳細については、「ドメイン名を使用してトラフィックを Amazon API Gateway の API にルーティングする」を参照してください。

Amazon CloudFront

ウェブコンテンツの配信を高速化するには、 AWS コンテンツ配信ネットワーク (CDN) である Amazon CloudFront を使用できます。CloudFront は、エッジロケーションのグローバルネットワークを使用して、動的、静的、ストリーミング、インタラクティブなコンテンツを含む、ウェブサイト全体を配信できます。ユーザーから見て最もレイテンシーが小さいエッジロケーションに、CloudFront が自動的にコンテンツのリクエストをルーティングします。Route 53 を使用して、ドメインのトラフィックを CloudFront ディストリビューションにルーティングできます。詳細については、「ドメイン名を使用したトラフィックの Amazon CloudFront ディストリビューションへのルーティング」を参照してください。

Amazon EC2

Amazon EC2 は、 AWS クラウドでスケーラブルなコンピューティング容量を提供します。事前設定されたテンプレート (Amazon マシンイメージ、または AMI) を使用して EC2 インスタンスを起動できます。AMI には、オペレーティングシステム (Linux または Microsoft Windows) と、ウェブサーバーやデータベースなどのソフトウェアが含まれます。

ウェブサイトをホストしたりEC2 インスタンスでウェブアプリケーションを実行したりすると、Route 53 を使用してドメインのトラフィックをサーバーにルーティングできます。詳細については、「Amazon EC2 インスタンスへのトラフィックのルーティング」を参照してください。

AWS Elastic Beanstalk

AWS Elastic Beanstalk を使用して AWS クラウドにアプリケーションをデプロイおよび管理する場合、Route 53 を使用してドメインの DNS トラフィックを Elastic Beanstalk 環境にルーティングできます。詳細については、「AWS Elastic Beanstalk 環境へのトラフィックのルーティング」を参照してください。

Elastic Load Balancing

複数の Amazon EC2 インスタンスでウェブサイトをホストする場合、Elastic Load Balancing (ELB) ロードバランサーを使用してインスタンス間でトラフィックを分散できます。ELB は、ウェブサイトへのトラフィックが時間の経過とともに変化するにつれてロードバランサーをスケーリングします。また、ロードバランサーは登録されたインスタンスの状態を監視し、トラフィックを正常なインスタンスにのみルーティングします。

Route 53 を使用して、ドメインのトラフィックを Classic、Application、または Network Load Balancer にルーティングできます。詳細については、「ELB ロードバランサーへのトラフィックのルーティング」を参照してください。

Amazon Lightsail

Amazon Lightsail は、ウェブサイト、ウェブアプリケーション、データベースをクラウドにデプロイおよび管理するためのコンピューティング、ストレージ、ネットワーキングを月額料金で提供します。

を使用する場合はLightsail、Route 53 を使用してトラフィックをインスタンスにルーティングできます。詳細については、「Route 53 を使用してドメインを Amazon Lightsail インスタンスへポイント」を参照してください。

Amazon S3

Amazon Simple Storage Service (Amazon S3) では、安全で耐久性があり、拡張性の高いクラウドストレージを提供します。ウェブページとクライアント側スクリプトを配置できる静的ウェブサイトをホストするよう S3 バケットを設定できます (S3 ではサーバー側スクリプトがサポートされていません)。Route 53 を使用して、Amazon S3 バケットにトラフィックをルーティングできます。詳細については、以下のトピックを参照してください。

- トラフィックをバケットにルーティングすることの詳細については、「Amazon S3 バケットでホストされているウェブサイトへのトラフィックのルーティング」を参照してください。
- S3 バケットで静的ウェブサイトをホストする方法の詳細については、「Amazon Route 53 の開始方法」を参照してください。

Amazon Virtual Private Cloud (Amazon VPC)

インターフェイスエンドポイントを使用すると、 AWS PrivateLink を使用するサービスに接続できます。これらのサービスには、一部の AWS サービス、他の AWS 顧客やパートナーが独自の VPCs でホストするサービス (エンドポイントサービスと呼ばれる) 、サポートされている AWS Marketplace パートナーサービスが含まれます。

Route 53 を使用して、トラフィックをインターフェイスエンドポイントにルーティングできます。詳細については、「ドメイン名を使用してトラフィックを Amazon Virtual Private Cloud インターフェイスエンドポイントにルーティングする」を参照してください。

Amazon WorkMail

ビジネス E メールに Amazon WorkMail を使用し、DNS サービスとして Route 53 を使用する場合は、Route 53 を使用して Amazon WorkMail E メールドメインにトラフィックをルーティングできます。詳細については、「Amazon WorkMail へのトラフィックのルーティング」を参照してください。

詳細については「AWS リソースへのインターネットトラフィックのルーティング」をご参照ください。

DNS ドメイン名の形式

ドメイン名 (ドメイン、ホストゾーン、レコードの名前を含みます) は、ドットで区切られた一連のラベルから構成されます。各ラベルは、63 バイトまでの長さにすることができます。ドメイン名の全体の長さは、ドットを含めて 255 バイト以内にする必要があります。Amazon Route 53 では、有効なドメイン名がすべてサポートされています。

命名要件は、ドメイン名を登録するのか、それとも、ホストゾーンまたはレコードの名前を指定するのかによって異なります。該当するトピックを参照してください。

ドメイン名登録用のドメイン名の形式

ドメイン名登録の場合、ドメイン名に使用できる文字は、a ~ z、0 ~ 9、– (ハイフン) のみです。ラベルの先頭または末尾にハイフンを指定することはできません。

国際化ドメイン名 (IDN) の登録方法については、「国際化ドメイン名の形式」を参照してください。

ホストゾーンとレコード用のドメイン名の形式

ホストゾーンおよびレコードの場合、ドメイン名には、次の印刷可能な任意の ASCII 文字を使用することができます (スペースを除く)。

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

大文字または小文字を指定するか、あるいはエスケープコードで対応する文字を指定するかどうかに関係なく、Amazon Route 53 は英字を小文字 (a ~ z) として格納します。

ドメイン名が以下の文字を含む場合は、エスケープコードを使って、*\3 ## 8 ####*という形式で文字を指定する必要があります。

- 8 進数で文字 000 ~ 040 (10 進数で 0 ~ 32、16 進数で 0x20 ~ 0x00)
- 8 進数で文字 177 ~ 377 (10 進数で 127 ~ 255、16 進数で 0xFF ~ 0x7F)

- . (ピリオド)。8 進数では文字 056 になります (10 進数で 46、16 進数で 0x2E)。ピリオドを区切り記号ではなく、ドメイン名の文字として使用する場合です。. をラベルの間の区切り記号として使用する場合は、エスケープコードを使用する必要はありません。

ドメイン名に、a ~ z、0 ~ 9、ハイフン (-)、アンダースコア (_) 以外の文字が含まれている場合、Route 53 API アクションはその文字をエスケープコードとして返します。これは、エンティティの作成時に文字を文字として指定した場合も、エスケープコードとして指定した場合も同様です。Route 53 コンソールでは、文字はエスケープコードとしてでなく文字として表示されます。

ASCII 文字および対応する 8 進コードのリストについては、インターネットで「ascii テーブル」を検索してください。

国際化ドメイン名 (IDN) を指定するには、名前を Punycode に変換します。詳細については、「国際化ドメイン名の形式」を参照してください。

ホストゾーンおよびレコード名のアスタリスク (*) を使用する

「*」を名前に含むホストゾーンおよびレコードを作成できます。

ホストゾーン

- 「*」をドメイン名の左端のラベルに含めることはできません。例えば、*.example.com はできません。
- 「*」を他の位置に含める場合、DNS はこれをワイルドカードとしてではなく、アスタリスク文字 (ASCII 42) として扱います。

レコード

DNSは、名前の中の位置に応じて、「*」をワイルドカードまたはアスタリスク (ASCII 42) として処理します。「*」をレコードの名前でワイルドカードとして使用する際は、以下の制約にご注意ください。

- 「*」はドメイン名の左側、*.example.com、または *.acme.example.com のように配置する必要があります。prod.*.example.com のように「*」を他のどのような位置に含めても、DNS はこれをワイルドカードとしてではなく、アスタリスク文字 (ASCII 42) として扱います。
- * は、ラベル全体を置き換える必要があります。例えば、*prod.example.com や prod*.example.com と指定することはできません。

- 特定のドメイン名が優先されます。例えば、*.example.com と acme.example.com のレコードを作成すると、Route 53 は常に acme.example.com レコードの値で acme.example.com の DNS クエリに応答します。
- 「*」は、アスタリスクが含まれたサブドメインレベル、およびそのサブドメインのすべてのサブドメインの DNS クエリに適用されます。例えば、*.example.com という名前のレコードを作成すると、Route 53 では (該当する名前を持つレコードがない場合には) そのレコードの値を使用して zenith.example.com、acme.zenith.example.com、および pinnacle.acme.zenith.example.com の DNS クエリに応答します。

  *.example.com という名前のレコードを作成し、example.com レコードがない場合、Route 53 は NXDOMAIN により(存在しないドメインとして) example.com の DNS クエリに応答します。

  > **Note**
  >
  > AWS Certificate Manager で Route 53 を使用している場合、ACM ワイルドカード証明書は 1 つのサブドメインレベルのみを保護することに注意してください。例えば、*.example.com の ACM 証明書は login.example.com と test.example.com を保護しますが、test.login.example.com は保護しません。詳細については、「AWS Certificate Manager 証明書の特性と制限」を参照してください。

- 同じレベルのすべてのサブドメインとドメイン名の両方の DNS クエリに対して、Route 53 が同じレスポンスを返すように設定できます。例えば、Route 53 が example.com レコードを使用して、acme.example.com や zenith.example.com などの DNS クエリに応答するように設定できます。以下のステップを実行します。

  1. ドメインのレコードを作成します (example.com など)。
  2. サブドメインのエイリアスレコードを作成します (*.example.com など)。ステップ 1 で作成したレコードの名前を、エイリアスレコードのターゲットとして指定します。
- NS タイプのあるレコードで「*」をワイルドカードとして使用することはできません。

国際化ドメイン名の形式

新しいドメイン名の登録時、あるいは、ホストゾーンとレコードの作成時には、a ~ z 以外の文字 (フランス語の ç など)、他のアルファベット文字 (キリル文字やアラビア文字など)、 および中国語、日本語、韓国語の文字を指定できます。Amazon Route 53 では、これらの国際化ドメイン名 (IDN) を、Unicode 文字を ASCII 文字列として表現する Punycode で格納します。

ドメイン名を登録する場合は、次の点に注意してください。

- トップレベルドメイン (TLD) が IDN をサポートし、使用する言語をサポートしている場合にのみ、a ~ z、0 ~ 9、- (ハイフン) 以外の文字を使用できます。TLD がサポートしている言語を確認するには、「Amazon Route 53 に登録できる最上位ドメイン」を参照してください。
- 名前に a ~ z の文字しか含まれていない場合は、サポートされていない言語で名前を指定できます。例えば、TLD がフランス語をサポートしていないのに、使用する名前に発音区別符号のない文字 a ~ z のみが含まれている場合でも、その名前を使用できます。この例では、「c」を含む名前を使用できます。「ç」を含む名前は使用できません。
- TLD が IDN をサポートしていない場合や、ドメイン名に使用する言語をサポートしていない場合、Punycode に a ~ z、0 ~ 9、- のみが含まれていても、Punycode で名前を指定することはできません。

以下の例は、国際化ドメイン名「中国.asia」の Punycode 表現を示しています:

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

現代的なブラウザのアドレスバーに IDN を入力すると、ブラウザはそれを Punycode に変換した後、DNS クエリを送信するか、HTTP リクエストを実行します。

IDN の入力方法は、作成対象 (ドメイン名、ホストゾーン、レコード) とその作成方法 (API、SDK、Route 53 コンソール) によって変わります。

- Route 53 API またはいずれかの AWS SDK を使用する場合は、プログラム的に Unicode 値から Punycode への変換が可能です。例えば、Java を使用する場合は、java.net.IDN ライブラリの toASCII メソッドを使って Unicode 値を Punycode に変換できます。
- Route 53 コンソールを使ってドメイン名を登録する場合は、(Unicode 文字も含めて) 名前を名前フィールドに貼り付けることができ、この値は保存される前にコンソールにより Punycode に変換されます。
- Route 53 コンソールを使ってホストゾーンまたはレコードを作成する場合は、ドメイン名を Punycode に変換した上で、名前を該当する [Name (名前)] フィールドに入力する必要があります。オンラインコンバーターについては、インターネットで「punycode コンバーター」を検索してください。

ドメイン名を登録する場合は、すべての最上位ドメイン (TLD) で IDN がサポートされているわけではないことに注意してください。Route 53 でサポートされる TLD の一覧については、「Amazon

Route 53 に登録できる最上位ドメイン」を参照してください。IDN をサポートしない TLD が注記されています。

Amazon Route 53 を使用したドメインの登録と管理

新しいドメイン名 (URL が http://example.com であれば、example.com という部分) を取得する場合は、ドメイン名を Amazon Route 53 に登録することができます。また、既存のドメインの登録を他のレジストラから Route 53 に移管することも、逆に、Route 53 に登録したドメインの登録を別のレジストラに移管することもできます。

この章の手順では、Route 53 コンソールを使用してドメインを登録し移管する方法、および、ドメイン設定の編集方法とドメインステータスの表示方法を説明します。登録し管理するドメインの数が少ない場合は、コンソールを使用するのが最も簡単な方法です。

多数のドメインを登録して管理する必要がある場合は、プログラムで変更したほうが好ましい場合があります。詳細については、「Amazon Route 53 を設定する」を参照してください。

> **Note**
>
> AWS SDK が存在する言語を使用している場合は、APIs を使用して作業するのではなく、SDK を使用します。SDK を利用すると、認証が簡素化され、開発環境との統合が容易になり、Route 53 コマンドに簡単にアクセスすることができます。

ドメイン名登録サービスは、ドメイン名登録の利用規約に基づいて提供されます。

トピック

- 新しいドメインの登録
- ドメインの設定の更新
- ドメインの登録の更新
- 失効した、または削除されたドメインの復元
- Route 53 に登録されているドメインのホストゾーンの置き換え
- ドメインの移管
- 承認および確認メールの再送信
- ドメインの DNSSEC の設定
- レジストラとドメインに関するその他の情報の検索
- ドメイン名登録の削除
- ドメイン登録の問題に関する AWS サポートへのお問い合わせ

- ドメイン請求レポートのダウンロード
- Amazon Route 53 に登録できる最上位ドメイン

新しいドメインの登録

このセクションでは、Amazon Route 53 への新しいドメインの登録に関連する以下のトピックについて説明します。

1. 新しいドメインの登録:
   - Route 53 コンソールを使用して新しいドメインを登録するステップバイステップの手順について説明します。
   - 問題、料金、サポートされている最上位ドメイン (TLDs)、ホストゾーンの自動作成について AWS サポートに問い合わせるなど、ドメイン登録に関する考慮事項と前提条件を理解します。
2. ドメインを登録または移管するときに指定する値:
   - 連絡先情報、プライバシー保護設定、自動更新オプションなど、ドメインの登録または転送時に指定する必要がある値について説明します。
   - ドメイン所有者や登録者の E メールアドレスなど、特定の値を変更した場合の影響を理解します。
3. ドメインの登録時に Amazon Route 53 が返す値:
   - 登録日、有効期限、ドメインステータスコード、転送ロックステータス、ネームサーバーなど、Route 53 がドメイン登録に成功した後に返す値について説明します。
4. ドメイン登録のステータスの表示:
   - ICANN ステータスコードを含むドメイン登録の現在のステータスや、登録者の E メールアドレスの検証などのユーザー側で必要なアクションを表示する方法について説明します。

新しいドメインの登録

新規ドメインを登録する、または既存ドメインのネームサーバーを更新する

Amazon Route 53 は、Route 53 で登録したドメインと、他の DNS プロバイダーで登録したドメインで使用できます。DNS プロバイダーに応じて次のいずれかの手順を選択し、Route 53 で新しいドメインを登録して使用します。

- 新しいドメインの登録については、「Route 53 を使用して新しいドメインを登録するには」を参照してください。

- 既存のドメインについては、「Amazon Route 53 を既存ドメインの DNS サービスとして使用する」をご確認ください。
- ドメインを別のレジストラに移管する方法は、「他の DNS サービスを使用するときにドメインのネームサーバーを更新するには」を参照してください。

ドメイン登録に関する考慮事項

開始する前に、次の点に注意してください。

AWS サポートへのお問い合わせ

ドメインの登録中に問題が発生した場合は、 AWS サポートに無料でお問い合わせください。詳細については、「ドメイン登録の問題に関する AWS サポートへのお問い合わせ」を参照してください。

ドメイン登録の料金

ドメイン登録のコストの詳細については、「Amazon Route 53 のドメイン登録料金」を参照してください。

サポートされるドメイン

サポートされている TLD のリストについては、「Amazon Route 53 に登録できる最上位ドメイン」を参照してください。

登録後にドメイン名を変更することはできません。

正しくないドメイン名を誤って登録した場合、そのドメイン名を変更することはできません。代わりに、別のドメイン名を登録し、正しい名前を指定する必要があります。また、誤って登録したドメイン名の返金を受け取ることはできません。

AWS クレジット

AWS クレジットを使用して、Route 53 に新しいドメインを登録するための料金を支払うことはできません。

特別料金またはプレミアム料金

TLD レジストリでは、一部のドメイン名に対して特別料金またはプレミアム料金を設定しています。Route 53 を使用して、特別料金またはプレミアム料金が設定されたドメインを登録することはできません。

ホストゾーンの料金

Route 53 にドメインを登録すると、Route 53 はドメインのホストゾーンを自動的に作成し、ドメイン登録の年間料金に加えて、ホストゾーンの月額料金が少額になります。このホストゾーンは、ドメインのトラフィックを、例えば Amazon EC2 インスタンスや CloudFront ディストリビューションにルーティングする方法についての情報を保存する場所です。ドメインを今すぐ使用するわけでない場合は、ホストゾーンを削除できます。ドメインの登録から 12 時間以内にホストゾーンを削除した場合、 AWS 請求書にホストゾーンの料金は記載されません。Route 53 は、ドメインに対して受信する DNS クエリに対しても少額の料金を請求します。詳細については、「Amazon Route 53 料金表」を参照してください。

ドメインのホストゾーンの置き換え

ドメイン用の新しいホストゾーンを作成した場合、この新しいホストゾーン用に同じネームサーバーを使用するためには、そのドメイン用にネームサーバーの更新を行う必要があります。詳細については、「Route 53 に登録されているドメインのホストゾーンの置き換え」を参照してください。

同じアカウントのルートユーザー E メールに Route 53 ドメインを使用しないでください。

> **Important**
>
> Route 53 に登録されているドメインを、同じ のルートユーザーの E メールドメインとして使用しないでください AWS アカウント。アカウントが閉鎖または停止された場合、ドメイン登録は 5 日以内に停止されます。ドメインの停止により E メール配信が停止され、ルートユーザーのパスワード復旧が防止されます。E メールアクセスがないと、アカウントを復旧したり、ドメインを復元したりすることはできません。30 日後、ドメインは修復パスなしで完全に削除されます。
>
> この循環依存を回避するには、次のいずれかのアーキテクチャを使用します。
>
> - ルートユーザーの E メールに使用されるドメインを別の専用 AWS アカウント (管理アカウントなど) に登録します。
> - ルートユーザーの外部 AWS でホストされている E メールアドレスを使用します。

詳細については、「Amazon Route 53 ドメイン登録のベストプラクティス」を参照してください。

Route 53 を使用して新しいドメインを登録するには

Route 53 を使用して新しいドメインを登録するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで、[ドメイン] を選択し、[登録済みドメイン] を選択します。
3. [登録済みドメイン] ページで、[ドメインを登録] を選択します。

   a. [ドメインの検索] セクションに登録するドメインの名前を入力し、[検索] を選択してそのドメイン名を使用できるかどうか確認します。

      登録するドメイン名に a-z、A-Z、0-9、および – (ハイフン) 以外の文字が含まれている場合は、次の点に注意してください。

      - 適切な文字を使用して名前を入力できます。名前を Punycode に変換する必要はありません。
      - 言語のリストが表示されます。指定した名前の言語を選択します。例えば、příklad (チェコ語で「例」) と入力した場合は、チェコ語 (CES) またはチェコ語 (CZE) を選択します。

      > **Note**
      >
      > 複数のコードを持つ言語の場合は、両方を試す必要がある場合があります。CES と CZE は同義ですが、どちらか一方しかサポートしていない TLD レジストリもあります。

      a ~ z、0 ~ 9、- (ハイフン) 以外の文字を指定する方法、および国際化されたドメイン名を指定する方法については、「DNS ドメイン名の形式」を参照してください。

      使用できる場合は入力したドメインが表示され、使用できない場合は、候補として似たドメインが表示されます。

      登録するドメインは 5 つまで選択できます。選択したドメインは、[選択済みドメイン] リストに表示されます。

   b. ドメインをさらに登録するときは、3a から 3b のステップを繰り返します。

4. [チェックアウトに進む] を選択します。
5. 料金ページで、ドメインを登録する年数と、有効期限が切れる前に Route 53 でドメイン登録を自動的に更新するかどうかを選択します。

> **Note**
>
> ドメイン名の登録および更新は返金の対象外です。自動ドメイン更新を有効にし、Route 53 が登録を更新した後にドメイン名が不要になった場合、更新のコストの返金を受けることはできません。

[次へ] を選択します。

6. [連絡先情報] ページで、ドメインの登録者、管理者、技術担当者、請求の連絡先を入力します。ここで入力した値は、登録しようとしているすべてのドメインに適用されます。詳細については、「ドメインを登録または移管するときに指定する値」を参照してください。

> **Important**
>
> ドメイン登録中に登録者として登録した連絡先には、ICANN 移転ポリシーに基づき、ドメイン名の登録名保有者としての特定の権利があります。ほとんどのドメインは、 の閉鎖時に削除されます AWS アカウント (詳細については、「」を参照してくださいAWS アカウントが閉鎖または完全に閉鎖され、ドメインが Route 53 に登録されている)。ただし、ドメインが閉鎖されたアカウントに残っている場合、登録者としてリストした連絡先は、外部レジストラへのドメイン名の移管をリクエストできる場合があります。したがって、リストに記載する登録者の連絡先は、自分または責任を持って行動できる別の信頼できる人物であることが重要です。

以下の考慮事項に注意してください。

First Name (名) と Last Name (姓)

[First Name] と [Last Name] は、公式 ID に名前を指定することをお勧めします。ドメイン設定の変更に際しては、一部のドメインレジストリで、身分証明書の提供が求められる場合があります。お客様の ID の名前は、ドメイン登録者の連絡先の名前と完全に一致する必要があります。

他の連絡先

デフォルトでは、Route 53 は 3 つの連絡先すべてに同じ情報を使用します。1 つまたは複数の連絡先で異なる情報を入力するときは、それぞれの連絡先について [登録者の連絡先と同じ] の値をオフの位置にします。

> **Note**
>
> .it ドメインの場合、登録者と管理者の連絡先は同じである必要があります。

> **Note**
>
> .jp ドメインの場合、登録者と管理者の連絡先は同じである必要があります。

複数のドメイン

複数のドメインを登録する場合、Route 53 はすべてのドメインに同じ連絡先情報を使用します。

その他の必須情報

一部の最上位ドメイン (TLDs) では、追加情報が必要です。そのような TLD の場合は、[Postal/Zip Code] の後に、該当する値を入力します。

プライバシー保護

WHOIS クエリに対して連絡先情報を非表示にするかどうかを選択します。

> **Note**
>
> 管理担当者、登録者、技術担当者、および請求の連絡先に同じプライバシー設定を指定する必要があります。

詳細については、以下の各トピックを参照してください。

- ドメインの連絡先情報のプライバシー保護の有効化/無効化
- Amazon Route 53 に登録できる最上位ドメイン

> **Note**
>
> .uk、.co.uk、.me.uk、.org.uk ドメインのプライバシー保護を有効にするには、サポートケースを開いてプライバシー保護をリクエストします。

[次へ] を選択します。

7. [確認] ページで入力した情報を確認し、必要があれば修正し、サービスの利用規約を読み、読んだことを確認するチェックボックスにチェックを入れます。

   [Submit] を選択してください。

8. ナビゲーションペインで [ドメイン] を選択し、次に [リクエスト] を選択します。

   このページではドメインのステータスが確認できます。また、登録者の連絡先確認メールに、返信する必要があるかどうかも確認できます。確認メールは再送信することも可能です。

   Route 53 でのドメインの登録に使用されたことがない登録者の連絡先の E メールアドレスを指定した場合、一部の TLD レジストリでは、アドレスが有効であることを確認する必要があります。

   Route 53 は、次のいずれかの E メールアドレスから検証 E メールを送信します。

   - noreply@registrar.amazon – Amazon Registrar によって登録された TLDs 用。
   - noreply@domainnameverification.net または noreply@emailverification.info – 当社のレジストラアソシエイトである Gandi によって登録された TLDs の場合。TLD のレジストラを調べる方法については、「レジストラの検索」を参照してください。

> **Important**
>
> 登録者の連絡先は、E メールの指示に従って E メールが受信されたことを確認するか、Route 53 が ICANN の要求に従ってドメインを停止する必要があります。ドメインが停止されると、インターネットでそのドメインにアクセスできなくなります。

> **Note**
>
> 検証 E メールには、www.registrar.amazon へのリンクが含まれている場合があります。これらのリンクは安全に使用できます。
> 一部の TLDs、検証 E メールの件名または本文にドメイン名が含まれていない場合があります。

a. 確認 E メールを受け取ったら、E メール内のリンクを選択し、指定した E メールアドレスが有効であることを確認します。E メールがすぐに届かない場合は、迷惑メールフォルダーを確認します。

b. [リクエスト] ページに戻ります。ステータスが自動的に [E メールアドレスが検証されました] に更新されない場合は、ブラウザでページを更新します。

9. ドメインの登録が完了したら、ドメインの DNS サービスとして Route 53 を使用するか他の DNS サービスを使用するかによって、次のステップは異なります。

- Route 53: ドメイン登録時に Route 53 が作成したホストゾーンで、ドメインおよびサブドメインへのトラフィックをどのようにルーティングするかを Route 53 に指示するためのレコードを作成します。

  例えば、誰かがブラウザにドメイン名を入力し、そのクエリが Route 53 に転送されたときに、Route 53 がそのクエリに対してお客様のデータセンターのウェブサーバーの IP アドレスを返すか、それとも ELB ロードバランサーの名前を返すかを指定します。

  詳細については、「レコードを使用する」を参照してください

  > **Important**
  >
  > Route 53 が自動的に作成するもの以外のホストゾーンでレコードを作成した場合、ドメインのネームサーバーを更新して新しいホストゾーンのネームサーバーを使用する必要があります。

- 他の DNS サービス - 他の DNS サービスに DNS クエリをルーティングするように新しいドメインを設定します。ネームサーバーを更新して別のレジストラを使用するの手順を実行します。

ドメインを登録または移管するときに指定する値

> **Note**
>
> Route 53 はドメインコンソールを更新しました。旧コンソールは移行期間中も引き続きご使用いただけます。新コンソールも使用可能です。Route 53 から返される情報の大半は、両方のコンソールで同じです。情報が異なる場合を以下に記します。

Amazon Route 53 にドメインを登録するかドメイン登録を移管するときは、このトピックで説明されている値を指定します。

> **Note**
>
> 複数のドメインを登録する場合、Route 53 はショッピングカートにあるすべてのドメインについて指定された値を使用します。

Route 53 に現在登録されているドメインの値を変更することもできます。次の点に注意してください。

- ドメインの連絡先情報を変更すると、Route 53 は登録者の連絡先に変更に関する E メール通知を送信します。この E メールは noreply@registrar.amazon から送信されます。ほとんどの変更について、登録者は応答する必要はありません。
- 所有権の変更を構成する連絡先情報の変更については、Route 53 は登録者の連絡先に追加の E メールを送信します。ICANN の規則は、登録者の連絡先に、メールを受領したことを確認するよう要求しています。詳細については、このセクションの [First Name]、[Last Name] および [Organization] の項目を参照してください。

既存のドメインの設定の変更については、「ドメインの設定の更新」を参照してください。

指定する値

- 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

登録者の連絡先と同じ

ドメインの登録者、管理者、技術担当者の連絡先として同じ連絡先情報を使用するかどうかを指定します。

連絡先のタイプ

この連絡先のカテゴリ。次の点に注意してください。

- [Person] 以外のオプションを選択した場合、組織名を入力する必要があります。
- 一部の TLD の場合、使用可能なプライバシー保護は、[連絡先のタイプ] に選択した値によって異なります。TLD のプライバシー保護設定については、「Amazon Route 53 に登録できる最上位ドメイン」を参照してください。
- .es ドメインの場合、3 つの連絡先すべてで [Contact Type (連絡先のタイプ)] の値が [Person (個人)] である必要があります。

名と姓

連絡先の姓名。

> **Important**
>
> [First Name] と [Last Name] は、公式 ID に名前を指定することをお勧めします。ドメイン設定を変更するには、ID の証明を提示する必要があります。ID の名前は、ドメインの登録者連絡先の名前と一致する必要があります。

ドメインを Route 53 に移管する際に次の条件に該当する場合は、ドメインの所有者を変更することになります。

- 連絡先のタイプが [Person (個人)] である。
- 登録者の連絡先の [First Name (名)] および [Last Name (姓)] フィールドを現在の設定から変更する。

この場合、ICANN では、承認を得るために Route 53 が登録者の連絡先に E メールを送信する必要があります。Route 53 は、次のいずれかの E メールアドレスから E メールを送信します。

TLD	承認メールの発信元となるメールアドレス
Amazon Registrar によって登録された TLD	noreply@registrar.amazon
.fr	nic@nic.fr (E メールは現在の登録者の連絡先と新しい登録者の連絡先の両方に送信されます。)
その他すべて	noreply@domainnameverification.net または noreply@emailverification.info

TLD のレジストラを調べる方法については、「Amazon Route 53 に登録できる最上位ドメイン」を参照してください。

> **Important**
>
> 登録者の連絡先は、E メールの指示に従って E メールが受信されたことを確認するか、Route 53 が ICANN の要求に従ってドメインを停止する必要があります。ドメインが停止されると、インターネットでそのドメインにアクセスできなくなります。

登録者の連絡先メールアドレスを変更した場合、通知メールは登録者の連絡先として指定された以前のメールアドレスと新しいメールアドレスの両方に送信されます。

一部の TLD レジストラでは、ドメイン所有者の変更は有料です。これらの値の 1 つを変更すると、有料かどうかを知らせるメッセージが Route 53 コンソールに表示されます。

組織

連絡先と関連付けられている組織 (存在する場合)。登録者と管理者の連絡先の場合、これは通常、ドメインを登録する組織です。技術担当者の連絡先の場合、これはドメインを管理する組織のこともあります。

連絡先のタイプが [Person] 以外のときに、登録者の連絡先の [Organization] フィールドを変更すると、ドメインの所有者が変更されます。ICANN では、Route 53 が承認を得るために登録者の連絡先に E メールを送信する必要があります。Route 53 は、次のいずれかの E メールアドレスから E メールを送信します。

TLD	承認メールの発信元となるメールアドレス
Amazon Registrar によって登録された TLD	noreply@registrar.amazon
.fr	nic@nic.fr (E メールは現在の登録者の連絡先と新しい登録者の連絡先の両方に送信されます。)
その他すべて	noreply@domainnameverification.net または noreply@emailverification.info

TLD のレジストラを調べる方法については、「Amazon Route 53 に登録できる最上位ドメイン」を参照してください。

登録者の連絡先メールアドレスを変更した場合、通知メールは登録者の連絡先として指定された以前のメールアドレスと新しいメールアドレスの両方に送信されます。

一部の TLD レジストラでは、ドメイン所有者の変更は有料です。[Organization] の値を変更すると、有料かどうかを知らせるメッセージが Route 53 コンソールに表示されます。

メール

連絡先のメールアドレス。

登録者の連絡先の E メールアドレスを変更すると、Route 53 は以前の E メールアドレスと新しい E メールアドレスに通知 E メールを送信します。この E メールは noreply@registrar.amazon から送信されます。

電話

連絡先の電話番号です。

- 米国またはカナダの電話番号を入力する場合は、最初のフィールドに「1」と入力し、2 番目のフィールドに 10 桁の市外局番と電話番号を入力します。
- そのほかの場所の電話番号を入力する場合は、最初のフィールドに国コードを入力し、2 番目のフィールドに電話番号の残りを入力します。電話の国コードのリストについては、Wikipedia の記事「国際電話番号の一覧」を参照してください。

Address1

連絡先の住所。

Address2

連絡先の追加の住所情報 (アパートの部屋番号や私書箱など)。

国

連絡先の国。

都道府県

連絡先の都道府県。

市町村

連絡先の市町村。

郵便番号

連絡先の郵便番号。

選択した最上位ドメインのフィールド

以下のトップレベルドメイン (TLD) では、追加の値を指定する必要があります。

- .com.au と .net.au
- .ca
- .es
- .fi
- .fr
- .it
- .ru

- .se
- .sg
- .co.uk、.me.uk、.org.uk、.uk

また、多くの TLD では VAT 識別番号が必要です。

有効な値の詳細については、Amazon Route 53 API リファレンスの「ExtraParam」を参照してください。

プライバシー保護

WHOIS クエリに対して連絡先情報を隠すかどうかを指定します。[プライバシー保護をオンにする] (新しいコンソール)、または [連絡先情報を隠す] を選択すると、WHOIS ("who is") クエリにより、レジストラの連絡先情報、または "Protected by policy" という値が返されます。

> **Note**
>
> 管理担当者、登録者、技術担当者、および請求の連絡先に同じプライバシー設定を指定する必要があります。

[Don't hide contact information] を選択した場合、指定したメールアドレスに送られてくるスパムメールの数が増えます。

だれでもドメインの WHOIS クエリを送信して、そのドメインのすべての連絡先情報を取得することができます。WHOIS コマンドは多くのオペレーティングシステムで利用でき、多くのウェブサイトでウェブアプリケーションとしても利用できます。

> **Important**
>
> ドメインに関連付けられた連絡先情報を必要とする正当なユーザーもいますが、最も一般的なユーザーは、迷惑メールや詐欺メールをドメインの連絡先に送りつけるスパム業者です。一般に、[Privacy Protection] では [Hide contact information] を選択することをお勧めします。

一部のドメインのプライバシー保護を有効または無効にするには、サポートケースを開いてプライバシー保護をリクエストする必要があります。

プライバシー保護の詳細については、以下のトピックを参照してください。

- ドメインの連絡先情報のプライバシー保護の有効化/無効化
- Amazon Route 53 に登録できる最上位ドメイン

自動更新 (ドメイン設定の編集時のみ利用可能)

有効期限切れになる前に Route 53 が自動的にドメイン登録を更新するかどうかを指定します。登録料金は AWS アカウントに請求されます。古いコンソールでは、この設定はドメイン設定を編集するときのみ使用できます。詳細については、「ドメインの登録の更新」を参照してください。

> **Important**
>
> 自動更新を無効にした場合、有効期限が過ぎるとドメイン登録は更新されず、お客様はそのドメイン名をコントロールできなくなる可能性があります。

ドメイン名を更新できる期間は最上位ドメイン (TLD) によって異なります。ドメインの更新に関する概要については、「ドメインの登録の更新」を参照してください。ドメイン登録を指定された年数延長する方法については、「ドメインの登録期間の延長」を参照してください。

ドメインの登録時に Amazon Route 53 が返す値

Amazon Route 53 にドメインを登録すると、Route 53 は指定した値に加えて、次の値を返します。

[Registered on]

ドメインが最初に Route 53 に登録された日付。

[Expires on]

現在の登録期間が失効する日時 (GMT = グリニッジ標準時)。

登録期間は通常 1 年間ですが、一部の最上位ドメイン (TLD) のレジストリでは登録期間が長い場合があります。TLD の登録および更新期間については、「Amazon Route 53 に登録できる最上位ドメイン」を参照してください。

ほとんどの TLD では、最大 10 年登録期間を延長できます。詳細については、「ドメインの登録期間の延長」を参照してください。

[Domain name status code]

ドメインの現在のステータス。

ドメイン名の中央データベースを維持する組織である ICANN は、ドメイン名ステータスコード (別称: EPP ステータスコード) を開発しました。これは、ドメイン名の各種操作のステータスを知らせるコードです。これらのステータスの例としては、ドメイン名の登録、ドメイン名の別のレジストラに対する移管、ドメイン名の登録更新などがあります。すべてのレジストラは、この同じステータスコードを使用します。

ドメイン名ステータスコードと各コードの意味を説明した現在の一覧については、ICANN ウェブサイトで epp status codes を検索してください (ICANN ウェブサイトで直接、検索してください。ウェブ検索ではドキュメントの古いバージョンが返されることがあります)。

[Transfer lock]

他人が許可なく他のレジストラにドメインを移管する可能性を減らすためにドメインをロックするかどうかを指定します。ドメインがロックされていると、[移管のロック] の値は [オン] になります。ドメインがロックされていないと、値は [オフ] になります。

[Auto renew]

有効期限が切れる少し前に Route 53 がこのドメインの登録を自動的に更新するかどうかを指定します。

[Authorization code]

このドメインの登録を他のレジストラに移管する場合に必要なコード。認可コードは、お客様が要求した場合にのみ生成されます。ドメインを別のレジストラに移管する方法については、「Amazon Route 53 から別のレジストラへのドメインの移行」を参照してください。

[Name servers]

このドメインに関する DNS クエリに応答する Route 53 サーバー。Route 53 ネームサーバーは削除しないことをお勧めします。

ネームサーバーを追加、変更、削除する方法については、「ドメインのネームサーバーおよびグルーレコードの追加あるいは変更」を参照してください。

ドメイン登録のステータスの表示

ドメイン名の中央データベースを維持する組織である ICANN は、ドメイン名ステータスコード (EPP ステータスコードとも呼ばれます) を開発しました。これは、ドメイン名の登録、他のレジストラへのドメイン名の移管、ドメイン名の登録の更新など、各種操作のステータスを知らせるコードです。すべてのレジストラは、この同じステータスコードを使用します。

ドメインのステータスコードを表示するには、次の手順を実行します。

ドメインの ICANN ステータスコードを表示するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで、[ドメイン] を展開し、[登録済みドメイン] を選択します。
3. ドメインのリンクされた名前を選択します。
4. 登録者の連絡先に確認メールを再送信するなどアクションを実行する必要がある場合、ページ上部のバナーに実行する必要のあるアクションが表示されます。
5. ドメインの現在のステータスを確認するときは、[ドメインのステータスコード] フィールドの値を見ます。

   ドメイン名ステータスコードと各コードの意味を説明した現在の一覧については、ICANN ウェブサイトで epp status codes を検索してください。(ICANN ウェブサイトで直接、検索してください。ウェブ検索ではドキュメントの古いバージョンが返されることがあります)。

登録ステータスは、[リクエスト] ページでも確認できます。

登録ステータスを確認するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで、[ドメイン] を展開し、[リクエスト] を選択します。
3. [リクエスト] ページでは、登録ステータスだけでなく、ドメインの削除、ドメイン移管のロック、DNSSEC キーの追加や削除など、ドメインに対して行った他のアクションのステータスも確認することができます。

   メールの確認など、プロセスを完了するために実行すべきアクションがあれば、それも表示されます。

   - アクションリクエストに応答するには、ドメイン名の横にあるラジオボタンを選択し、[アクション] ドロップダウンからアクションを選択します。

ドメインの設定の更新

このセクションでは、Route 53 でのドメイン設定の管理に関連する以下のトピックについて説明します。

1. ドメインの連絡先情報と所有者の更新:
   - 管理担当者、技術担当者、登録者および請求の連絡先など、ドメインの連絡先情報を更新する方法について説明します。
   - レジストリがドメインの所有者変更フォームを要求する場合のドメイン所有者の変更のプロセスについて理解します。
2. ドメインの連絡先情報のプライバシー保護の有効化/無効化:
   - WHOIS クエリから個人情報を表示または非表示にする連絡先情報のプライバシー保護を有効または無効にする方法について説明します。
3. ドメインの自動更新の有効化/無効化:
   - ドメインの自動更新を有効または無効にする方法について説明します。これにより、Route 53 が有効期限前に登録を自動的に更新するかどうかが決まります。
4. 別のレジストラへの許可のない移管を防ぐためのドメインのロック:
   - 別のレジストラへの不正な転送を防ぐためにドメインをロックする方法と、必要に応じてロックを無効にする方法について説明します。
5. ドメインの登録期間の延長:
   - ドメインの登録期間を、通常 1 年単位で最大 10 年延長するプロセスについて理解します。
6. ネームサーバーを更新して別のレジストラを使用する および ドメインのネームサーバーおよびグルーレコードの追加あるいは変更:
   - 別の DNS サービスを使用するようにネームサーバーを更新する方法またはホワイトラベル (バニティ) ネームサーバーを設定する方法について説明します。
   - ネームサーバーとグルーレコードを変更する際の考慮事項とベストプラクティスについて説明します。

ドメインの連絡先情報と所有者の更新

ドメインの管理者および技術担当者の連絡先については、変更の承認を必要とせずにすべての連絡先情報を変更できます。詳細については、「ドメインの連絡先情報の更新」を参照してください。

登録者の連絡先については、変更の承認を必要とせずにほとんどの値を変更できます。ただし、TLD の中には、ドメインの所有者を変更するには承認が必要となるものがあります。詳細については、該当するトピックを参照してください。

トピック

- ドメインの所有権の変更をトリガーするものは何ですか?

- 所有者を変更するために特別な処理を必要とする TLD
- ドメインの連絡先情報の更新
- レジストリがドメインの所有者変更フォームを要求する場合のドメイン所有者の変更

ドメインの所有権の変更をトリガーするものは何ですか?

> **Important**
>
> 登録者として登録した連絡先には、ICANN 移転ポリシーに基づき、ドメイン名の登録名保有者としての特定の権利があります。ほとんどのドメインは、 の閉鎖時に削除されます AWS アカウント (詳細については、「」を参照してくださいAWS アカウントが閉鎖または完全に閉鎖され、ドメインが Route 53 に登録されている)。ただし、ドメインが閉鎖されたアカウントに残っている場合、登録者としてリストした連絡先は、外部レジストラへのドメイン名の移管をリクエストできる場合があります。したがって、リストに記載する登録者の連絡先は、自分または責任を持って行動できる別の信頼できる人物であることが重要です。

登録者の連絡先情報に対する次の変更により、ドメインの所有権変更プロセスがトリガーされます。

個人問い合わせタイプの場合

[First Name] (名) または [Last Name] (姓) フィールドを変更すると、所有権の変更がトリガーされます。

個人以外の問い合わせタイプ (会社、協会、公共団体) の場合

[Organization] (組織) フィールドを変更すると、所有権の変更がトリガーされます。

追加のトリガー (すべての問い合わせタイプ)

ドメインの TLD 要件によっては、次のような他の問い合わせフィールドの変更によって所有権変更プロセスがトリガーされる場合があります。

- 登録者の E メールアドレスの変更
- 他の識別情報フィールドの変更

所有権の変更をトリガーする特定のフィールドは TLD によって異なり、ドメインレジストリのポリシーによって決まります。

> **Warning**
>
> 重要: 所有権の変更がトリガーされると、承認 E メールが届く場合があります。この E メールに 3 ~ 15 日以内に応答しない場合 (TLD に応じて)、変更リクエストがキャンセルされる場合があります。
> 変更によって E メール検証がトリガーされ、3 ~ 15 日以内に確認されない場合 (TLD に応じて)、ドメインが停止され、ウェブサイトや E メールサービスが中断される可能性があります。
> 連絡先を変更する前に、必ず登録者の連絡先メールアドレスにアクセスできることを確認してください。

ドメインの所有者の変更に関する以下の点に注意してください。

- TLD によっては、ドメインの所有者を変更するための料金がかかります。ドメインの TLD に料金がかかるかどうかを判断するには、「Amazon Route 53 のドメイン登録料金」の「所有価格の変更」列を参照してください。

  > **Note**
  >
  > AWS クレジットを使用して料金を支払うことで、ドメインの所有者を変更することはできません。

- 一部の TLDs では、ドメインの所有者を変更すると、Route 53 は登録者の連絡先の E メールアドレスに認可 E メールを送信します。連絡を受信した登録者は、E メールの指示に従って変更を承認する必要があります。
- 一部の TLD では、Amazon Route 53 のサポートエンジニアが値の更新を行うために、ドメインの所有者の変更フォームを入力したうえで身分確認証明を送付する必要がある場合もあります。ドメインの TLD がドメインの所有者の変更フォームを要求する場合、コンソールにサポートケースを開くためのリンクとなるお知らせが表示されます。詳細については、「レジストリがドメインの所有者変更フォームを要求する場合のドメイン所有者の変更」を参照してください。

所有者を変更するために特別な処理を必要とする TLD

ドメインの所有者を変更する場合、一部の TLD のレジストリでは特別な処理が必要になります。次のいずれかのドメインの所有者を変更する場合は、該当する手順を実行します。他のドメインの所有

者を変更する場合は、プログラムまたは Route 53 コンソールを使用して、所有者を自分で変更できます。「ドメインの連絡先情報の更新」を参照してください。

次の TLD では、ドメインの所有者を変更するために特別な処理が必要です。

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

.be

.be ドメインのレジストリから転送コードを取得し、 AWS サポートでケースを開く必要があります。

- 移管コードを取得する方法については、「https://www.dnsbelgium.be/en/manage-your-domain-name/change-holder#transfer」を参照し、プロンプトに従います。
- ケースを開くには、「ドメイン登録の問題に関する AWS サポートへのお問い合わせ」を参照してください。

.cl

フォームに記入して AWS サポートに送信する必要があります。「レジストリがドメインの所有者変更フォームを要求する場合のドメイン所有者の変更」を参照してください。

.com.ar

フォームに記入して AWS サポートに送信する必要があります。「レジストリがドメインの所有者変更フォームを要求する場合のドメイン所有者の変更」を参照してください。

.com.br

フォームに記入して AWS サポートに送信する必要があります。「レジストリがドメインの所有者変更フォームを要求する場合のドメイン所有者の変更」を参照してください。

.es

フォームに記入して AWS サポートに送信する必要があります。「レジストリがドメインの所有者変更フォームを要求する場合のドメイン所有者の変更」を参照してください。

.fi

Route 53 コンソール上から、所有者の変更を開始します。この変更を開始すると、E メールアドレス fi-domain-tech@traficom.fi からホルダートランスファーキーが送られます。キーを受け取ったら、 AWS Support でサポートケースを開き、キーコードを当社と共有します。「ドメイン登録の問題に関する AWS サポートへのお問い合わせ」を参照してください。

.qa

フォームに記入して AWS サポートに送信する必要があります。「レジストリがドメインの所有者変更フォームを要求する場合のドメイン所有者の変更」を参照してください。

.ru

フォームに記入して AWS サポートに送信する必要があります。「レジストリがドメインの所有者変更フォームを要求する場合のドメイン所有者の変更」を参照してください。

.se

フォームに記入して AWS サポートに送信する必要があります。「レジストリがドメインの所有者変更フォームを要求する場合のドメイン所有者の変更」を参照してください。

.sh

フォームに記入して AWS サポートに送信する必要があります。「レジストリがドメインの所有者変更フォームを要求する場合のドメイン所有者の変更」を参照してください。

ドメインの連絡先情報の更新

ドメインの連絡先情報を更新するには、以下の手順を実行します。

> **Warning**
>
> 重要: 連絡先の変更によって所有者の変更プロセスがトリガーされた場合、承認 E メールが届くことがあります。この E メールに 3 ~ 15 日以内に応答しない場合 (TLD に応じて)、変更リクエストがキャンセルされる場合があります。
> 変更によって E メール検証がトリガーされ、3 ~ 15 日以内に確認されない場合 (TLD に応じて)、ドメインが停止され、ウェブサイトや E メールサービスが中断される可能性があります。
> 連絡先を変更する前に、必ず登録者の連絡先メールアドレスにアクセスできることを必ず確認してください。

ドメインの連絡先を更新する前

ドメインの登録者の連絡先情報を変更する前に、次のチェックリストを完了してください。

1. □ E メールアクセスを確認する - 現在の登録者の E メールアドレスで E メールを受信できることを確認します

2. □ 所有者変更トリガーを理解する - 「the section called “ドメインの所有権の変更をトリガーするものは何ですか?”」を確認して、所有者変更プロセスをトリガーする可能性のある変更について理解します。
3. □ 認可の計画 - 所有者の変更がトリガーされた場合、認可 E メールに返信するまで 3 ~ 15 日かかります。そうしないと、変更リクエストがキャンセルされる場合があります。

ドメインの連絡先情報を更新するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [Registered Domains] をクリックします。
3. 連絡先情報を更新するドメインの名前を選択します。
4. [連絡先情報] タブで、[編集] をクリックします。
5. 登録者の連絡先の E メールアドレスへのアクセス権がない場合は、以下のステップを実行します。登録者の連絡先のメールアドレスへのアクセス権がある場合は、ステップ 6 に進みます。

   a. 登録者の連絡先の E メールアドレスのみを変更します。ドメインのいずれの連絡先についても、他の値を変更しないでください。他の値も変更する場合は、プロセスの後半でその値を変更します。

      [Save changes] (変更の保存) をクリックします。

      新しい E メールアドレスを検証するために、Route 53 は新しいアドレスに検証 E メールを送信します (TLD で必要な場合)。新しい E メールアドレスが有効であることを確認するには、E メールにあるリンクを選択する必要があります。新しい E メールアドレスの確認が必要であるにもかかわらず確認しない場合、Route 53 では ICANN の要件に従ってドメインが保留されます。

      確認メールを再送信する必要がある場合は、[登録済みドメイン] ページに進み、更新したドメイン名の横にあるラジオボタンを選択して、更新するドメインの名前を選択します。[ドメインの停止を回避するために E メールを検証] アラートで、[E メールを再送信] を選択します。

   b. ドメインの登録者、管理者、技術担当者、または請求の連絡先の他の値を変更する場合は、ステップ 1 をもう一度実行します。

6. 目的の値を更新します。[登録者の連絡先をコピー] を選択すれば、登録者の連絡先に入力したものと同じ情報を、自動で入力することができます。詳細については、「ドメインを登録または移管するときに指定する値」を参照してください。

   ドメインの TLD と変更する値によって、コンソールは次のメッセージを表示する場合があります。

   「To change the registrant name or organization, open a case」

   メッセージが表示された場合、この手順の残りを省略します。詳細については、「レジストリがドメインの所有者変更フォームを要求する場合のドメイン所有者の変更」を参照ください。

7. [保存] を選択します。

8. 「」で説明されているようにドメイン所有者を変更した場合ドメインの所有権の変更をトリガーするものは何ですか?、Route 53 はドメインの登録者の連絡先に E メールを送信します。E メールでは、所有者の変更の承認が要求されます。

   Route 53 が 3 ~ 15 日以内に変更の承認を受け取らない場合、最上位ドメインに応じて、Route 53 は ICANN の要求に従ってリクエストをキャンセルする必要があります。

   メールは次のメールアドレスの 1 つから送信されます。

TLD	許可メールの発信元となるメールアドレス
.fr	nic@nic.fr
.com.au .net.au	noreply@emailverification.info
その他すべて	以下のいずれかの E メールアドレス: • noreply@registrar.amazon • noreply@domainnameverification.net • noreply@emailverification.info

TLD	許可メールの発信元となるメールアドレス

9. 連絡先情報の更新中に問題が発生した場合は、 AWS サポートに無料でお問い合わせください。詳細については、「ドメイン登録の問題に関する AWS サポートへのお問い合わせ」を参照してください。

連絡先情報の更新に使用できる API の詳細については、「UpdateDomainContact」を参照してください。

レジストリがドメインの所有者変更フォームを要求する場合のドメイン所有者の変更

ドメインのレジストリでドメイン所有権の変更を完了し、 AWS サポートにフォームを送信する必要がある場合は、次の手順を実行します。この手順を実行する必要があるかどうかを判断するには、次のトピックを参照してください。

- 変更している値が所有者の変更と見なされるかどうかを判断するには、「ドメインの所有権の変更をトリガーするものは何ですか?」を参照してください。
- ドメインに ドメイン所有権の変更フォームが必要かどうかを判断するには、「所有者を変更するために特別な処理を必要とする TLD」を参照してください。

レジストリがドメインの所有者変更フォームを要求する場合のドメイン所有者の変更方法

1. このトピックの概要を参照し、ドメインのレジストリで、ドメイン所有者を変更するための特別な処理が必要かどうかを判断します。特別な処理が必要で、ドメイン所有者の変更フォームが必要な場合は、次の手順に進みます。

   ドメイン所有者の変更フォームが必要ない場合は、該当するトピックに示されている手順を実行します。
2. ドメイン所有者の変更フォームをダウンロードします。ファイルは .zip ファイルに圧縮されます。
3. フォームに入力します。
4. ドメインの以前の所有者および新しい所有者に対する登録者の連絡先の場合は、ID カード、運転免許証、パスポート、またはその他の法的な身分証明書など、個人の署名入りの身分証明書のコピーを準備してください。

さらに、登録者の組織が法人と表示されている場合は、ドメインの以前の所有者および新しい所有者に関する以下の情報を収集します。

- ドメインが登録されている組織が存在することの証明。
- 以前の所有者および新しい所有者の代理人が組織の代表として行動する権限を保有することの証明。この書類は、組織名および署名権限保有者としての代理人の名前 (CEO、社長、取締役など) の両方が記されている認証法的文書である必要があります。

5. ドメイン所有者変更フォームと必要な書類をスキャンします。.pdf ファイルや .png ファイルなどの一般的な形式でスキャンしたドキュメントを保存します。
6. ドメインが現在登録されている AWS アカウントを使用して、AWS サポートセンターにサインインします。

> **Important**
>
> ルートアカウントを使用するか、以下の 1 つ、または複数の方法で IAM 許可が付与されているユーザーを使用してサインインする必要があります。
>
> - ユーザーには、AdministratorAccess 管理ポリシーが割り当てられます。
> - ユーザーには、AmazonRoute53DomainsFullAccess 管理ポリシーが割り当てられます。
> - ユーザーには、AmazonRoute53FullAccess 管理ポリシーが割り当てられます。
>
> ルートアカウントまたは必要なアクセス許可を持つユーザーを使用してサインインしない場合、Route 53 はドメイン所有者を更新できません。この要件によって、権限のないユーザーがドメインの所有者を変更することを防ぎます。

7. 次の値を指定します。

内容

デフォルト値の [アカウントと請求] をそのまま使用します。

サービス

デフォルト値の [ドメイン] をそのまま使用します。

Category

デフォルト値の [所有権の変更] をそのまま使用します。

緊急度

デフォルト値の [一般的な質問] をそのまま使用します。

[次のステップ: 追加情報] を選択します。

件名

[Change the owner of a domain (ドメインの所有者の変更)] を指定します

説明

以下の情報を記述します。

- 所有者を変更するドメイン
- ドメインが登録されているアカウントの 12 桁のアカウント ID AWS

添付ファイルの追加

ステップ 5 でスキャンしたドキュメントをアップロードします。

連絡方法

連絡方法を指定し、適切な値を入力します。

8. [Submit] を選択してください。

AWS サポートエンジニアは、指定した情報を確認し、設定を更新します。更新が完了したとき、または追加情報が必要な場合に、エンジニアから連絡が送信されます。

ドメインの連絡先情報のプライバシー保護の有効化/無効化

Amazon Route 53 にドメインを登録するか、Route 53 にドメインを移管すると、Route 53 はドメインのすべての連絡先に対してデフォルトでプライバシー保護を有効にします。これによって一般的に、WHOIS ("Who is") クエリから返される連絡先情報の大部分が非表示になり、送られてくるスパムの数が減少します。プライバシー保護を有効にすると、お客様の連絡先情報は、レジストラの連絡先情報に置き換えられるか、「REDACTED FOR PRIVACY」(プライバシー保護のために編集済み) または「On behalf of <domain name> owner」(<ドメイン名> の所有者に代わって) という文言に置き換えられます。

プライバシー保護を無効にする場合は、ドメインのすべての連絡先を対象にする必要があります。プライバシー保護を無効にすると、誰でもドメインに関する WHOIS クエリを送信でき、ほとんどの最上位ドメイン (TLD) について、名前、住所、電話番号、E メールアドレスなど、ドメインの登録時

または移管時に指定したすべての連絡先情報を取得できる可能性があります。WHOIS コマンドは広く利用できます。多くのオペレーティングシステムに付属し、多くのウェブサイトでウェブアプリケーションとしても利用できます。

ドメインを別のレジストラに移管しており、ドメイン連絡先に対してプライバシー保護が有効化されているという場合、移管を確認するための E メールは、Amazon レジストラに登録されている TLD 用の identity-protect.org アドレスから配信されます。TLD のレジストラを調べる方法については、「レジストラの検索」を参照してください。

WHOIS クエリから隠すことのできる情報は 2 つの主な要因によって決まります。

最上位ドメインのレジストリ

ほとんどの TLD レジストリですべての連絡先情報が自動的に隠されますが、すべての連絡先情報を隠すかどうかを選択できるレジストリや、一部の情報のみを隠すことができるレジストリ、どの情報も隠すことができないレジストリもあります。一部の TLD レジストリは、ローカルの規制またはレジストリポリシーに準拠するために、プライバシー保護を意図的に抑制します。

ドメインのプライバシー保護を有効にすると、お客様の連絡先情報は、プライバシー保護サービスの連絡先情報に置き換えられるか、「REDACTED FOR PRIVACY」(プライバシーのために編集済み) という文言に置き換えられます。プライバシー保護サービスはスパム防止機能 (アドレスローテーションと SPF/DKIM/スパム分析) を適用し、大抵はこれらのフィルターを通過したメールを自動的に転送します。ただし、プライバシー保護対象の E メールアドレスに重要な E メールを送信することはお勧めしません。スパムメカニズムがこれらの E メールの転送を妨げる可能性があるためです。

また、ドメインにどのプライバシー保護メカニズムを使用するかの選択は設定できず、システムによって自動的に選択されます。プライバシー保護サービスの連絡先情報を手動で更新することはできません。

> **Note**
>
> 一部のドメインのプライバシー保護を有効または無効にするには、サポートケースを開いてプライバシー保護をリクエストする必要があります。詳細については、「Amazon Route 53 に登録できる最上位ドメイン」の該当するセクションを参照してください。
>
> - .co.uk (英国)
> - .me.uk (英国)
> - .org.uk (英国)

- .link

レジストラ

ドメインを Route 53 に登録する場合やドメインを Route 53 に移管する場合、ドメインのレジストラは Amazon Registrar または当社のレジストラ関連会社である Gandi のいずれかです Amazon Registrar と Gandi では、デフォルトで非表示になる情報が異なります。

- Amazon Registrar- デフォルトでは、お客様の連絡先情報すべてが非表示です。ただし、TLD レジストリの規則が優先されます。
- Gandi -デフォルトでは、組織名 (存在する場合) を除いて、お客様の連絡先情報すべてが非表示です。ただし、TLD レジストリの規則が優先されます。

  プライバシー保護を許可しない地域別 TLD では、個人情報は Gandi ウェブサイトの Whois ディレクトリ検索ページで「編集された」とマークされます。ただし、個人情報はドメインレジストリまたはサードパーティーの WHOIS ウェブサイトから入手できます。

お使いのドメインの TLD で非表示になる情報を確認するには、「Amazon Route 53 に登録できる最上位ドメイン」を参照してください。

Route 53 を使用して登録したドメインのプライバシー保護を有効または無効にする場合は、次の手順を実行します。

Important

プライバシー保護の可用性: プライバシー保護はすべての TLD で利用できるわけではありません。プライバシー保護をサポートしていない一般的な TLD には、.de、.us、.com.au、.es などがあります。
ドメインの連絡先情報を編集するときに「プライバシー保護」セクションが表示されない場合、ドメインの TLD ではプライバシー保護はサポートされていません。
プライバシー保護をサポートしていない TLD の完全なリストについては「プライバシー保護をサポートしていない TLD」を参照してください。TLD のプライバシー保護サポートの詳細については「Amazon Route 53 に登録できる最上位ドメイン」を参照してください。

ドメインの連絡先情報のプライバシー保護を有効または無効にするには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [Registered Domains] をクリックします。
3. プライバシー保護を有効または無効にするドメインの名前を選択します。
4. [連絡先情報] セクションで、[編集] をクリックします。
5. [プライバシー保護] セクションで、連絡先情報を隠すかどうかを選択します。4 種類の連絡先 (管理担当者、登録者、技術担当請求、および請求) のすべてに同じプライバシー設定を指定する必要があります。

   > **Note**
   >
   > お使いの TLD でプライバシー保護がサポートされていない場合、プライバシー保護セクションは表示されません。連絡先情報は、プライバシー保護をサポートしていないドメインの WHOIS クエリで公開されます。

6. [Save changes] (変更の保存) をクリックします。
7. プライバシー保護の有効化または無効化中に問題が発生した場合は、 AWS サポートに無料でお問い合わせください。詳細については、「ドメイン登録の問題に関する AWS サポートへのお問い合わせ」を参照してください。

プライバシー保護をサポートしていない TLD

以下の TLD はプライバシー保護をサポートしていません。ドメインがこれらの TLD のいずれかを使用している場合、連絡先情報は WHOIS クエリで公開されます。

汎用 TLD

.audio、.ceo、.diet、.flowers、.guitars、.hosting、.juegos、.property、.sexy

地域別 TLD

.cl (チリ)、.com.ar (アルゼンチン)、.com.au (オーストラリア)、.com.br (ブラジル)、.com.sg (シンガポール)、.de (ドイツ)、.es (スペイン)、.in (インド)、.net.au (オーストラリア)、.qa (カタール)、.ru (ロシア)、.sg (シンガポール)、.us (米国)、.vg (英領バージン諸島)

> **Note**
>
> このリストには、プライバシー保護をサポートしていない最も一般的な TLD が含まれています。特定の TLD のプライバシー保護サポートに関する完全な最新情報については、「Amazon Route 53 に登録できる最上位ドメイン」の個々の TLD ページを参照してください。

プライバシー保護の問題のトラブルシューティング

プライバシー保護オプションは コンソールでは使用できません

これは、ドメインの TLD がプライバシー保護をサポートしていないことを示します。連絡先情報は WHOIS クエリで公開されます。これは、レジストリポリシーまたはローカル規制による特定の TLD の通常の動作です。

TLD がプライバシー保護をサポートしているかどうかを確認するには、Amazon Route 53 に登録できる最上位ドメイン の個々の TLD ページを確認するか、「プライバシー保護をサポートしていない TLD」を参照してください。

連絡先情報は、プライバシー保護を有効にした後も引き続き表示されます。

一部のレジストリは独自の WHOIS データベースを維持し、Route 53 でプライバシー保護が有効になっている場合でも連絡先情報を表示し続ける場合があります。これは、Route 53 ではなく TLD レジストリによって制御されます。

さらに、一部の TLD レジストリは、ドメインに対して限定的なプライバシー保護または秘匿化サービスを意図的に維持しています。

ドメインの自動更新の有効化/無効化

Amazon Route 53 により、ドメインが有効期限切れになる少し前に登録を自動更新するかどうかの変更を行う場合、または自動更新の現在の設定を表示するには、次の手順を実行します。

クレジットを使用してドメインの登録を更新するための料金 AWS を支払うことはできません。

> **Note**
>
> AWS アカウントをキャンセルするときは、必ず自動更新をオフにします。それ以外の場合は、更新通知が引き続き送信されます AWS。ただし、アカウントを再度有効にしない限り、ドメインは更新されません。

ドメインの自動更新を有効または無効にするには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [Registered Domains] をクリックします。
3. 更新するドメインの名前を選択します。
4. [詳細] セクションの [アクション] ドロップダウンで、[自動更新をオンにする] を選択します。

   [<ドメイン名> の自動更新をオンにしますか?] で年間料金の支払いに同意して、[オンにする] を選択します。

   > **Note**
   >
   > 記載の料金はその時点における登録期間のものであり、変更される場合があります。詳細については、「Amazon Route 53 のドメイン登録料金」を参照してください。

5. 自動更新をオフにするには、[アクション] ドロップダウンで [自動更新をオフにする] を選択します。
6. 自動更新の有効化または無効化中に問題が発生した場合は、 AWS サポートに無料でお問い合わせください。詳細については、「ドメイン登録の問題に関する AWS サポートへのお問い合わせ」を参照してください。

別のレジストラへの許可のない移管を防ぐためのドメインのロック

すべての汎用 TLDs と多くの地理的 TLDs のドメインレジストリは、ドメインのロックをサポートし、ユーザーの許可なしに誰かがドメインを別のレジストラに転送できないようにします。ドメインのレジストリがドメインのロックをサポートしているかどうかを確認するには、「」を参照してくださいAmazon Route 53 に登録できる最上位ドメイン。ロックがサポートされていて、ドメインをロックする場合は、次の手順を実行します。また、ドメインを別のレジストラに移管する場合は、ロックを無効にする手順を使用できます。

レジストラへの許可のない移管を防ぐためにドメインをロックするには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [Registered Domains] を選択します。
3. 更新するドメインの名前を選択します。
4. [詳細] セクションの [アクション] ドロップダウンで、移管ロックをオンにするか、オフにするかに応じて、[移管ロックをオンにする] または [移管ロックをオフにする] を選択します。

   [リクエスト] ページに進むと、リクエストの進捗状況を確認できます。
5. ドメインのロック中に問題が発生した場合は、 AWS サポートに無料でお問い合わせください。詳細については、「ドメイン登録の問題に関する AWS サポートへのお問い合わせ」を参照してください。

WHOIS 検索では、このステータスは次のように表示されます: `clientTransferProhibited`。一部の TLD には、さらに次のステータスがある場合があります。

- `clientUpdateProhibited`
- `clientDeleteProhibited`

ドメインの登録期間の延長

Amazon Route 53 にドメインを登録するか、Route 53 にドメイン登録を移管すると、Route 53 は自動的に更新するようにドメインを設定します。自動更新期間は通常 1 年間となりますが、いくつかの最上位ドメイン (TLD) のレジストリにおいては更新期間がさらに延長する場合があります。

次の点に注意してください。

最大更新期間

すべての汎用 TLD と多くの国コード TLD は、ドメイン登録を長期間 (1 年単位で最大 10 年まで) 延長することができます。ドメインの登録期間を延長できるかどうか判断するには、「Amazon Route 53 に登録できる最上位ドメイン」を参照してください。長い登録期間が認められる場合、以下の手順を実行します。

ドメイン登録を更新または延長できる時期の制限

TLD レジストリの中には、ドメイン登録を更新または延長できる時期に制限を設けているものがあります (期限が切れる 2 か月前以降など)。レジストリによりドメインの登録期間の延長が許可される場合でも、ドメインの有効期限がもっと近づいてからでないと延長できないことがあります。

> **Note**
>
> 例えば、ドメインがある TLD の最大許容更新期間が 5 年の場合、5 年の制限に達するまでいつでも年次更新を追加できます。具体的には、現在有効期間が 2.5 年のドメインがある場合、更新できるのは最大 2 年間のみです。

AWS クレジット

AWS クレジットを使用して、ドメインの登録期間を延長するための料金を支払うことはできません。

ドメインの登録期間を延長するには

1. Route 53 コンソール (https://console.aws.amazon.com/route53/) を開きます。
2. ナビゲーションペインで [Registered Domains] を選択します。
3. 登録期間を延長したいドメイン名を選択します。
4. [詳細] セクションの [アクション] ドロップダウンで、[ドメイン登録の更新] を選択します。
5. [ドメイン登録の更新] ダイアログボックスの [更新期間] ドロップダウンで、登録を延長する年数を選択します。

   このリストには、現在の有効期限終了日とこのドメインのレジストリにより許可される最大登録期間に基づく現在のオプションがすべて表示されます。指定した年数から算出された有効期限日が、期間の下に表示されます。
6. [ドメイン登録の更新] を選択します。

   Route 53 は、有効期限を更新したという確認をレジストリから受け取ると、有効期限が変更されたことを確認する E メールを送信します。

7. ドメインの登録期間の延長中に問題が発生した場合は、 AWS サポートに無料でお問い合わせください。詳細については、「ドメイン登録の問題に関する AWS サポートへのお問い合わせ」を参照してください。

ネームサーバーを更新して別のレジストラを使用する

DNS 管理を別のレジストラに移管する場合は、次を指すようにネームサーバーを更新する必要があります。

他の DNS サービスを使用するときにドメインのネームサーバーを更新するには

1. DNS サービスから提供されるプロセスを使用して、ドメインのネームサーバーを取得します。
2. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
3. ナビゲーションペインで [Registered Domains] をクリックします。
4. 他の DNS サービスを使用するように設定するドメインの名前を選択します。
5. [詳細] セクションの [アクション] ドロップダウンで、[ネームサーバーの編集] を選択します。
6. 既存のネームサーバーを削除し、ステップ 1 で DNS サービスから取得したネームサーバーの、ネームサーバー名を追加します。
7. [Save changes] (変更の保存) をクリックします。
8. (オプション) ドメインの登録時に Route 53 によって自動的に作成されたホストゾーンを削除します。これにより、使用していないホストゾーンに料金がかかることがなくなります。

    a. ナビゲーションペインで [Hosted Zones] を選択します。
    b. ドメインと同じ名前のホストゾーンのラジオボタンを選択します。
    c. [Delete Hosted Zone] を選択します。
    d. [Confirm] を選択して、ホストゾーンの削除を確定します。

ドメインのネームサーバーおよびグルーレコードの追加あるいは変更

Route 53 にドメインを登録すると、Route 53 はドメインのホストゾーンを自動的に作成し、4 つのネームサーバーをホストゾーンに割り当て、それらのネームサーバーを使用するようにドメイン登録を更新します。通常は、別の DNS サービスまたはホワイトラベルネームサーバーを使用する場合以外は、これらの設定を変更する必要はありません。

Route 53 のドメインあたりの最大ネームサーバー数は 6 です。

> **Warning**
>
> ネームサーバーを間違った値に変更したり、グルーレコードで間違った IP アドレスを指定したり、新しいネームサーバーを指定しないでネームサーバーを削除したりすると、最大 2 日間、ウェブサイトまたはアプリケーションがインターネットで使用できなくなることがあります。

トピック

- ネームサーバーとグルーレコードの変更に関する考慮事項
- ネームサーバーまたはグルーレコードの追加または変更

ネームサーバーとグルーレコードの変更に関する考慮事項

設定を変更する前に、以下の点を考慮してください。

トピック

- 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

Route 53 をドメインの DNS サービスにする

別の DNS サービスを現在使用していて、Route 53 をドメインの DNS サービスにする場合、DNS サービスを Route 53 に移行する方法の詳細については、「Amazon Route 53 を既存ドメインの DNS サービスとして使用する」を参照してください。

> **Important**
>
> 移行プロセスに厳密に従わないと、ドメインがインターネットで最大 2 日間利用できなくなることがあります。

別の DNS サービスを使用する場合

ドメインで Route 53 以外の DNS サービスを使用する場合は、次の手順に従って、ドメイン登録のネームサーバーを他の DNS サービスで提供されるネームサーバーに変更します。

> **Note**
>
> ネームサーバーを変更したときに Route 53 が次のエラーメッセージを返す場合、指定したネームサーバーは TLD のレジストリでは有効なネームサーバーとして認識されていません。
> `"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 レジストリでは通常、パブリック DNS サービスで提供されているネームサーバーはサポートされていますが、Amazon EC2 インスタンスで設定した DNS サーバーなどのプライベート DNS サーバーは、レジストリにそのネームサーバーの IP アドレスが登録されている場合を除いてサポートされていません。Route 53 は、TLD レジストリで認識されていないネームサーバーの使用をサポートしていません。このエラーが発生した場合、Route 53 のネームサーバーまたは別のパブリック DNS サービスに変更する必要があります。

ホワイトラベルネームサーバーを使用する場合

ネームサーバーの名前を自分のドメインのサブドメインにする場合は、ホワイトラベルネームサーバーを作成できます。(ホワイトラベルネームサーバーは、バニティネームサーバーやプライベートネームサーバーとも呼ばれます)。例えば、ドメイン example.com の ns4.example.com を使用してネームサーバー ns1.example.com を作成します。ホワイトラベルネームサーバーを使用するには、次の手順に従って、ネームサーバーの名前ではなく IP アドレスを指定します。この IP アドレスはグルーレコードと呼ばれています。

ホワイトラベルネームサーバーの設定の詳細については、「ホワイトラベルネームサーバーの設定」を参照してください。

.it ドメインのネームサーバーを変更している

IT ドメインのネームサーバーは DNS チェックに合格する必要があります。変更リクエストを送信する前に、「https://dns-check.nic.it/」でネームサーバーをチェックすることをおすすめしま

す。レジストリは、変更を行う前のネームサーバーを使用して DNS クエリに応答し続けます。以前のネームサーバーが使用できなくなった場合、ドメインはインターネットで使用できなくなります。

> **Important**
>
> ドメインのネームサーバーを変更するたびに、古い DNS サービスをキャンセルしたり、古いネームサーバーを使用していた Route 53 ホストゾーンを削除したりする前に、DNS が新しいネームサーバーを使用してクエリに応答していることを確認してください。

.it ドメインのレジストリを使用してネームサーバーの名前を修正 AWS するためのヘルプを から取得する方法については、「」を参照してください[ドメイン登録の問題に関する AWS サポートへのお問い合わせ](#)。

ネームサーバーまたはグルーレコードの追加または変更

ネームサーバーまたはグルーレコードを追加または変更するには、以下の手順を実行します。

> **Note**
>
> デフォルトでは、DNS リゾルバーは通常、ネームサーバーの名前を 2 日間キャッシュします。その結果、変更が反映されるまでに 2 日かかる場合があります。詳細については、「[Amazon Route 53 によりドメインのトラフィックをルーティングする方法](#)」を参照してください。

ドメインのネームサーバーまたはグル–レコードを追加または変更するには

1. 「[ネームサーバーとグルーレコードの変更に関する考慮事項](#)」を確認し、該当する問題がある場合は対処します。
2. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
3. ナビゲーションペインで [Registered Domains] をクリックします。
4. 設定を編集するドメインの名前を選択します。
5. [詳細] セクションの [アクション] ドロップダウンで、[ネームサーバーの編集] を選択します。

6. [ネームサーバーの編集] ダイアログボックスでは、以下を実行できます。

   - ドメインの DNS サービスを変更するには、次のいずれかの操作を実行します。
     - 別の DNS サービスのネームサーバーを、Route 53 ホストゾーンのネームサーバーに置き換えます。
     - Route 53 ホストゾーンのネームサーバーを、別の DNS サービスのネームサーバーに置き換えます。
     - Route 53 ホストゾーンのネームサーバーを、別の Route 53 ホストゾーンのネームサーバーに置き換えます。

     ドメインの DNS サービスの変更については、「Amazon Route 53 を既存ドメインの DNS サービスとして使用する」を参照してください。ドメインの DNS サービスに使用する Route 53 ホストゾーンのネームサーバーの取得については、「パブリックホストゾーンに対するネームサーバーの取得」を参照してください。
   - ネームサーバーを追加します (複数可)。
   - 既存のネームサーバーの名前を置き換えます。
   - ホワイトラベルネームサーバーを指定する場合は、グルーレコードの IP アドレスを追加または変更します。IPv4 または IPv6 形式でアドレスを入力できます。ネームサーバーに複数の IP アドレスがある場合は、各アドレスを個別の行に入力します。

     ホワイトラベルネームサーバーでは、ネームサーバーの名前にお客様のドメイン名 (example.com など) が含まれています。例えば、ns1.example.com となっています。ホワイトラベルネームサーバーを指定すると、Route 53 からネームサーバーに 1 つ以上の IP アドレスを指定するように求められます。この IP アドレスはグルーレコードと呼ばれます。詳細については、「ホワイトラベルネームサーバーの設定」を参照してください。
   - ネームサーバーを削除します。そのネームサーバーのフィールドの右側にある X 印のアイコンを選択します。

   > ⚠ Warning
   >
   > ネームサーバーを間違った値に変更したり、グルーレコードで間違った IP アドレスを指定したり、新しいネームサーバーを指定しないでネームサーバーを削除したりすると、最大 2 日間、ウェブサイトまたはアプリケーションがインターネットで使用できなくなることがあります。

7. [更新] を選択します。

8. ネームサーバーまたはグルーレコードの追加または変更中に問題が発生した場合は、 AWS サポートに無料でお問い合わせください。詳細については、「ドメイン登録の問題に関する AWS サポートへのお問い合わせ」を参照してください。

ドメインの登録の更新

Amazon Route 53 にドメインを登録するか、Route 53 にドメイン登録を移管すると、Route 53 は自動的に更新するようにドメインを設定します。自動更新期間は通常 1 年間となりますが、いくつかの最上位ドメイン (TLD) のレジストリにおいては更新期間がさらに延長する場合があります。TLD の登録および更新期間については、「Amazon Route 53 に登録できる最上位ドメイン」を参照してください。

> **Note**
>
> AWS クレジットを使用して、ドメインの登録を更新するための料金を支払うことはできません。

ほとんどの最上位ドメイン (TLD) では、ドメインの有効期限を変更できます。詳細については、「ドメインの登録期間の延長」を参照してください。

> **Important**
>
> 自動更新を停止したら、ドメインに対する次の影響に注意してください。
>
> - TLD レジストリのなかには、更新を十分な時間的余裕を持って行わなかった場合に、有効期限切れ以前でもドメインが削除されるものがあります。ドメイン名の維持を希望する場合には、自動更新を有効にしておくことを強くお勧めします。
> - また、有効期限が切れた後にドメインを再登録しないことを強くお勧めします。ドメインが有効期限切れになった直後にそのドメインを登録することを許可するレジストラもあり、この場合、他者によってドメインが取得される以前に再登録できないことがあります。
> - レジストリのなかには、有効期限が切れたドメインの復元に高額の割増金を請求することもあります。
> - 有効期限日当日またはその近日になると、ドメインはインターネット上で利用できなくなります。

自動更新がドメインに対して有効かどうかを確認するには、「ドメインの自動更新の有効化/無効化」を参照してください。

自動更新が有効な場合は、以下のような過程になります。

有効期限切れの 45 日前

Route 53 は、登録者の連絡先に E メールを送信します。この E メールには、自動更新が現在有効であること、および自動更新を無効にする方法が記載されています。登録者の連絡先 E メールアドレスを最新状態にして、この E メールを見逃さないようにしておきます。

有効期限の 30 日から 35 日前

.com.ar ドメインと .com.br ドメインを除くすべてのドメインについて、Route 53 は有効期限の 35 日前にドメイン登録を更新し、ドメイン名の有効期限が切れる前に更新の問題を解決する時間を確保します。

.com.ar ドメインと .com.br ドメインのレジストリでは、Route 53 が有効期限の 30 日以内にドメインを更新する必要があります。レジストラアソシエイトである Gandi から、有効期限の 30 日前に更新 E メールが届きます。これは、自動更新が有効になっている場合に Route 53 がドメインを更新するのと同じ日です。

> **Note**
>
> Route 53 がドメインを更新すると、Route 53 はドメインの更新を通知する E メールを送信します。更新が失敗した場合、Route 53 は失敗した理由を説明する E メールを送信します。

自動更新が無効になっている場合、ドメイン名に関しては、以下の過程になります。

有効期限の 45 日前

Route 53 は、ドメインの登録者の連絡先に E メールを送信します。この E メールには、自動更新が現在無効になっており、有効にする方法が記載されています。登録者の連絡先 E メールアドレスを最新状態にして、この E メールを見逃さないようにしておきます。

有効期限切れの 7 日から 30 日前

ドメインで自動更新が無効になっている場合、ドメイン登録の運営組織である ICANN は、レジストラが E メールを送信することを義務付けています。メールは次のメールアドレスの 1 つから送信されます。

- noreply@registrar.amazon – ドメインのレジストラが Amazon Registrar の場合。
- noreply@domainnameverification.net または noreply@emailverification.info – レジストラが当社のレジストラアソシエイトであるドメインの場合、Gandi。

TLD のレジストラを調べる方法については、「Amazon Route 53 に登録できる最上位ドメイン」を参照してください。

有効期限の 30 日前に自動更新を有効にし、更新期間が経過していない場合、Route 53 は 24 時間以内にドメインを更新します。

> **Important**
>
> いくつかの TLD 登録にはドメインを更新できる時期に制限があります。ドメインに固有の詳細については、「Amazon Route 53 に登録できる最上位ドメイン」を参照してください。さらに、更新処理には 1 日以上かかる可能性があります。自動更新を有効にする時期が遅れると、更新処理が完了する以前にドメインが失効してしまい、ドメインが失われる場合もあります。有効期間が近づいている場合、ドメインの有効期限を手動で延長することをお勧めします。詳細については、「ドメインの登録期間の延長」を参照してください。

更新期間の詳細については、「Amazon Route 53 に登録できる最上位ドメイン」の TLD の「ドメインの更新と復元の期限」セクションを参照してください。

有効期限経過後

ほとんどのドメインは、有効期限が過ぎた後に短期間保持されるため、失効したドメインを有効期間後に更新できる場合もあります。ただし、ドメインを維持したい場合は自動更新を有効にしておくことが強く推奨されます。有効期間を経過後にドメインを更新するためについての詳細は、「失効した、または削除されたドメインの復元」を参照してください。

ドメインの有効期限が切れたが、ドメインで後期更新が許可されている場合は、標準更新価格でドメインを更新できます。ドメインがまだ後期更新期間内であるかどうかを確認するには、「ドメインの登録期間の延長」セクションの手順を実行します。ドメインがまだリストされる場合は、後期更新期間内です。

更新期間の詳細については、「Amazon Route 53 に登録できる最上位ドメイン」の TLD の「ドメインの更新と復元の期限」セクションを参照してください。

失効した、または削除されたドメインの復元

後期更新期間が終了する前にドメインを更新しないか、ドメインを誤って削除した場合、最上位ドメイン (TLD) のいくつかのレジストリにより、他のユーザーが登録できるようになる前に、ドメインを復元することができます。

ドメインが削除されるか、後期更新期間の期限が過ぎた場合は、Amazon Route 53 コンソールに表示されなくなります。

> **Important**
>
> 通常、ドメインの復元料金は高額で、場合によってはドメインの登録または更新の料金よりもはるかに高くなることがあります。ドメイン復元の現行料金については、「Amazon Route 53 のドメイン登録料金」の「復元料金」を参照してください。

AWS クレジットを使用して、期限切れのドメインの復元料金を支払うことはできません。

ドメインが削除されたか、後期更新期間の有効期限が切れた場合にドメイン登録の復元を試みるには

1. ドメインの TLD レジストリがドメインの復元をサポートしているかどうかと、サポートしている場合は復元が可能な期間を確認します。

   a. Amazon Route 53 に登録できる最上位ドメイン に移動します。

      > **Important**
      >
      > 登録後最初の 5 日以内に削除された汎用 TLD ドメインの場合、標準の 30 日間の交換期間 (実際の交換期間日数を確認するには「Amazon Route 53 に登録できる最上位ドメイン」を参照してください) は適用されません。代わりに、これらのドメインはすぐに新しい登録に使用できるようになります。

   b. ドメインの TLD を検索し、「ドメインの更新と復元の期限」セクションで値を確認します。

      > **Important**
      >
      > Route 53 は復元リクエストを Gandi に転送し、月曜日から金曜日の営業時間中にリクエストを処理します。Gandi はパリに拠点を置くため、時間帯には UTC (協定世界時) /

GMT (標準時) + 1 時間が適用されます。このため、リクエストを送信する時間により、まれにリクエスト処理に 1 週間以上かかる場合があります。

2. ドメインの復元料金を確認します。場合によってはドメインの登録または更新の料金よりもはるかに高くなることがあります。「Amazon Route 53 のドメイン登録料金」で、ドメインの TLD (.com など) を見つけ、「復元料金」列で料金を確認します。それでもドメインを復元する場合は、料金を書き留めておきます。この名前は後のステップで必要になります。
3. ドメインが登録された AWS アカウントを使用して、 AWS サポートセンターにサインインします。
4. 次の値を指定します。

   内容

   デフォルト値の [アカウントと請求] をそのまま使用します。

   サービス

   デフォルト値の [ドメイン] をそのまま使用します。

   Category

   デフォルト値の [復元] をそのまま使用します。

   緊急度

   デフォルト値の [一般的な質問] をそのまま使用します。

   [次のステップ: 追加情報] を選択します。

   件名

   [Restore an expired domain (失効したドメインの復元)] または [Restore a deleted domain (削除されたドメインの復元)] を選択します。

   説明

   以下の情報を記述します。

   - 復元するドメイン
   - ドメインが登録されたアカウントの 12 桁のアカウント ID AWS
   - ドメイン復元の料金に同意することの確認。以下のテキストを使用します。

     「ドメインを復元するための ____ USD の料金に同意します。」

空白を、ステップ 2 で確認した料金に置き換えます。

連絡方法

連絡方法を指定し、適切な値を入力します。

5. [Submit] を選択してください。
6. AWS サポートがドメインを復元できるかどうかを決定すると、担当者から連絡があります。さらに、Route 53 がドメインを復元すると、ドメインがコンソールに再表示されます。有効期限は、ドメインの有効期限が切れたか、誤って削除されたかによって異なります。

   ドメインの有効期限が切れた

   新しい有効期限は通常、古い有効期限の 1 年後または 2 年後 (TLD によって異なります) です。

   > **Note**
   > 新しい有効期限は、ドメインが復元された日付から起算されません。

   ドメインが誤って削除された

   通常、有効期限は変更されません。

Route 53 に登録されているドメインのホストゾーンの置き換え

ドメインのホストゾーンを削除する場合、ドメインをインターネットで利用する準備ができたときに、別のホストゾーンを作成する必要があります。以下の手順を実行します。

ドメインのホストゾーンを置き換えるには

1. パブリックホストゾーンを作成します。詳細については、「パブリックホストゾーンの作成」を参照してください
2. ホストゾーンにレコードを作成します。レコードは、ドメイン (example.com) とサブドメイン (acme.example.com、zenith.example.com) のトラフィックをどのようにルーティングするかを定義します。詳細については、「レコードを使用する」を参照してください

3. 新しいホストゾーンのネームサーバーを使用するようにドメイン設定を更新します。詳細については、「ドメインのネームサーバーおよびグルーレコードの追加あるいは変更」を参照してください

> **Important**
>
> ホストゾーンを作成する場合、Route 53 はホストゾーンに一連の 4 つのネームサーバーを割り当てます。ホストゾーンを削除して新しいゾーンを作成すると、Route 53 は他の一連のネームサーバー 4 つを割り当てます。通常、新しいホストゾーンのネームサーバーは、以前のホストゾーンのネームサーバーと一致しません。新しいホストゾーンのネームサーバーを使用するようにドメイン設定を更新しないと、ドメインはインターネット上で利用できなくなります。

4. ドメインのホストゾーンの置き換え中に問題が発生した場合は、 AWS サポートに無料でお問い合わせください。詳細については、「ドメイン登録の問題に関する AWS サポートへのお問い合わせ」を参照してください。

ドメインの移管

別のレジストラから Amazon Route 53 に、AWS アカウント間で、または Route 53 から別のレジストラに、ドメインの登録を移管できます。ある AWS アカウントから別のアカウントへのドメイン移管には、料金は発生しません。

このセクションのこのトピックでは、ドメイン移管に関連する以下のトピックについて説明します。

1. 移管タイプを選択する
   - Route 53 へのドメイン登録の移管と、DNS ホスティングのみに Route 53 を使用することの違いについて説明します。
   - ドメイン管理と DNS ホスティングの目標に基づき、ニーズに適したオプションについて説明します。
2. 移管前チェックリスト
   - 一般的な移管の失敗を避けるために、ドメインを Route 53 に移管する前に、重要な準備手順を完了してください。
   - ドメインの適格性を検証し、認可コードを取得し、スムーズな移管プロセスのために DNS 設定を準備します。
3. ドメイン登録の Amazon Route 53 への移管

- 前提条件、認可コード、DNS 設定の更新など、ドメインを別のレジストラから Route 53 に転送するステップバイステップの手順について説明します。
- ドメインの移管が、有効期限とさまざまな最上位ドメイン (TLD) の考慮事項にどのような影響を与えるかについて理解します。

4. 一般的な移管の問題
   - ドメインの要件、認可プロセス、タイミングに関する考慮事項を理解することで、一般的な移管の問題を回避します。
   - 移管の問題を解決する方法と、移管が遅延するか拒否された場合の対処方法について説明します。
5. Amazon Route 53 から別のレジストラへのドメインの移行
   - Route 53 から別のレジストラにドメインを移管するプロセスを理解します。これには、認可コードの取得、DNS 設定の更新、確認 E メールへの応答が含まれます。
   - DNS サービスを別のプロバイダーに移管するときの考慮事項と、エイリアスレコードやルーティングポリシーなどの Route 53 固有の機能に対する潜在的な影響に注意してください。
6. ドメインを別の AWS アカウントに転送する
   - 移管の開始と承諾に必要なロールとアクセス許可など、ドメインをある AWS アカウントから別のアカウントに移管する方法を説明します。
   - ドメインの移管後にホストゾーンを新しいアカウントに移行するオプションのステップについて説明します。
7. 移管ステータス
   - ドメイン移管リクエストのステータスと、移管プロセス中のさまざまなステータスコードの意味を表示する方法について説明します。
8. ドメインを Amazon Route 53 に移管するとドメイン登録の有効期限が受ける影響
   - Route 53 へのドメインの移管が、ドメインの有効期限にどのように影響する可能性があるかについて説明します。

上記のトピックに記載されている情報に従って、Route 53 との間でドメインを効果的に移管し、移管プロセスを管理し、適切な DNS 設定とルーティングを維持しながら確実に円滑な移管を行うことができます。

Route 53 移管タイプを選択する

ドメインで Amazon Route 53 を使用する場合は、2 つのオプションがあります。違いを理解することは、ニーズに合った適切なアプローチを選択するのに役立ちます。

ドメイン登録を Route 53 に移管する

このオプションでは、Route 53 がドメインレジストラになります。つまり、ドメインの更新、連絡先情報、DNS 設定はすべて Route 53 を通じて管理します。

次のような場合にこのオプションを選択してください。

- ドメイン管理と DNS ホスティングを 1 か所に統合する
- Route 53 ドメイン管理機能を活用する
- 請求書にドメインの更新を含めることで AWS 請求を簡素化する

予想されること:

- 完了までの時間: 5 ~ 7 日
- 前提条件: 現在のレジストラからの認可コード、ドメインのロック解除、登録者の E メールの確認
- 更新に対して支払うユーザー: Route 53

次のステップ: ドメイン移管の移管前チェックリスト を完了して移管の準備をします。

DNS ホスティングにのみ Route 53 を使用する

このオプションでは、現在のドメインレジストラは保持しますが、DNS サービスとして Route 53 を使用します。

次のような場合にこのオプションを選択してください。

- 既存のレジストラ関係を維持する
- レジストラを変更せずに Route 53 の高度な DNS 機能を使用する
- 最小限の前提条件ですぐに開始する

予想されること:

- 完了までの時間: 最大 2 日間 (DNS 伝達によって異なります)
- 前提条件: なし
- 更新のお支払い先: 現在のレジストラ

次のステップ: DNS サービスとしての Amazon Route 53 の設定 に進み、DNS ホスティングを設定します。

> **Important**
>
> Route 53 を DNS サービスとして使用するには、ドメイン登録を移管する必要はありません。既存のレジストラを保持し、DNS ホスティングにのみ Route 53 を使用できます。

ドメイン移管の移管前チェックリスト

Amazon Route 53 へのドメイン登録の移管を開始する前に、次のチェックを完了して、一般的な移管の失敗を回避し、スムーズなプロセスを確保してください。

移管する内容を決定する

ニーズに一致するオプションを選択します。

ドメイン登録を Route 53 に移管する

レジストラが Amazon Route 53 になります。ドメインの更新に対して Route 53 に支払いを行い、Route 53 コンソールを使用してドメイン設定を管理します。

次のステップ: このチェックリストを続行し、ドメイン登録の Amazon Route 53 への移管 に従います。

DNS ホスティングにのみ Route 53 を使用する

現在のレジストラは維持しますが、DNS 解決には Route 53 ネームサーバーを使用します。更新に対して現在のレジストラに引き続き支払います。

次のステップ: このチェックリストをスキップし、DNS サービスとしての Amazon Route 53 の設定 に従います。

前提条件チェックリスト

ドメイン移管を開始する前に、以下のすべてを完了してください。

移管前チェックリスト (すべての項目を完了)

1. □ 登録者の E メールアクセスを確認する

ドメイン移管承認 E メールを受信するため、登録者の E メールアドレスで E メールを受信できることを確認します。

> **Important**
>
> 現在の登録者の E メールアドレスにアクセスできない場合は、現在のレジストラで登録者の連絡先 E メールアドレスを更新し、移管されるまで 60 日間待ちます。

2. □ ドメインのロックを解除する

   現在のレジストラドメイン設定にアクセスし、「ドメインロック」または「移管ロック」保護が有効になっている場合は無効にします。

   > **Note**
   >
   > ロックを無効にしたら、変更が有効になるまで数分待ってから移管を開始します。

3. □ 認可コードを取得する

   現在のレジストラに認可コード (認証コード) をリクエストし、その機密性を維持します。このコードはこの移管プロセスで後から Route 53 コンソールに入力します。

4. □ ドメインの経過時間と適格性を確認する

   ドメインが ICANN 移管要件を満たしていることを確認します。

   - ドメインは、初回登録から 60 日以上経過している必要があります。
   - ドメイン登録の有効期限が切れて、復元した場合は、復元後、少なくとも 60 日間が経過している必要があります。

   > **Tip**
   >
   > 登録者の連絡先の詳細が最近更新された場合 (名前や E メールの変更など)、ICANN ルールによって転送が一時的にブロックされる場合があります。一部のレジストラでは、この保留をオプトアウトできます。不明な場合は、現在のレジストラに確認してください。

5. □ 支払い方法を準備する

AWS アカウントに有効な支払い方法があることを確認します。ドメインを Route 53 に移管する場合、 AWS アカウントに適用される移管料金は最上位ドメインによって異なります。

現在の料金については、「Route 53 料金表」を参照してください。

> **Note**
>
> AWS クレジットを使用してドメイン移管の支払いを行うことはできません。Route 53 は、プロセスを開始する前に移管料金を請求し、移管が失敗した場合はすぐに返金します。

6. □ DNSSEC を無効にする (有効になっている場合)

現在のレジストラで DNSSEC が現在有効になっている場合は、移管を開始する前に一時的に無効にします。これにより、DNS 検証の問題なしで移管を完了できます。

DNSSEC の無効化が重要である理由:

ドメインを移管する場合、現在のレジストラに保存されている DNSSEC キー (KSK/ZSK) と DS レコードは自動的に Route 53 に移管されません。Route 53 でこれらのキーを再設定せずに DNSSEC を再度有効にすると、ドメインが DNS 検証に失敗する可能性があります。

安全なアプローチ (推奨):

1. 移管を開始する前に、現在のレジストラで DNSSEC を無効にします。
2. ドメイン移管を完了し、Route 53 ホストゾーンを作成します (まだ作成されていない場合) 。
3. DNSSEC を有効にせずに、すべての DNS レコードが正しく解決されていることを確認します。
4. ホストゾーンの新しい KSK/ZSK 値を使用して Route 53 で DNSSEC を設定します。
5. TLD レジストラ (現在の Route 53) で新しい DS レコードを発行することで、DNSSEC を再度有効にします。

> **Tip**
>
> Route 53 で新しいホストゾーンを作成すると同時にドメインを移管する場合は、移管する前に DNSSEC を無効にし、ホストゾーンの設定が確認され、DNS 解決が正しく機能

するまで待ちます。これを確認したら、Route 53 コンソールから DNSSEC を再度安全に有効にできます。DNSSEC を再度有効にする前に、Route 53 で DNS 設定を必ず確認してください。Route 53 における DNSSEC の詳細については、「ドメインの DNSSEC の設定」を参照してください。

オプション: 最初に DNS サービスを移管する

ドメイン登録を移管する前に、DNS サービスを Route 53 に移管することを検討してください。このアプローチには以下の利点があります。

- 移管中のウェブサイトまたは E メールのダウンタイムのリスクを軽減できます
- フル移管にコミットする前に Route 53 DNS 機能をテストできます
- ドメイン移管で問題が発生した場合にフォールバックオプションを提供します

最初に DNS サービスを移管するには、「DNS サービスとしての Amazon Route 53 の設定」を参照してください。

次の手順

このチェックリストを完了した後:

1. 「ドメイン登録の Amazon Route 53 への移管」のステップバイステップの移管プロセスに従います。
2. 移管プロセス中に承認メッセージがないか E メールをモニタリングします。

ドメイン登録の Amazon Route 53 への移管

Important

.cc と .tv を除くすべての国コードトップレベルドメイン (ccTLD) を Route 53 に移管する場合、所有者連絡先の更新は行われず、レジストリの所有者連絡先データが使用されます。移管が完了すると、連絡先情報を更新できます。詳細については、「ドメインの連絡先情報と所有者の更新」を参照してください。

ドメイン登録を Amazon Route 53 へ移管するには、このトピックの手順に従います。

移管プロセスの概要

ドメイン移管には、以下の主要なステップが含まれます。

1. 移管前チェックリストを完了する

   移管の失敗を避けるため、前提条件を確認します。「ドメイン移管の移管前チェックリスト」を参照してください。
2. Route 53 コンソールでの移管をリクエストする

   ドメイン名と認可コードを入力します。「ステップ 5: 移管をリクエストする」を参照してください。
3. E メールで承認する (顧客のアクションが必要)

   5 日以内に登録者の E メールに送信された承認リンクをクリックします。「ステップ 6: 確認と承認 E メールのリンクをクリックする」を参照してください。
4. 完了まで待機する

   現在のレジストラによって拒否されない限り、移管は自動的に完了します。コンソールでステータスをモニタリングします。

最も一般的な障害ポイント

一般的な問題の解決策を次に示します。

- E メールが受信されない: 登録者の E メールにアクセスできることを確認し、スパムフォルダを確認します。
- ドメインロック: 移管を開始する前に現在のレジストラでロック解除します。
- 無効な認証コード: 現在のレジストラに新しい認可コードをリクエストします。
- 60 日間のルール違反: 60 日間の ICANN ルール (資格ウィンドウ) 。移管は、初回登録または登録者の連絡先の変更から 60 日以内にブロックされます。一部のレジストラは、変更前にオプトアウトを許可しています。該当する場合は、現在のレジストラに質問してください。

> **Important**
>
> 手順をスキップすると、お客様のドメインはインターネットで使用できなくなる可能性があります。

次の点に注意してください。

AWS サポートへのお問い合わせ

ドメインの転送中に問題が発生した場合は、 AWS Support に無料でお問い合わせください。詳細については、「ドメイン登録の問題に関する AWS サポートへのお問い合わせ」を参照してください

有効期限日

ドメインの移管が現在の有効期限に及ぼす影響については、「ドメインを Amazon Route 53 に移管するとドメイン登録の有効期限が受ける影響」を参照してください。

移管料金

ドメインを Route 53 に移管する場合、 AWS お客様のアカウントに適用される移管料金は、.com や .org などの最上位ドメインによって異なります。詳細については、「Route 53 料金表」を参照してください。

AWS クレジットを使用して、Route 53 にドメインを移管するための料金を支払うことはできません。

> **Note**
>
> Route 53 は、移管プロセスを開始する前に、ドメインの移管に対して料金を請求します。何らかの理由で移管が失敗した場合は、直ちにお客様のアカウントに移管の費用を返却します。

特別なドメイン名とプレミアムドメイン名

TLD レジストリでは、一部のドメイン名に対して特別料金またはプレミアム料金を設定しています。ドメインに特別料金またはプレミアム料金が設定されている場合、ドメインを Route 53 に転送することはできません。

ドメインクォータ

AWS アカウントあたりのデフォルトのドメインの最大数は 20 です。クォータによる上限の引き上げをリクエストできます。詳細については、「ドメインのクォータ」を参照してください。

ネームサーバーの制限

Route 53 のドメインあたりの最大ネームサーバー数は 6 です。

トピック

- 最上位ドメインの移管に関する要件
- ステップ 1: Amazon Route 53 で最上位ドメインがサポートされていることを確認する
- ステップ 2 (オプション): DNS サービスを Amazon Route 53 または別の DNS サービスプロバイダーに移管する
- ステップ 3: 現在のレジストラで設定を変更する
- ステップ 4: ネームサーバーの名前を取得する
- ステップ 5: 移管をリクエストする
- ステップ 6: 確認と承認 E メールのリンクをクリックする
- ステップ 7: ドメイン設定を更新する

最上位ドメインの移管に関する要件

ほとんどのドメインレジストラは、他のレジストラへのドメインの移管について要件を設定しています。これらの要件の主な目的は、不正なドメインの所有者が、別のレジストラにドメインを繰り返し移管するのを防ぐことです。要件は異なりますが、以下の要件が一般的です。

- 少なくとも 60 日前にドメインを登録または現在のレジストラに移管している必要があります。
- ドメイン名登録の有効期限が切れて、復元する必要があった場合は、復元後、少なくとも 60 日間が経過している必要があります。
- ドメインのドメイン名ステータスコードが以下のいずれかであってはいけません。
  - clientTransferProhibited
  - pendingDelete
  - pendingTransfer
  - redemptionPeriod
  - serverTransferProhibited
- 一部の最上位ドメインのレジストリは、ドメインの所有者の変更などの変更が完了するまで、移管を許可しません。

ドメイン名のステータスコードと各コードの意味を記した最新のリストは、ICANN のウェブサイトで EPP のステータスコードを検索すると確認できます。(ICANN ウェブサイトで直接、検索してください。ウェブ検索ではドキュメントの古いバージョンが返されることがあります)。

> **Note**
>
> ICANN は、ドメイン名の登録と移管を管理するポリシーを定めている組織です。

Whois のウェブサイトでご自分のドメイン名を検索し、ドメインのステータスコードやその他の情報を確認することもできます。

ステップ 1: Amazon Route 53 で最上位ドメインがサポートされていることを確認する

「Amazon Route 53 に登録できる最上位ドメイン」を参照してください。移管するドメインの最上位ドメインがリストにある場合は、そのドメインを Amazon Route 53 に移管できます。

その TLD がリストにない場合は、現在そのドメイン登録を Route 53 に移管することはできません。その他の TLD がリストに追加される場合があるため、お客様のドメインのサポートが追加されているかどうかを再確認してください。

ステップ 2 (オプション): DNS サービスを Amazon Route 53 または別の DNS サービスプロバイダーに移管する

DNS を最初に移管する理由

一部のレジストラは無料の DNS サービスを提供していますが、Route 53 からドメイン登録の移管リクエストを受け取ると、すぐに無効となってしまうものがあります。Route 53 でドメインの DNS サービスを提供する場合は、Amazon Route 53 を既存ドメインの DNS サービスとして使用する をご覧ください。

ステップ 3: 現在のレジストラで設定を変更する

現在のレジストラが用意している方法を使用して、移管する各ドメインについて次のいずれかを実行します。

- 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)

ドメインの登録者の連絡先が最新であることを確認する

当社は登録者の連絡先の E メールアドレスに E メールを送信して、移管の承認をリクエストします。転送を承認するには、E メール内のリンクを選択する必要があります。リンクを選択しない場合は、転送をキャンセルする必要があります。

> **Important**
>
> 登録者として登録した連絡先には、ICANN 移転ポリシーに基づき、ドメイン名の登録名保有者としての特定の権利があります。ほとんどのドメインは、 の閉鎖時に削除されます AWS アカウント (詳細については、「」を参照してくださいAWS アカウントが閉鎖または完全に閉鎖され、ドメインが Route 53 に登録されている)。ただし、ドメインが閉鎖されたアカウントに残っている場合、登録者としてリストした連絡先は、外部レジストラへのドメイン名の移管をリクエストできる場合があります。したがって、リストに記載する登録者の連絡先は、自分または責任を持って行動できる別の信頼できる人物であることが重要です。

移管可能にするためにドメインのロックを解除する

ドメイン登録の管理組織である ICANN の要件に従って、ドメインを移管する前にドメインのロックを解除する必要があります。

ドメインのステータスが移管可能であることを確認する

詳細については、「最上位ドメインの移管に関する要件」を参照してください。

ドメインの DNSSEC を無効にします

ドメインで DNSSEC を使用し、ドメイン登録を Route 53 に移管する場合は、移管する前に現在のレジストラでドメインの DS レコードを削除する必要があります。DS レコードを削除したら、変更が反映されるまで少なくとも 24 時間待ってから転送を続行します。次に、ドメイン登録を移管した後、Route 53 でドメインの DNSSEC を設定できます。Route 53 では、ドメイン登録と DNSSEC 署名で、DNSSEC がサポートされています。詳細については、「Amazon Route 53 での DNSSEC 署名の設定」を参照してください。

> **Important**
>
> DNSSEC が設定されている場合にドメイン登録を Route 53 に移管すると、DNSSEC パブリックキーも移管されます。DNSSEC をサポートしていないプロバイダーに DNS

サービスを 移管する場合、ドメインから DNSSEC キーを削除するまで DNS 解決が断続的に失敗します。詳細については、「ドメインのパブリックキーの削除」を参照してください。

認可コードを取得する

Route 53 へのドメイン登録の移管をリクエストするには、現在のレジストラから認可コードを取得する必要があります。このコードは後で Route 53 コンソールに入力します。

一部の最上位ドメインには、以下の追加の要件があります。

.co.za のドメイン

.co.za ドメインを Route 53 に移管するために認可コードを取得する必要はありません。

.uk、.co.uk、.me.uk、.org.uk のドメイン

.uk、.co.uk、.me.uk、または .org.uk ドメインを Route 53 に移管する場合は、認可コードを取得する必要はありません。代わりに、現在のドメインレジストラが用意している方法を使って、ドメインの IPS タグの値を GANDI (すべて大文字) に更新します (IPS タグは .uk ドメイン名のレジストリである Nominet が必要としています)。レジストラが IPS タグの値を変更する方法を提供していない場合は、Nominet にお問い合わせください。

IPS タグの変更に関する以下の点に注意してください。

5 日以内に移管をリクエストする必要があります

IPS タグを変更してから 5 日以内に移管をリクエストしない場合、タグは以前の値に戻ります。IPS タグの値を再度変更する必要があります。変更しないと、移管のリクエストは失敗します。

WHOIS クエリでの IPS タグの表示

IPS タグへの変更は、Route 53 への転送が完了するまで WHOIS クエリに表示されません。

Gandi からの E メール

レジストラアソシエイトである Gandi から、移管プロセスに関するメールが届く場合があります。Gandi (transfer-auth@gandi.net) からドメインの移管に関する E メールを受け取った場合は、E メールの指示は無視してください。これ

は、.uk、.co.uk、.me.uk、.org.uk ドメインに関連しないためです。代わりに、このトピックの手順に従ってください。

ドメイン (一部の地理的 TLD) を移管する前にドメイン登録を更新します

ほとんどの TLD では、ドメインを移管すると、登録は自動的に 1 年延長されます。ただし、一部の地理的 TLD では、ドメインを移管しても登録は延長されません。これらのいずれかの TDL を持つ Route 53 にドメインを移管する場合は、移管前にドメイン登録を更新することをお勧めします (特に、有効期限が近づいている場合)。

> **Important**
>
> 移管前にドメインを更新しなかった場合、移管が完了する前に、登録が期限切れになる可能性があります。この場合、ドメインはインターネットで使用できなくなり、他者がそのドメイン名を購入できるようになる可能性があります。

次のドメインを別のレジストラに移管するときは、登録は自動的に延長されません。

- .ch (スイス)
- .cl (チリ)
- .co.uk (英国)
- .co.za (南アフリカ)
- .com.au (オーストラリア)
- .cz (チェコ共和国)
- .es (スペイン)
- .fi (フィンランド)
- .im (マン島)
- .jp (日本)
- .me.uk (英国)
- .net.au (オーストラリア)
- .org.uk (英国)
- .se (スウェーデン)
- .uk (英国)

ステップ 4: ネームサーバーの名前を取得する

Amazon Route 53 を DNS サービスとして使用しているか、既存の DNS サービスを継続して使用している場合は、プロセスの後で自動的にネームサーバーの名前が取得されます。「ステップ 5: 移管をリクエストする」へ進んでください。

ドメインを Route 53 に移管するのと同時に、DNS サービスを Route 53 以外のプロバイダに変更する場合は、DNS サービスプロバイダが用意している手順に従って、移管する各ドメインのネームサーバーの名前を取得します。

> **Important**
>
> ドメインのレジストラがドメインの DNS サービスプロバイダーでもある場合は、ドメイン登録の移管プロセスを続行する前に、DNS サービスを Route 53 または別の DNS サービスプロバイダーに移管します。
> ドメイン登録を移管するのと同時に DNS サービスを移管する場合、ドメインに関連付けられたウェブサイト、E メール、およびウェブアプリケーションは利用できなくなることがあります。詳細については、「ステップ 2 (オプション): DNS サービスを Amazon Route 53 または別の DNS サービスプロバイダーに移管する」を参照してください。

ステップ 5: 移管をリクエストする

現在のレジストラから Amazon Route 53 にドメイン登録を移管するには、Route 53 コンソールを使用して移管をリクエストします。Route 53 は、ドメインの現在のレジストラとの通信を処理します。

コンソールを使用してドメインを 5 つまで移管できます。

使用する手順は、移管するドメインの数 (1 つ、または 5 つまで) に応じて異なります。

- 1 つのドメインのドメイン登録を Route 53 に移管するには
- 最大 5 つのドメインのドメイン登録を Route 53 に移管するには

1 つのドメインをアカウントに移管するときは、[ドメインをアカウントに移管する] のプロセスを使用します。

1 つのドメインのドメイン登録を Route 53 に移管するには

1. Route 53 コンソール (https://console.aws.amazon.com/route53/) を開きます。

2. ナビゲーションペインで [Registered Domains] をクリックします。
3. [登録済みドメイン] のページで、[移管 (イン)] ドロップダウンから [単一のドメイン] を選択します。
4. [ドメインをアカウントに移管する] ページの [ドメイン移管可否の確認] セクションに、登録を Route 53 に移管させるドメインの名前を入力し、[チェック] をクリックします。
5. ドメイン登録が移管可能である場合は、最上位のドメインの移管要件が満たされていることを確認し、[次へ] をクリックします。

   ドメイン登録が移管できない場合は、Route 53 コンソールに理由が表示されます。登録の移管を妨げている問題の解決方法については、レジストラにお問い合わせください。
6. [DNS サービス] のページで、ネームサーバーの情報を確認し、[次へ] をクリックします。
7. 画面で指示されたら、現在のレジストラから取得した認可コードまたは IPS タグを ステップ 3: 現在のレジストラで設定を変更する に入力します。

   > **Note**
   >
   > .co.za、.uk、.co.uk、.me.uk、または .org.uk ドメインを Route 53 に移管するために認可コードを入力する必要はありません。

   [次へ] を選択します。
8. [ドメインの料金オプション] ページで、移管するドメインを登録する年数と、有効期限が切れる前にドメイン登録を自動更新するかどうかを選択します。

   > **Note**
   >
   > ドメイン名の登録および更新は返金の対象外です。ドメインの自動更新を有効にし、登録更新後にドメイン名が必要なくなった場合、更新費用の返金を受け取ることはできません。

   [次へ] を選択します。
9. [連絡先情報] ページで、ドメインの登録者、管理者、技術担当者、請求の連絡先情報を入力します。ここで入力した値は、登録しようとしているすべてのドメインに適用されます。詳細については、「ドメインを登録または移管するときに指定する値」を参照してください

以下の考慮事項に注意してください。

First Name (名) と Last Name (姓)

[First Name] と [Last Name] は、公式 ID に名前を指定することをお勧めします。ドメイン設定の変更に際しては、一部のドメインレジストリで、身分証明書の提供が求められる場合があります。お客様の ID の名前は、ドメイン登録者の連絡先の名前と完全に一致する必要があります。

他の連絡先

デフォルトでは、3 種類の連絡先すべてについて同じ情報が使用されます。1 つまたは複数の連絡先で異なる情報を入力するときは、それぞれの連絡先について [登録者の連絡先と同じ] の値をオフの位置にします。

> **Note**
>
> .it ドメインの場合、登録者と管理者の連絡先は同じである必要があります。

その他の必須情報

一部の最上位ドメイン (TLD) では追加情報を収集する必要があります。そのような TLD の場合は、[Postal/Zip Code] の後に、該当する値を入力します。

プライバシー保護

WHOIS クエリに対して連絡先情報を非表示にするかどうかを選択します。

> **Note**
>
> 管理担当者、登録者、技術担当者には、同じプライバシー設定を指定する必要があります。

詳細については、以下の各トピックを参照してください。

- ドメインの連絡先情報のプライバシー保護の有効化/無効化
- Amazon Route 53 に登録できる最上位ドメイン

> **Note**
>
> .uk、.co.uk、.me.uk、.org.uk ドメインのプライバシー保護を有効にするには、サポートケースを開いてプライバシー保護をリクエストします。

[次へ] を選択します。

10. [確認] ページで、入力した情報を確認し、必要に応じて修正します。サービスの利用規約を読み、読んだことを確認するチェックボックスをオンにします。

    [Submit request (リクエストの送信)] を選択します。

11. ナビゲーションペインで [ドメイン] を選択し、次に [リクエスト] を選択します。

    このページではドメインのステータスを確認できます。また、登録者の連絡先確認メールに、返信する必要があるかどうかも確認できます。確認メールは再送信することも可能です。

    Route 53 でのドメインの登録に使用されたことがない登録者の連絡先の E メールアドレスを指定した場合、一部の TLD レジストリでは、アドレスが有効であることを確認する必要があります。

    以下のいずれかの E メールアドレスより、確認 E メールが送信されます。

    - noreply@registrar.amazon – Amazon Registrar によって登録された TLDs 用。
    - noreply@domainnameverification.net または noreply@emailverification.info – 当社のレジストラアソシエイトである Gandi によって登録された TLDs の場合。TLD のレジストラを調べる方法については、「レジストラの検索」を参照してください。

> **Important**
>
> 登録者は、E メールの指示に従って、メールを受信したことを確認する必要があります。これを行わない場合、お客様のドメインは ICANN の規定に従って停止されます。ドメインが停止されると、インターネットでそのドメインにアクセスできなくなります。

a. 確認 E メールを受け取ったら、E メール内のリンクを選択し、指定した E メールアドレスが有効であることを確認します。E メールがすぐに届かない場合は、迷惑メールフォルダーを確認します。

b. [リクエスト] ページに戻ります。ステータスが自動的に [email-address is verified (E メールアドレスが検証されました)] に更新されない場合は、[ステータスの更新] を選択します。

12. ドメインの移管が完了したら、ドメインの DNS サービスとして Route 53 を使用するか他の DNS サービスを使用するかによって、次のステップは異なります。

- Route 53: ドメイン登録時に Route 53 が作成したホストゾーンで、ドメインおよびサブドメインへのトラフィックをどのようにルーティングするかを Route 53 に指示するためのレコードを作成します。

  例えば、誰かがブラウザにドメイン名を入力し、そのクエリが Route 53 に転送されたときに、Route 53 がそのクエリに対してお客様のデータセンターにあるウェブサーバーの IP アドレスを返すか、それとも Elastic Load Balancing ロードバランサーの名前を返すかを指定します。

  詳細については、「レコードを使用する」を参照してください。

  > **Important**
  >
  > Route 53 が自動的に作成するもの以外のホストゾーンでレコードを作成した場合、ドメインのネームサーバーを更新して新しいホストゾーンのネームサーバーを使用する必要があります。

- 他の DNS サービス - 他の DNS サービスに DNS クエリをルーティングするように新しいドメインを設定します。ネームサーバーを更新して別のレジストラを使用するの手順を実行します。

5 つまでのドメインをアカウントに移管するときは、次の方法に従います。

最大 5 つのドメインのドメイン登録を Route 53 に移管するには

1. Route 53 コンソール (https://console.aws.amazon.com/route53/) を開きます。
2. ナビゲーションペインで [Registered Domains] をクリックします。

3. [登録済みドメイン] のページで、[移管 (イン)] ドロップダウンから [複数のドメイン] を選択します。
4. [複数のドメインをアカウントに移管] ページで、移管するドメインを最大で 5 つ入力し、必要に応じて認可コードを 1 行ずつ入力して、[チェック] を選択します。
5. 移管にドメイン登録を使用できる場合は、[ドメインの可用性] リストに使用可能として表示されます。登録を移管するドメインの横にあるチェックボックスを選択し、最上位のドメインの移管要件が満たされていることを確認して、[次へ] をクリックします。

   ドメイン登録が移管できない場合は、Route 53 コンソールに理由が表示されます。登録の移管を妨げている問題の解決方法については、レジストラにお問い合わせください。
6. [DNS サービス] のページで、ネームサーバーの情報を確認し、[次へ] をクリックします。

> **Note**
>
> ドメイン名の登録と更新は、返金の対象外です。ドメインの自動更新を有効にし、登録更新後にドメイン名が必要なくなった場合、更新費用の返金を受け取ることはできません。

7. [連絡先情報] ページで、ドメインの登録者、管理者、技術担当者の連絡先情報を入力します。ここで入力した値は、移管しようとしているすべてのドメインに適用されます。

> **Important**
>
> 登録者の連絡先 (ドメイン所有者) には、次の値を指定することをお勧めします。
>
> - 姓名: 公式 ID に表示される名前を指定することをお勧めします。ドメイン設定の変更に際しては、一部のドメインレジストリで、身分証明書の提供が求められる場合があります。お客様の ID の名前は、ドメイン登録者の連絡先の名前と完全に一致する必要があります。
> - 連絡先の詳細: ドメインの移管時は、現在のレジストラで指定した値と同じ値を指定することをお勧めします。登録者の連絡先の連絡先詳細を変更するときは、ドメインの所有者を変更します。TLD レジストリによっては、ドメインの移管時にドメインの所有者を変更できません。登録者の連絡先の連絡先詳細を変更すると、移管に失敗することがあります。ドメインを移管した後、登録者の連絡先の連絡先詳細を変更できます。

デフォルトでは、3 種類の連絡先すべてについて同じ情報が使用されます。1 つまたは複数の連絡先で異なる情報を入力するときは、[登録者の連絡先と同じ] の値をオフの位置にします。

> **Note**
>
> .it ドメインの場合、登録者と管理者の連絡先は同じである必要があります。

詳細については、「ドメインを登録または移管するときに指定する値」を参照してください。

8. 一部の TLD では、追加情報を収集する必要があります。そのような TLD の場合は、[Postal/Zip Code] の後に、該当する値を入力します。
9. [Contact Type] の値が [Person] の場合、WHOIS クエリに対して連絡先情報を非表示にするかどうかを選択します。詳細については、「ドメインの連絡先情報のプライバシー保護の有効化/無効化」を参照してください。
10. [Submit] を選択してください。
11. 入力した情報を確認し、サービスの利用規約を読み、利用規約を読んだことを確認するチェックボックスをオンにします。
12. [Submit request (リクエストの送信)] を選択します。

    ドメインが移管可能であることが確認されると、ドメイン移管の承認を求める E メールが、そのドメインの登録者の連絡先に送信されます。
13. ナビゲーションペインで [ドメイン] を選択し、次に [リクエスト] を選択します。

    このページではドメインのステータスが確認できます。また、登録者の連絡先確認メールに、返信する必要があるかどうかも確認できます。確認メールは再送信することも可能です。

    Route 53 でのドメインの登録に使用されたことがない登録者の連絡先の E メールアドレスを指定した場合、一部の TLD レジストリでは、アドレスが有効であることを確認する必要があります。

    以下のいずれかの E メールアドレスより、確認 E メールが送信されます。

    - noreply@registrar.amazon – Amazon Registrar によって登録された TLDs 用。
    - noreply@domainnameverification.net または noreply@emailverification.info – 当社のレジストラアソシエイトである Gandi によって登録された TLDs の場合。TLD のレジストラを調べる方法については、「レジストラの検索」を参照してください。

> **Important**
>
> 登録者は、E メールの指示に従って、メールを受信したことを確認する必要があります。これを行わない場合、お客様のドメインは ICANN の規定に従って停止されます。ドメインが停止されると、インターネットでそのドメインにアクセスできなくなります。

a. 確認 E メールを受け取ったら、E メール内のリンクを選択し、指定した E メールアドレスが有効であることを確認します。E メールがすぐに届かない場合は、迷惑メールフォルダーを確認します。

b. [リクエスト] ページに戻ります。ステータスが自動的に [email-address is verified (E メールアドレスが検証されました)] に更新されない場合は、[ステータスの更新] を選択します。

14. ドメインの移管が完了したら、ドメインの DNS サービスとして Route 53 を使用するか他の DNS サービスを使用するかによって、次のステップは異なります。

- Route 53: ドメイン登録時に Route 53 が作成したホストゾーンで、ドメインおよびサブドメインへのトラフィックをどのようにルーティングするかを Route 53 に指示するためのレコードを作成します。

  例えば、誰かがブラウザにドメイン名を入力し、そのクエリが Route 53 に転送されたときに、Route 53 がそのクエリに対してお客様のデータセンターのウェブサーバーの IP アドレスを返すか、それとも ELB ロードバランサーの名前を返すかを指定します。

  詳細については、「レコードを使用する」を参照してください

  > **Important**
  >
  > Route 53 が自動的に作成するもの以外のホストゾーンでレコードを作成した場合、ドメインのネームサーバーを更新して新しいホストゾーンのネームサーバーを使用する必要があります。

- 他の DNS サービス - 他の DNS サービスに DNS クエリをルーティングするように新しいドメインを設定します。ネームサーバーを更新して別のレジストラを使用するの手順を実行します。

ステップ 6: 確認と承認 E メールのリンクをクリックする

移管をリクエストするとすぐに、1 つ以上の E メールがドメイン登録者の連絡先に送信されます。

登録者の連絡先に到達可能であることを確認する E メール

Route 53 にドメインを登録したことがない場合、またはドメインを Route 53 に移管したことがない場合、E メールが有効であることを確認する E メールが送信されます。この情報は保持されるので、この確認メールを再度送信する必要はありません。

E メールでドメインを移管する承認を得る

一部の TLD では、ドメインの移管を承認するために E メールに応答する必要があります。

.com、.net、.org などの一般的な TLD

.com、.net、.org などの汎用 TLD を持つドメインには認可は必要ありません。

.co.uk や .jp などの地理的 TLD

地域別 TLD を持つドメインの場合、ドメインの移管に対する承認が必要になります。10 個のドメインを移管する場合は、10 個の E メールを送信する必要があり、それぞれで認可リンクを選択する必要があります。

E メールはすべてドメインの登録者の連絡先に送信されます。

- お客様がドメインの登録者の連絡先の場合は、メールの指示に従って移管を承認します。
- お客様以外の人が登録者の連絡先である場合は、その人に E メールの指示に従って移管を承認するように依頼します。

> **Important**
>
> 地域別 TLD を持つドメインを移管する場合、レジストラに対し、移管の承認を得るための連絡を実行するよう最大 5 日間の時間が与えられます。5 日間以内に登録者の連絡先から返信がない場合、移管処理はキャンセルされ、キャンセルを通知するメールが登録者の連絡先に送信されます。

トピック

- 新しい所有者または E メールアドレス用の承認 E メール
- 承認メールの発信元となるメールアドレス

- 現在のレジストラからの承認
- 次に起こること

新しい所有者または E メールアドレス用の承認 E メール

以下の値を変更する場合、承認を求める別の E メールが送信されます。

ドメイン所有者

「ドメインの所有権の変更をトリガーするものは何ですか?」で説明するようにドメインの所有者を変更する場合、ドメインの登録者連絡先に E メールが送信されます。

登録者の連絡用 E メールアドレス (一部の TLD に対してのみ)

一部の TLD では、登録者の連絡先 E メールアドレスを変更した場合、通知メールは登録者の連絡先として指定された古い E メールアドレスと新しい E メールアドレスの両方に送信されます。どちらかの E メールアドレスの担当者によって、この E メールの指示に従った変更の承認をする必要があります。

ドメイン所有者または登録者の連絡先の E メールアドレスの変更について、最上位ドメインに応じて 3 ~ 15 日以内に変更の認可を受け取らなかった場合、変更リクエストをキャンセルすることがあります。

承認メールの発信元となるメールアドレス

メールはすべて次のメールアドレスの 1 つから送信されます。

TLD	許可メールの発信元となるメールアドレス
.com.au と .net.au	以下のいずれかの E メールアドレス: • no-reply@ispapi.net (http://transfers.ispapi.net へのリンクを含む) • icann-transfers@key-systems.net
.fr	

TLD	許可メールの発信元となるメールアドレス
	nic@nic.fr: ドメインを移管するときに、.fr ドメイン名の登録者の連絡先を変更する場合。(E メールは現在の登録者の連絡先と新しい登録者の連絡先の両方に送信されます。)
その他すべて	以下のいずれかの E メールアドレス: • noreply@registrar.amazon • noreply@domainnameverification.net • noreply@emailverification.info • icann-transfers@key-systems.net

TLD のレジストラを調べる方法については、「Amazon Route 53 に登録できる最上位ドメイン」を参照してください。

現在のレジストラからの承認

登録者の連絡先が移管を承認すると、当社は現在のレジストラと共にドメインの移管処理を開始します。このステップは、ドメインの TLD に応じて最大 10 日かかる場合があります。

- 汎用最上位ドメイン - 最大 7 日かかります
- 地理的最上位ドメイン (国コードの最上位ドメインとも呼ばれます) 最大 10 日かかります

現在のレジストラが移管リクエストに応答しない場合 (これはレジストラではよくあることです)、移管は自動的に実行されます。現在のレジストラが移管リクエストを拒否した場合、現在の登録者の連絡先にメール通知が送信されます。登録者は現在のレジストラに連絡し、移管の問題を解決する必要があります。

次に起こること

ドメインの移管が承認されると、登録者の連絡先に別のメールが送信されます。プロセスの詳細については、「ドメイン移管のステータスの表示」を参照してください。

移管が完了するとすぐに、ドメイン移管に対して AWS アカウントに課金されます。TLD 別の料金の一覧については、「Amazon Route 53 のドメイン登録価格」を参照してください。

> **Note**
>
> これは 1 回限りの料金であるため、CloudWatch 請求メトリクスには表示されません。CloudWatch メトリクスの詳細については、Amazon CloudWatch ユーザーガイドの「Amazon CloudWatch メトリクスの使用」を参照してください。

ステップ 7: ドメイン設定を更新する

移管が完了したら、必要に応じて、以下の設定を変更できます。

[Transfer lock]

ドメインを Route 53 に移管するには、移管のロックを無効にする必要がありました。不正な移管を防ぐためにロックを再び有効にする場合は、「別のレジストラへの許可のない移管を防ぐためのドメインのロック」を参照してください。

自動更新

有効期限が近づくと自動的に更新されるように、移管したドメインを設定します。この設定を変更する方法については、「ドメインの自動更新の有効化/無効化」を参照してください。

延長登録期間

デフォルトでは、Route 53 はドメインを毎年更新します。ドメインを長期間登録する場合は、「ドメインの登録期間の延長」を参照してください。

DNSSEC

ドメイン用の DNSSEC の設定については、「ドメインの DNSSEC の設定」を参照してください。

Route 53 の一般的な移管問題の防止

ドメイン移管の進行中に問題が発生した場合、最も一般的な問題とその解決方法は次のとおりです。

> **Note**
>
> 移管がすでに失敗している場合は、障害後のトラブルシューティングについては、「マイドメインを Amazon Route 53 に移管できませんでした」を参照してください。

認可 E メールが届いていません

Route 53 から認可 E メールが届かない場合は、最も一般的な原因と解決策を次に示します。

- スパムフォルダを確認する - 認可 E メールは、E メールプロバイダーによってフィルタリングされる場合があります。
- E メールアドレスを確認する - ドメインの連絡先情報の登録者の E メールアドレスが最新でアクセス可能であることを確認します。
- 連絡先情報の更新 - E メールアドレスが古い場合は、転送を開始する前に現在のレジストラで更新してください。
- 認可 E メールの再送信 - Route 53 コンソールで、転送ステータスのドメインの「認可 E メールの再送信」をクリックします。

「無効な認可コード」エラーが発生しています

「無効な認可コード」エラーが表示された場合は、次のソリューションを試してください。

- コードの再確認 - 認可コードでは大文字と小文字が区別されます。レジストラのインターフェイスから直接コードをコピーして貼り付け、入力エラーを回避します。
- コードの有効期限が切れているかどうかを確認する - 認可コードの有効期限は、現在のレジストラに応じて 5 ~ 30 日です。有効期限が切れている場合は、新しいコードをリクエストします。
- 余分なスペースを削除する - コードを入力するときに、先頭または末尾にスペースがないことを確認します。
- 新しい認可コードを取得する - コードが引き続き失敗する場合は、現在のレジストラに新しい認可コードをリクエストします。

ドメインが現在のレジストラでロックされている

現在のレジストラで移管ロックが有効になっている場合 (「ドメインロック」または「クライアント移管禁止」とも呼ばれます)、ドメイン移管が失敗する可能性があります。これは、不正な転送を防止する一般的なセキュリティ設定です。

この問題を解決するには:

- ドメインのロックを解除する - 現在のレジストラのコントロールパネルにログインし、ドメイン移管ロックを無効にします。
- ロックが削除されていることを確認する - 任意のパブリック WHOIS ルックアップツールを使用して、ドメインのステータスが「clientTransferProhibited」ではなく「OK」であることを確認します。
- レジストラからサポートを受ける - ドメインをロック解除するオプションが表示されない場合は、現在のレジストラのサポートチームにお問い合わせください。ロックの削除に役立ちます。

ドメインは移管の対象ではありません

資格の問題によりドメイン移管が拒否された場合は、以下を確認してください。

- ドメインの有効期間を確認する - ドメインは、登録または最終移管から 60 日以上経過している必要があります。
- TLD サポートを確認する - Route 53 がドメインの最上位ドメイン (TLD) をサポートしていることを確認します。サポートされている TLD については、「Amazon Route 53 に登録できる最上位ドメイン」を参照してください。
- ドメインステータスを確認する - 特定のステータスコード (「pendingTransfer」や「redemptionPeriod」など) を持つドメインは移管できません。
- 有効期限の確認 - 有効期限が切れているか、有効期限から 15 日以内にドメインを移管できない場合があります。
- 請求の問題を解決する - 現在のレジストラのすべての未払い料金が支払われていることを確認します。

移管に予想よりも時間がかかる

移管が遅れていると思われる場合は、次の点に注意してください。

- 通常の時間枠 - ほとんどの転送は 5 ~ 7 日以内に完了しますが、最大 10 日かかる場合があります。
- 移管ステータスのモニタリング - Route 53 コンソールで移管の進行状況を確認します。詳細については、「ドメイン移管のステータスの表示」を参照してください。
- E メールにすばやく応答する - どちらのレジストラも、応答を続行する必要がある確認 E メールを送信する場合があります。
- 現在のレジストラに問い合わせる - 移管が遅れた場合は、現在のレジストラに連絡して、移管がブロックされていないことを確認します。

AWS サポートに連絡するタイミング

上記のソリューションを試しても問題が解決しない場合は、 AWS サポートにお問い合わせください。

- 正しい情報を使用して複数回試行した後の移管失敗
- 移管プロセス中の請求または支払いの問題
- Route 53 コンソールで移管を開始できないテクニカルエラー
- 10 日以上「保留中」ステータスのままの移管

サポートに連絡するときは、ドメイン名、転送リクエスト ID (利用可能な場合) 、および発生している特定のエラーまたは問題に関する詳細を含めます。

Amazon Route 53 から別のレジストラへのドメインの移行

Amazon Route 53 から別のレジストラにドメインを移管するときは、Route 53 から情報を取得して、それを新しいレジストラに渡します。残りの作業は新しいレジストラが実行します。

> **Important**
>
> 現在、DNS サービスプロバイダとして Route 53 を使っていて、DNS サービスも別のプロバイダに移管する場合は、次の Route 53 の機能が他の DNS サービスプロバイダの提供する機能では直接代替できないことに注意してください。新しい DNS サービスプロバイダと協力して、同等の機能を実現する方法を決める必要があります。
>
> - エイリアスレコード。詳細については、「エイリアスレコードと非エイリアスレコードの選択」を参照してください。
> - シンプルなルーティングポリシー以外のルーティングポリシー。詳細については、「ルーティングポリシーの選択」を参照してください。
> - レコードに関連付けられているヘルスチェック。詳細については、「DNS フェイルオーバーの設定」を参照してください。

ほとんどのドメインレジストラは、他のレジストラへのドメインの移管について要件を設定しています。これらの要件の主な目的は、不正なドメインの所有者が、別のレジストラにドメインを繰り返し移管するのを防ぐことです。要件は異なりますが、以下の要件が一般的です。

- ドメインを現在のレジストラに登録するか、少なくとも 14 日前にドメインの登録を現在のレジストラに移管しておく必要があります。
- ドメインのドメイン名ステータスコードが以下のいずれかであってはいけません。
  - pendingDelete
  - pendingTransfer
  - redemptionPeriod
  - clientTransferProhibited
  - serverTransferProhibited

ドメイン名ステータスコードと各コードの意味を説明した現在の一覧については、ICANN ウェブサイトで epp status codes を検索してください (ICANN ウェブサイトで直接、検索してください。ウェブ検索ではドキュメントの古いバージョンが返されることがあります)。

> **Note**
>
> ドメインを別のドメインレジストラに移管したいが、 AWS ドメインが登録されているアカウントが閉鎖、停止、または終了している場合は、 AWS サポートにお問い合わせください。登録後 14 日以内はドメインを移行させることはできません。詳細については、「ドメイン登録の問題に関する AWS サポートへのお問い合わせ」を参照してください。

> **Note**
>
> 新しいレジストラで REG-ID コードが必要な場合は、 AWS サポートにお問い合わせください。詳細については、「ドメイン登録の問題に関する AWS サポートへのお問い合わせ」を参照してください。

ドメインを Route 53 から別のレジストラに移管するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [Registered Domains] をクリックします。
3. 別のレジストラに移管するドメインの名前を選択します。

4. [ドメイン名] ページで、[ドメイン名のステータスコード] の値を確認します。以下の値のいずれかである場合、現在、そのドメインを移管することはできません。

   - pendingDelete
   - pendingTransfer
   - redemptionPeriod
   - clientTransferProhibited
   - serverTransferProhibited

   ドメイン名ステータスコードと各コードの意味を説明した現在の一覧については、ICANN ウェブサイトで epp status codes を検索してください (ICANN ウェブサイトで直接、検索してください。ウェブ検索ではドキュメントの古いバージョンが返されることがあります)。

   ドメイン名ステータスコードの値が serverTransferProhibited の場合は、 AWS サポートに無料で問い合わせて、ドメインを移管するために実行する必要があることを確認できます。詳細については、「ドメイン登録の問題に関する AWS サポートへのお問い合わせ」を参照してください。

5. [移管のロック] の値が [オン] の場合は、[アクション] ドロップダウンで [移管のロックをオフにする] を選択します。

6. .be、.co.za、.ru、.uk、.co.uk、.me.uk、.org.uk の各ドメインを除くすべてのドメイン – [ドメイン名] ページで、[移管 (OUT)] のドロップダウンから [別のレジストラに移管] を選択します。

   [別のレジストラへ移管] ダイアログボックスで、[コピー] を選択してドメイン移管の認可コードをコピーします。この値は、後述する手順で新しいレジストラに伝えます。

   > **Note**
   >
   > .eu ドメインの場合、レジストリ https://my.eurid.eu/ の「My.eu」パネルを使用して認可コードを生成することもできます。

   .be、.co.za、.es、.ru、.uk、.co.uk、.me.uk、.org.uk ドメイン - 次の手順を実行します。

   .be ドメイン

   DNS Belgium ウェブサイトで .be ドメインのレジストリから認可コードを取得します。

.co.za のドメイン

.co.za ドメインを別のレジストラに移管するために認可コードを取得する必要はありません。

.ru のドメイン

https://www.nic.ru/en/auth/recovery/ で、.ru ドメインのレジストリから認可コードを取得します。

a. ドメイン名で認証情報を回復するためのオプションを選択します。

b. ドメイン名を入力し、[Continue (続行)] を選択します。

c. 画面上の指示に従って、RU-CENTER 管理者ページにアクセスします。

d. [Manage your account (アカウントの管理)] セクションで、[Domain transfer (ドメイン移管)] を選択します。

e. REGRU-RU で移管を確定します。

.uk、.co.uk、.me.uk、.org.uk のドメイン

IPS タグを新しいレジストラの値に変更します。

a. Nominet ウェブサイトの [Find a Registrar] ページにアクセスし、新しいレジストラの IPS タグを見つけます。(Nominet は .uk、.co.uk、.me.uk、および .org.uk ドメインのレジストリです。)

b. [Registered Domains] (登録済みドメイン) > [domain name](ドメイン名) ページで、[Transfer out] (移管)、ドロップダウン、[Update IPS Tag] (IPS タグの更新) を選択し、ステップ 6a で取得した値を指定します。

c. [更新] を選択します。

> **Note**
>
> Nominet コンソールで IPS タグを更新することもできます。手順については、「レジストラの切り替え」を参照してください。

7. 現在、ドメインの DNS サービスプロバイダーとして Route 53 を使用していない場合は、ステップ 10 に進みます。

   現在、ドメインの DNS サービスプロバイダとして Route 53 を使用している場合は、次のステップを実行します。

a. [ホストゾーン] を選択します。

b. ドメインのホストゾーンの名前を選択します。ドメインの名前とホストゾーンの名前は同じです。

c. ドメインの DNS サービスプロバイダとして Route 53 を引き続き使用する場合: Route 53 がホストゾーンに割り当てた 4 つのネームサーバーの名前を取得します。詳細については、「パブリックホストゾーンに対するネームサーバーの取得」を参照してください。

   ドメインの DNS サービスプロバイダとして Route 53 を使い続けない場合: NS レコードと SOA レコード以外のレコードのすべての設定をメモします。エイリアスレコードなど、Route 53 特有の機能については、新しい DNS サービスプロバイダーと協力して、同等の機能を実現する方法を決める必要があります。

8. DNS サービスを別のプロバイダに転送している場合は、新しい DNS サービスによって提供される方法を使用して、以下のタスクを実行します。

   - ホストゾーンの作成
   - Route 53 レコードの機能を再現するレコードを作成します。
   - 新しい DNS サービスがホストゾーンに割り当てたネームサーバーを取得する

9. 新しいレジストラに用意されたプロセスを使用して、ドメインの移管をリクエストします。

   .co.za、.uk、.co.uk、.me.uk、.org.uk のドメインを除くすべてのドメイン: この手順のステップ 6 で Route 53 コンソールから取得した認可コードを入力するよう求められます。

10. DNS サービスプロバイダーとして Route 53 を引き続き使用する場合は、新しいレジストラが提供するプロセスを使用して、ステップ 7 で取得した Route 53 ネームサーバーの名前を指定します。別の DNS サービスプロバイダーを使用する場合は、ステップ 8 で新しいホストゾーンを作成したときに新しいプロバイダーから示されたネームサーバーの名前を指定します。

11. 確認 E メールに従って行動します。

    .jp のドメインを除くすべてのドメイン

    Route 53 は、ドメインの登録者の連絡先に確認メールを送信します。

    - TLD に応じて、確認 E メールには次のいずれかのドメインからのリンクが含まれます。このリンクを使用して、転送を承認または拒否します。
      - registrar.amazon
      - domainnameverification.net
      - emailverification.info

- key-systems.net

- アクションを実行しない場合、転送は指定された日付に自動的に続行されます。

.jp のドメイン

Route 53 は、アドレス noreply@domainnameverification.net または noreply@emailverification.info からドメインの登録者の連絡先に、移管を確認するためのリンクを記載した確認 E メールを送信します。

- このリンクを使用して、転送を承認または拒否します。ステップ 7 で取得したドメイン認可コードを指定する必要があります。
- アクションを実行しない場合、転送は指定された日付にキャンセルされます。

また、WIXI.jp からメールが届く場合があります。このメールは無視して構いません。

12. ドメインの移管先のレジストラから移管に失敗したことがレポートした場合は、そのレジストラに詳細を問い合わせてください。ドメインを別のレジストラに移管すると、すべてのステータス更新は新しいレジストラに送信されるため、Route 53 には移管が失敗した理由に関する情報がありません。

    Route 53 から取得した認可コードが無効であるため、新しいレジストラから移管に失敗したことがレポートされた場合は、 AWS Support にケースを提出してください。(サポート契約は必要なく、料金はかかりません)。詳細については、「ドメイン登録の問題に関する AWS サポートへのお問い合わせ」を参照してください。

    > **Note**
    >
    > Gandi によって生成された認可コードは、約 5 日間有効です。この期間後に移管が試行された場合、コードの有効期限が切れているために失敗する可能性があります。

13. DNS サービスを他の DNS サービスプロバイダに移管した場合、DNS リゾルバーが Route 53 ネームサーバーの名前の DNS クエリへの応答を停止した後で、ホストゾーンのレコードを削除し、ホストゾーンを削除することができます。これには、通常 2 日かかります。一般的に DNS リゾルバーがドメインのネームサーバーの名前をキャッシュするのにかかる時間の長さです。

    > **Important**
    >
    > DNS リゾルバーが Route 53 ネームサーバーの名前の DNS クエリにまだ応答している間にホストゾーンを削除すると、ドメインはインターネットで利用できなくなります。

ホストゾーンを削除すると、Route 53 では、ホストゾーンの月額料金が請求されなくなります。詳細については、次のドキュメントを参照してください。

- レコードの削除
- パブリックホストゾーンの削除
- Route 53 料金表

ドメインを別の AWS アカウントに転送する

1 つの AWS アカウントを使用してドメインを登録し、そのドメインを別の AWS アカウントに移管する場合は、新しいコンソールを使用するか、 AWS CLI または他のプログラムによる方法を使用して簡単にドメインを移管できます。

トピック

- ステップ 1: ドメインを別の AWS アカウントに転送する
- ステップ 2 (オプション): ホストゾーンを別の AWS アカウントに移行する

ステップ 1: ドメインを別の AWS アカウントに転送する

登録後 14 日以内はドメインを移行させることはできません。

ドメイン移管を開始するときは、ルートアカウントを使用するか、以下のいずれかの方法で IAM 許可が付与されているユーザーを使用して、サインインする必要があります。

- ユーザーには、AdministratorAccess 管理ポリシーが割り当てられます。
- ユーザーには、AmazonRoute53DomainsFullAccess 管理ポリシーが割り当てられます。
- ユーザーには、AmazonRoute53FullAccess 管理ポリシーが割り当てられます。
- ユーザーには、PowerUserAccess 管理ポリシーが割り当てられます。
- ユーザーには、`TransferDomains`、`DisableDomainTransferLock`、および `RetrieveDomainAuthCode` のすべてのアクションを実行するアクセス権限があります。

ルートアカウントまたは必要なアクセス許可を持つユーザーを使用してサインインしない場合、Route 53 は転送を実行できません。この要件は、権限のないユーザーがドメインを他の に転送することを防ぎます AWS アカウント。

移管のプロセスには 2 つのステップがあります。最初に、移管元のアカウント所有者が別の AWS アカウントへの移管を開始する手順で移管を開始します。次に、移管先のアカウント所有者が、別の AWS アカウントから移管を受け入れる手順で移管を受け入れます。

ドメインを別の AWS アカウントに転送するには

1. ドメインが現在登録 AWS アカウント されている AWS を使用して にサインインします。
2. Route 53 コンソール (https://console.aws.amazon.com/route53/) を開きます。
3. ナビゲーションペインで [Registered Domains] をクリックします。
4. 別の AWS アカウントに移管するドメインの名前を選択します。
5. [詳細] セクションの上にある、 [移管 (OUT)] のドロップダウンで [別の AWS アカウントに移管] を選択します。
6. [別の AWS アカウントに移管] ダイアログに、移管先のアカウント ID を入力します。この ID は、移管先の AWS アカウント 所有者から取得できます。
7. [確認] を選択します。
8. パスワードの生成ダイアログで、パスワードをコピーし、受信側 AWS アカウント 所有者に転送します。

   リクエストページで、ドメインのステータスに進行中が表示され、タイプに内部転送が表示されます。

別の AWS アカウントからのドメイン移管を受け入れるには

1. ドメインを受信 AWS アカウント している AWS を使用して にサインインします。
2. Route 53 コンソール (https://console.aws.amazon.com/route53/) を開きます。
3. ナビゲーションペインで、[リクエスト] を選択します。
4. リクエストページで、別のドメイン名から転送するドメイン名の横にあるラジオボタンを選択します AWS アカウント。ドメインの移管準備が整うと、[ステータス] が [必要なアクション] に、[タイプ] が [でのドメインの内部移管] になります。

   リクエストの承諾期間は 3 日間です。3 日以内に移管を承諾しなければ、その移管リクエストはキャンセルされます。
5. [アクション] ドロップダウンで、[承諾] を選択します。

   [拒否] を選択すると、移管のプロセスをキャンセルできます。

6. 承諾したら、[ドメインをアカウントに移管する] ページの [パスワード] のセクションに、移管元のアカウント所有者から受け取ったパスワードを入力します。

   利用規約に同意して、[次へ] を選択します。

7. [リクエスト] ページに移動し、移管の状況やその他の行うべき手順を確認します。

8. 移管が完了すると、連絡先情報を更新できます。詳細については、「ドメインの連絡先情報と所有者の更新」を参照してください。

プログラムを使ってドメインを移管する

、 AWS SDKs の 1 つ AWS CLI、または Route 53 API を使用して、プログラムでドメインを移管することもできます。詳細については、次のドキュメントを参照してください。

- 移管プロセスの概要と、Route 53 ドメイン登録 API を使って、ドメインを移管する場合に使用する API アクションに関するドキュメントについては、Amazon Route 53 API リファレンスの「TransferDomainToAnotherAwsAccount」をご覧ください。
- ドメインをプログラムで移管するためのその他のオプションに関するドキュメントについては、SDKs とツールキット」を参照してください。AWS
- 移管先のアカウントが、transfer-domain-to-another-aws-account API を使って移管元アカウントからアカウントを受け入れられる期間は 3 日間です。3 日以内に移管を承諾しなければ、その移管リクエストはキャンセルされます。

> **Important**
>
> ドメインを別の AWS アカウントに移管する場合、ドメインのホストゾーンは移管されません。ホストゾーンを移管する場合は、ドメインが移管されるまで待ってから、「ステップ 2 (オプション): ホストゾーンを別の AWS アカウントに移行する」を参照してください。

ステップ 2 (オプション): ホストゾーンを別の AWS アカウントに移行する

ドメインの DNS サービスとして Route 53 を使用している場合、Route 53 はドメインを別の AWS アカウントに移管するときにホストゾーンを移管しません。ドメイン登録があるアカウントに関連付けられていて、該当するホストゾーンが別のアカウントに関連付けられている場合、ドメイン登録も DNS 機能も影響を受けません。唯一の影響は、ドメインを確認するには片方のアカウントを使用し

て Route 53 コンソールにサインインする必要があり、ホストゾーンを確認するには、もう片方のアカウントを使用してサインインする必要があるという点です。

ドメインの移管先のアカウントとドメインの移管元のアカウントの両方を所有している場合は、ドメインのホストゾーンを別のアカウントに移行できます。ただし、これはオプションであり、必須ではありません。Route 53 は、既存のホストゾーンのレコードを引き続き使用して、ドメインのトラフィックをルーティングします。

> **Important**
>
> ドメインを移管するアカウントとドメインを移管するアカウントの両方を所有していない場合は、既存のホストゾーンをドメインを移管する AWS アカウントに移行するか、所有する AWS アカウントに新しいホストゾーンを作成する必要があります。ドメインのトラフィックをルーティングするホストゾーンの作成元のアカウントを所有していない場合、トラフィックのルーティング方法は制御できません。

既存のホストゾーンを新しいアカウントに移行するには、「ホストゾーンを別の AWS アカウントに移行する」を参照してください。

新しいホストゾーンを作成するには、「Amazon Route 53 を既存ドメインの DNS サービスとして使用する」を参照してください。このトピックは通常、別のレジストラから Route 53 にドメインを移管する場合に使用されますが、あるアカウントから別の AWS アカウントにドメインを移管する場合もプロセスは同じです。

> **Important**
>
> ホワイトラベルネームサーバー: ドメインがホワイトラベルネームサーバー (ns1.example.com などのカスタムネームサーバーホスト名) を使用している場合は、追加のステップが必要です。
>
> - ドメイン登録の移管時: 移管完了後に新しいレジストラでグルーレコードを更新します。
> - ホストゾーンを移行する場合: ホスト名が同じであっても IP アドレスが変更されるため、ゾーン移行後にドメインレジストラでグルーレコードを更新します。
>
> 詳細な手順については、「the section called “ステップ 7: グルーレコードを作成し、レジストラの名前サーバーを変更します。”」を参照してください。

ドメイン移管のステータスの表示

別のドメインレジストラから Amazon Route 53 へのドメインの移管を開始すると、Route 53 コンソールの [リクエスト] ページ (新コンソール) または [保留中のリクエスト] ページ (旧コンソール) ページから、ステータスを追跡できます。[ステータス] に現在のステップの簡単な説明が表示されます。以下のリストは、コンソールに表示されるテキストと、各ステップの詳細な説明です。

> **Note**
>
> 移管リクエストを送信したときに、最初のステータスは "Domain transfer request submitted" です。これは、お客様のリクエストが届いたことを示します。

ドメインが転送要件を満たしているかを判断 (ステップ 1/14)

ドメインのステータスが移管可能であるか確認しています。お客様はドメインのロックを解除する必要があり、移管リクエストを送信するときにドメインのステータスコードが以下のいずれかであってはいけません。

- clientTransferProhibited
- pendingDelete
- pendingTransfer
- redemptionPeriod

地域別 TLD のみ: WHOIS 情報の確認 (ステップ 2/14)

地域別 TLD があるドメインを移管する場合、ドメインのプライバシー保護を無効にしたかどうか確認するために、ドメインの WHOIS クエリが送信されています 現在のレジストラでプライバシー保護が依然として有効な場合、ドメイン移管に必要な情報にアクセスすることができません。

> **Note**
>
> .com、.net、.org などの汎用 TLD を持つドメインには認可は必要ありません。

地域別 TLD のみ: 移管の承認を得るため、E メールが登録者の連絡先に送信される (ステップ 3/14)

地域別 TLD があるドメインを移管する場合、ドメインの登録者の連絡先に E メールが送信されています。この E メールの目的は、ドメインの許可されている連絡先によって移管がリクエストされたことの確認です

> **Note**
>
> .com、.net、.org などの汎用 TLD を持つドメインには認可は必要ありません。

現在のレジストラを使用した転送の確認 (ステップ 4/14)

ドメインの現在のレジストラに移管開始のリクエストを送信しました。

地域別 TLD のみ: 登録者の連絡先からの承認待ち (ステップ 5/14)

ドメインの登録者の連絡先に E メールを送信しました (ステップ 3/14 を参照) 。登録者の連絡先が E メール内のリンクを選択して移管を承認するのを待っています。地域別 TLD があるドメインを移管する場合に、何らかの理由で E メールが届かないときは、「承認および確認メールの再送信」を参照してください。

現在のレジストラに連絡して転送をリクエスト済 (ステップ 6/14)

移管作業を完了するために、ドメインの現在のレジストラと協力しています。

現在のレジストラが転送を完了するのを待機中 (ステップ 7/14)

ドメインが移管の要件を満たしているか現在のレジストラが確認しています。このステップは、ドメインの TLD に応じて最大 10 日かかる場合があります。

- 汎用最上位ドメイン - 最大 7 日かかります
- 地理的最上位ドメイン(国コードの最上位ドメインとも呼ばれます) 最大 10 日かかります

> **Note**
>
> .JP ドメインの移管時に Route 53 から送信された確認メールを承認したものの、ステップ 7。で数日間停止している場合は、AWS サポートセンターまでお問い合わせください。

ほとんどのレジストラにおいて、プロセスは完全に自動化されているため、高速化することはできません。レジストラによっては、移管の承認を求める E メールが送信されることがあります。

レジストラからこの確認 E メールが送信されてきたら、プロセスは少なくとも 7 日から 10 日早めることができます。

レジストラによって移管が拒否される場合は、「最上位ドメインの移管に関する要件」を参照してください。

連絡先が転送を開始したことを登録者の連絡先に確認（ステップ 8/14）

一部の TLD レジストリは、登録者の連絡先に別のメールを送信して、ドメインの移管が正式なユーザーによって要求されたか確認します。

ネームサーバーとレジストリの同期（ステップ 9/14）

このステップは、移管リクエストの一部として指定したネームサーバーが、現在のレジストラに記録されたネームサーバーとは異なる場合にのみ発生します。指定された新しいネームサーバーにネームサーバーが更新されます。

設定とレジストリの同期（ステップ 10/14）

移管が正常に完了したことを確認し、ドメイン関連のデータをレジストラアソシエイトと同期しています。

更新された連絡先情報をレジストリに送信（ステップ 11/14）

移管のリクエスト時にドメインの所有権を変更した場合、所有権の変更を実施しています。ただし、ほとんどのレジストリでは、ドメイン移管プロセスの一環として所有権を移管することを認めていません。

Route 53 への転送を完了する（ステップ 12/14）

移管プロセスが成功したか確認しています。

転送の完了（ステップ 13/14）

Route 53 でドメインを設定しています。

転送完了（ステップ 14/14）

移管が正常に完了しました。

ドメインを Amazon Route 53 に移管するとドメイン登録の有効期限が受ける影響

レジストラ間でドメインを移管すると、同じ有効期限を保持する TLD レジストリもあれば、有効期限を 1 年延長するレジストリや、有効期限を移管日の 1 年後に変更するレジストリもあります。

> **Note**
>
> ほとんどの TLD では、Amazon Route 53 にドメインを移行してから最大 10 年間ドメインの登録期間を延長できます。詳細については、「ドメインの登録期間の延長」を参照してください。

汎用 TLD

汎用 TLD (例えば .com) のドメインを Route 53 に移管すると、ドメインの新しい有効期限は前のレジストラの有効期間に 1 年を加えたものになります。

地域別 TLD

地域別 TLD (例えば .co.uk) のドメインを Route 53 に移管すると、ドメインの新しい有効期限は TLD に左右されます。次の表で TLD を探して、ドメインを移管すると有効期間にどのような影響があるか判断してください。

大陸	地域別 TLD とドメイン移管が有効期限に及ぼす影響
アフリカ	.co.za - 有効期限は同じままです。
アメリカ大陸	.cl、.com.ar、.com.br - 有効期限は同じままです。 .ca、.co、.mx、.us - 有効期限が 1 年延長されます。
アジア/オセアニア	.com.au、.com.sg、.jp、.net.au、.sg - 有効期限は同じままです。 .co.nz、.in、.net.nz、.org.nz – 古い有効期限に 1 年が追加されています。
欧州	.ch、.co.uk、.es、.fi、.me.uk、.org.uk、.se - 有効期限は同じままです。 .berlin、.eu、.io、.me、.ruhr、.wien - 有効期限が 1 年延長されます。 .be、.de、.fr、.it、.nl: 新しい有効期限は移管日の 1 年後です。

承認および確認メールの再送信

ドメイン登録に関連するいくつかの処理について、ICANN の要件に従って、当社はドメインの登録者の連絡先から承認を得たり、登録者の連絡先の E メールアドレスが有効であることの確認を得たりする必要があります。承認や確認を得るために、当社はリンクを含む E メールを送信します。オペレーションと最上位ドメインに応じて、リンクの選択には 3 ~ 15 日かかります。この期間の経過後、リンクは機能しなくなります。

割り当てられた時間内に E メール内のリンクを選択しない場合、ICANN では、通常、実行しようとしている内容に応じて、ドメインを停止するか、オペレーションをキャンセルする必要があります。

ドメインを登録する

当社はドメインを一時停止し、インターネットでアクセスできないようにします。確認 E メールを再送信するには、「ドメイン登録の確認 E メールを再送信するには」を参照してください。

地域別 TLD のみ: Amazon Route 53 へのドメインの移管

地域別 TLD を持つドメインの移管を実行すると、移管はキャンセルされます 承認 E メールを再送信するには、「ドメインの移管の承認 E メールを再送信するには」を参照してください。

> **Note**
>
> .com、.net、.org などの汎用 TLD を持つドメインには認可は必要ありません。

ドメインの登録者 (所有者) の連絡先の名前または E メールアドレスの変更

変更がキャンセルされます。承認 E メールを再送信するには、「登録者の連絡先を更新するためやドメインを削除するために承認 E メールを再送信するには」を参照してください。

ドメインの削除

削除リクエストがキャンセルされます。承認 E メールを再送信するには、「登録者の連絡先を更新するためやドメインを削除するために承認 E メールを再送信するには」を参照してください。

地域別 TLD のみ: Route 53 から別のレジストラへのドメインの移管

地域別 TLD を持つドメインの移管を実行すると、新しいレジストラによって移管がキャンセルされます。

> **Note**
>
> .com、.net、.org などの汎用 TLD を持つドメインには認可は必要ありません。

トピック

- E メールアドレスの更新
- E メールの再送信

E メールアドレスの更新

ドメインの登録者の連絡先のメールアドレスには、確認および許可メールが送信されます。TLD の一部では、次の場合に登録者の連絡先の古いメールアドレスと新しいメールアドレスに E メールを送信する必要があります。

- Amazon Route 53 に登録済みのドメインの E メールアドレスを変更しようとしています
- Route 53 に転送しているドメインのメールアドレスを変更しようとしています

E メールの再送信

該当する手順を使用して、確認または承認 E メールを再送信します。

- ドメイン登録の確認 E メールを再送信するには
- ドメインの移管の承認 E メールを再送信するには
- 登録者の連絡先を更新するためやドメインを削除するために承認 E メールを再送信するには

ドメイン登録の確認 E メールを再送信するには

1. 登録者の連絡先の E メールアドレスを確認し、必要に応じて更新します。詳細については、「ドメインの連絡先情報と所有者の更新」を参照してください。
2. E メールアプリケーションの迷惑 E メールフォルダーで、以下のいずれかの E メールアドレスからの E メールを確認します。

   長期間が経過していると、リンクは機能しなくなっていますが、当社から別の確認 E メールが送信されるときに、確認 E メールをどこで探すかはわかります。

TLD	承認または確認メールの送信元の E メールアドレス
.fr	nic@nic.fr
その他すべて	以下のいずれかの E メールアドレス: • noreply@registrar.amazon • noreply@domainnameverification.net • noreply@emailverification.info

> **Note**
>
> E メールには、www.registrar.amazon へのリンクが含まれている場合があります。これらのリンクは安全に使用できます。
> 一部の TLDs、検証 E メールの件名または本文にドメイン名が含まれていない場合があります。

3. Amazon Route 53 コンソールを使用して確認メールを再送信する

   a. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。

   b. ナビゲーションペインで [Registered Domains] をクリックします。

   c. E メールを再送信するドメインの名前を選択します。

   d. "Your domain might be suspended" というタイトルの警告ボックスで、[Send email again] を選択します。

   > **Note**
   >
   > 警告ボックスがない場合、登録者の連絡先の E メールアドレスが有効であることは確認済みです。

4. 確認 E メールの再送信中に問題が発生した場合は、 AWS サポートに無料でお問い合わせください。詳細については、「ドメイン登録の問題に関する AWS サポートへのお問い合わせ」を参照してください。

ドメインの移管の承認 E メールを再送信するには

この方法は、.jp ドメインの転送リクエストでは機能しません。

1. 現在のドメインレジストラから提供された方法を使用して、ドメインのプライバシー保護が無効になっていることを確認します。無効になっていない場合は、無効にします。

   当社は、現在のレジストラが WHOIS データベースに保存した E メールアドレスに承認 E メールを送信します。プライバシー保護が有効になっている場合、その E メールアドレスは通常、難読化されています。現在のレジストラでは、Amazon Route 53 によって WHOIS データベース内の E メールアドレスに送信された E メールは、実際の E メールアドレスに転送できません。

   > **Note**
   >
   > ドメインの現在のレジストラでプライバシー保護を無効にできない場合、ステップ 5: 移管をリクエストするで有効な認可コードを指定しても、ドメインを移管できます。

2. 登録者の連絡先の E メールアドレスを確認し、必要に応じて更新します。ドメインの現在のレジストラから提供された方法を使用します。
3. E メールアプリケーションの迷惑 E メールフォルダーで、以下のいずれかの E メールアドレスからの E メールを確認します。

   長期間が経過していると、リンクは機能しなくなっていますが、当社から別の承認 E メールが送信されるときに、承認 E メールをどこで探すかはわかります。

TLD	承認または確認メールの送信元の E メールアドレス
.com.au と .net.au	no-reply@ispapi.net メールには、https://approve.domainadmin.com へのリンクが含まれます。

TLD	承認または確認メールの送信元の E メールアドレス
.fr	nic@nic.fr
その他すべて	以下のいずれかの E メールアドレス: • noreply@registrar.amazon • noreply@domainnameverification.net • noreply@emailverification.info

> **Note**
>
> E メールには、www.registrar.amazon へのリンクが含まれている場合があります。これらのリンクは安全に使用できます。
> 一部の TLDs、検証 E メールの件名または本文にドメイン名が含まれていない場合があります。

4. 移管が進行中でなくなった場合 (長時間が経過してすでにキャンセルされた場合)、移管を再びリクエストすると、別の承認 E メールが届きます。

> **Note**
>
> 転送をリクエストしてから最初の 15 日間に、Route 53 コンソールの [ダッシュボード] ページで、通知テーブルをチェックすると、転送のステータスを決定できます。15 日後、 AWS CLI を使用してステータスを取得します。詳細については、AWS CLI コマンドリファレンスの「route53domains」を参照してください。

移管がまだ進行中の場合は、以下の手順を実行して承認 E メールを再送信します。

a. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。

b. [通知] の表で、移管するドメインを見つけます。

c. そのドメインの [Status] 列で、[Resend email] を選択します。

5. ドメイン転送のために認可 E メールを再送信中に問題が発生した場合は、 AWS Support に無料でお問い合わせください。詳細については、「ドメイン登録の問題に関する AWS サポートへのお問い合わせ」を参照してください。

登録者の連絡先を更新するためやドメインを削除するために承認 E メールを再送信するには

1. 登録者の連絡先の E メールアドレスを確認し、必要に応じて更新します。詳細については、「ドメインの連絡先情報と所有者の更新」を参照してください。
2. E メールアプリケーションの迷惑 E メールフォルダーで、以下のいずれかの E メールアドレスからの E メールを確認します。

   長期間が経過していると、リンクは機能しなくなっていますが、当社から別の承認 E メールが送信されるときに、承認 E メールをどこで探すかはわかります。

TLD	許可メールの発信元となるメールアドレス
.fr	nic@nic.fr
その他すべて	以下のいずれかの E メールアドレス: • noreply@registrar.amazon • noreply@domainnameverification.net • noreply@emailverification.info

> **Note**
>
> E メールには、www.registrar.amazon へのリンクが含まれている場合があります。これらのリンクは安全に使用できます。

一部の TLDs、検証 E メールの件名または本文にドメイン名が含まれていない場合があります。

3. 変更または削除をキャンセルします。これには2つのオプションがあります。

   - 3 ～ 15 日間の待機期間が経過するのを待つことができます。その期間の経過後、リクエストした処理は自動的にキャンセルされます。
   - または、 AWS サポートに連絡して、オペレーションをキャンセルするよう依頼することもできます。

   Important

   移管タイプとキャンセル方法: キャンセル方法は移管のタイプによって異なります。

   - Route 53 への外部レジストラ: このトピックの手順に従います (自動キャンセルを待つか、 AWS サポートにお問い合わせください)。
   - AWS アカウント間: `CancelDomainTransferToAnotherAwsAccount` API を使用するか、 AWS サポートにお問い合わせください

   AWSで既に進行中の移管をキャンセルすることはできないため、Route 53 への移管をキャンセルするために現在の外部レジストラに連絡しないでください。

4. 変更または削除がキャンセルされた後、連絡先情報を変更したり、ドメインを再び削除したりすると、別の承認 E メールが届きます。
5. 認可 E メールの再送信中に問題が発生した場合は、 AWS Support に無料でお問い合わせください。詳細については、「ドメイン登録の問題に関する AWS サポートへのお問い合わせ」を参照してください。

ドメインの DNSSEC の設定

攻撃者は、DNS クエリを傍受し、それらのエンドポイントの実際の IP アドレスの代わりに自身の IP アドレスを DNS リゾルバーに返すことにより、ウェブサーバーなどのインターネットエンドポイントへのトラフィックをハイジャックすることがあります。その後、ユーザーは、偽のウェブサイトなど、なりすましされたレスポンスで攻撃者から提供された IP アドレスにルーティングされます。

DNS スプーフィングや中間者 (MITM) 攻撃と呼ばれるこのタイプの攻撃からは、DNS トラフィックを保護するプロトコルであるドメインネームシステムセキュリティ拡張 (DNSSEC) を設定することでドメインを保護できます。

> **Important**
>
> Amazon Route 53 では、ドメイン登録で DNSSEC 署名と DNSSEC がサポートされています。Route 53 で登録されたドメインに DNSSEC 署名を設定する場合は、Amazon Route 53 での DNSSEC 署名の設定 をご覧ください。

トピック

- DNSSEC がドメインを保護する方法の概要
- ドメインに DNSSEC を設定する際の前提条件と最大数
- ドメインへのパブリックキーの追加
- ドメインのパブリックキーの削除

DNSSEC がドメインを保護する方法の概要

ドメインの DNSSEC を構成すると、DNS リゾルバーは中間リゾルバーからのレスポンスに対して信頼チェーンを確立します。信頼チェーンの先頭は、ドメインの TLD レジストリ (ドメインの親ゾーン) で、末尾は DNS サービスプロバイダーにある権威ネームサーバーです。すべての DNS リゾルバーが DNSSEC をサポートしているわけではありません。DNSSEC をサポートするリゾルバーのみが署名または信頼性チェックを実行します。

Amazon Route 53 に登録されているドメインの DNSSEC を設定して、インターネットホストを DNS スプーフィングから保護する方法は次のとおりです。

1. DNS サービスプロバイダーにより提供されたメソッドを使用し、非対称キーペアのプライベートキーによって、ホストゾーン内のレコードに署名します。

   > **Important**
   >
   > Route 53 では、DNSSEC 署名と、ドメイン登録用の DNSSEC がサポートされています。詳細については Amazon Route 53 での DNSSEC 署名の設定 を参照してください。

2. パブリックキーをキーペアからドメインレジストラに提供し、キーペアの生成に使用されたアルゴリズムを指定します。ドメインレジストラは、パブリックキーとアルゴリズムを最上位ドメイン (TLD) レジストリに転送します。

   Route 53 に登録したドメインに対してこのステップを実行する方法については、「ドメインへのパブリックキーの追加」を参照してください。

DNSSEC を設定したら、以下のようにして DNS スプーフィングからドメインを保護できます。

1. ウェブサイトを参照するか、E メールメッセージを送信することにより、DNS クエリを送信します。
2. リクエストは DNS リゾルバーにルーティングされます。リゾルバーは、ウェブサーバーの IP アドレスや E メールサーバーの IP アドレスなど、リクエストに基づいて正しい値をクライアントに返します。
3. IP アドレスが DNS リゾルバーにキャッシュされている場合、リゾルバーは IP アドレスをクライアントに返します。その後、クライアントはその IP アドレスを使用してホストにアクセスします。

   IP アドレスが DNS リゾルバーにキャッシュされていない場合、リゾルバーは TLD レジストリのドメインの親ゾーンにリクエストを送信します。TLD レジストリは 2 つの値を返します。

   - Delegation Signer (DS) レコード。レコードの署名に使用されたプライベートキーに対応するパブリックキーです。
   - ドメインの権威ネームサーバーの IP アドレス。
4. DNS リゾルバーはリクエストを別の DNS リゾルバーに送信します。そのリゾルバーに IP アドレスがない場合、リゾルバーが DNS サービスプロバイダーにあるネームサーバーにリクエストを送信するまでプロセスを繰り返します。ネームサーバーにより 2 つの値が返されます。
   - ドメインのレコード (example.com など)。通常、これにはホストの IP アドレスが含まれています。
   - DNSSEC を設定したときに作成したレコードの署名。
5. DNS リゾルバーは、ドメインレジストラおよび TLD レジストリに転送されたレジストラに提供したパブリックキーを使用して、2 つの処理を実行します。
   - 信頼チェーンを確立します。
   - DNS サービスプロバイダーからの署名済みレスポンスが正当であり、攻撃者により不正なレスポンスに置き換えられていないことを確認します。
6. レスポンスが本物の場合、リゾルバーはリクエストを送信したクライアントに値を返します。

応答を確認できない場合、リソルバーはユーザーにエラーを返します。

ドメインの TLD レジストリがドメインのパブリックキーを持っていない場合、リゾルバーは DNS サービスプロバイダーから返された情報を使用して DNS クエリに応答します。

ドメインに DNSSEC を設定する際の前提条件と最大数

ドメインに DNSSEC を設定するには、ドメインと DNS サービスプロバイダーが次の前提条件を満している必要があります。

- TLD のレジストリで DNSSEC がサポートされている必要があります。TLD のレジストリで DNSSEC がサポートされているかどうかを確認するには、「Amazon Route 53 に登録できる最上位ドメイン」を参照してください。
- ドメインの DNS サービスプロバイダーでは、DNSSEC がサポートされている必要があります。

> **Important**
>
> Route 53 では、DNSSEC 署名と、ドメイン登録用の DNSSEC がサポートされています。詳細についてはAmazon Route 53 での DNSSEC 署名の設定を参照してください。

- ドメインのパブリックキーを Route 53 に追加する前に、ドメインの DNS サービスプロバイダーで DNSSEC を設定する必要があります。
- ドメインに追加できるパブリックキーの数は、ドメインの TLD によって異なります。
  - .com および .net ドメイン: 最大 13 個のキー
  - 他のすべてのドメイン: 最大 4 個のキー

ドメインへのパブリックキーの追加

キーをローテンションしたり、ドメインで DNSSEC を有効にしたりするときは、ドメインの DNS サービスプロバイダーで DNSSEC を設定した後、以下の手順を実行します。

ドメインにパブリックキーを追加するには

1. DNS サービスプロバイダーを使用してまだ DNSSEC を設定していない場合、サービスプロバイダーにより提供された方法を使用して DNSSEC を設定します。

2. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
3. ナビゲーションペインで [Registered Domains] をクリックします。
4. キーを追加するドメインの名前を選択します。
5. [DNSSEC キー] タブで、[キーの追加] を選択します。
6. 次の値を指定します。

   キーのタイプ

   キー署名キー (KSK) またはゾーン署名キー (ZSK) をアップロードするかどうかを選択します。

   アルゴリズム

   ホストゾーンのレコードの署名に使用したアルゴリズムを選択します。

   パブリックキー

   DNS サービスプロバイダーで DNSSEC を設定するときに使用した非対称キーペアからパブリックキーを指定します。

   次の点に注意してください。

   - ダイジェストではなく、公開キーを指定します。
   - キーは base64 形式で指定する必要があります。
7. [Add] (追加) を選択します。

   > **Note**
   >
   > 一度に追加できるパブリックキーは 1 つだけです。さらにキーを追加する必要がある場合は、Route 53 から確認メールを受け取るまで待ちます;。

8. Route 53 がレジストリからレスポンスを受け取ると、ドメインの登録者にメールが送信されます。メールは、パブリックキーがレジストリのドメインに追加されたことを確認するか、キーを追加できなかった理由を説明するものです。

ドメインのパブリックキーの削除

キーをローテンションしたり、ドメインの DNSSEC を無効にしたりする場合、DNS サービスプロバイダーで DNSSEC を無効にする前に、以下の手順を使用してパブリックキーを削除します。次の点に注意してください。

- パブリックキーをローテーションする場合、新しいパブリックキーを追加してから古いパブリックキーを削除するまで最大 3 日待つことをお勧めします。
- DNSSEC を無効にする場合、まずドメインのパブリックキーを削除します。ドメインの DNS サービスで DNSSEC を無効にする前に、最大 3 日待つことをお勧めします。

> **Important**
>
> ドメインの DNSSEC が有効な場合に、DNS サービスで DNSSEC を無効にした場合、DNSSEC がサポートされている DNS リゾルバーは `SERVFAIL` エラーをクライアントに返し、クライアントはドメインに関連付けられたエンドポイントにアクセスできなくなります。

ドメインのパブリックキーを削除するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [Registered Domains] をクリックします。
3. キーを削除するドメインの名前を選択します。
4. [DNSSEC キー] タブで、削除するキーの横にあるラジオボタンをクリックし、[キーの削除] をクリックします。
5. [Delete DNSSEC key] (DNSSEC キーの削除) ダイアログボックスで、テキストボックスに「削除」と入力してキーを削除することを確認し、[Delete] (削除) をクリックします。

> **Note**
>
> 一度に削除できるパブリックキーは 1 つだけです。さらにキーを削除する必要がある場合は、Amazon Route 53 から確認メールを受け取るまで待ちます。

6. Route 53 がレジストリからレスポンスを受け取ると、ドメインの登録者にメールが送信されます。メールは、パブリックキーがレジストリのドメインから削除されたことを確認するか、キーを削除できなかった理由を説明するものです。

レジストラとドメインに関するその他の情報の検索

GetDomainDetail API を使用してドメイン情報を表示するには、任意の SDKsまたは を使用できます AWS CLI。詳細については、「get-domain-detail」を参照してください。

get-domain-detail CLI を使用してドメインの情報を表示するには

- 次の CLI を使用します。

```
aws route53domains get-domain-detail \
    --region us-east-1 \
    --domain-name example.com
```

> **Note**
>
> このコマンドは us-east-1 でのみ実行されます AWS リージョン。

レジストラ、登録日、プライバシー設定など、ドメインに関するすべての情報が出力に表示されます。

Route 53 に登録されているドメインに関する情報の表示

> **Note**
>
> 2025 年 1 月 28 日以降、一部のドメインレジストリは、ドメイン登録データクエリのために WHOIS から登録データアクセスプロトコル (RDAP) に移行する可能性があります。WHOIS 経由でレジストリから直接ドメイン登録情報にアクセスする場合は、関連するレジストリが WHOIS サポートを停止した場合に、RDAP エンドポイントを使用するようにアプリケーションを更新する必要がある場合があります。

> Route 53 ドメインのサービス機能は変更されません。この通知は、Route 53 サービス以外で実行される直接レジストリ WHOIS クエリにのみ適用されます。

Route 53 を使用して登録したドメインに関する情報を閲覧できます。これには、ドメインの初回登録時に提供した情報、ドメイン所有者、技術担当者、管理者、請求の連絡先情報が含まれます。

WHOIS

WHOIS は、ドメインのレジストラとレジストリが提供しているドメインについての情報を掲載した、無料で利用できる公開のディレクトリです。ポート 43 でクエリを受け入れるサービスと、IPv4 および IPv6 からアクセスできるウェブサイトの両方として提供されています。WHOIS は分散型の階層参照です。詳細については、「WHOIS について」を参照してください。

異なる階層に WHOIS リクエストを行うことで、さまざまな情報が得られます。

- ルート WHOIS (whois.iana.org) にリクエストを行うと、レジストリに関する情報が得られます。
- レジストリ WHOIS にリクエストを行うと、レジストラと、ドメインに関する公開情報の一部が得られます。
- レジストラ WHOIS にリクエストを行うと、ドメインに関するすべての公開情報が得られます。

TLD レジストリとドメインレジストラによって運用される WHOIS ルックアップなど、WHOIS には複数のレベルがあるため、Route 53 コンソールでプライバシー保護をオフにすると、レジストラが提供する WHOIS でのみオフになる可能性があります。一部のレジストリでは、WHOIS 参照サービスのプライバシー保護または改訂サービスが、Route 53 でオフにされているかどうかにかかわらず、意図的に維持されています。ドメインに関する詳細な情報を入手するため、レジストラが提供している WHOIS を使用することが推奨されます。

次の点に注意してください。

プライバシー保護が有効になっている場合にドメインの連絡先を E メールで送信する

> ドメインに対してプライバシー保護が有効になっている場合、登録者、技術担当者、管理者の連絡先情報は、Amazon Registrar プライバシーサービスの連絡先情報に置き換えられます。例えば、example.com というドメインが Amazon Registrar に登録され、プライバシー保護が有効になっている場合、WHOIS のクエリに対する応答では、[登録者 E メール] の値は owner1234@example.com.identity-protect.org のような値になります。

プライバシー保護が有効になっている場合にドメインの連絡先に問い合わせるには、対応する E メールアドレスに E メールを送信します。Route 53 は、E メールを該当する連絡先に自動的に転送します。

不正使用の報告

不適切なコンテンツ、フィッシング、マルウェア、スパムなど、違法行為または適正使用ポリシーの違反を報告するには、trustandsafety@support.aws.com に E メールを送信してください。

Route 53 に登録されているドメインの情報を表示するには

1. ウェブブラウザで、次のいずれかのウェブサイトを開きます。
   - Amazon Registrar: https://registrar.amazon/lookup
   - Gandi WHOIS: https://whois.gandi.net (ドメインレジストラが Gandi の場合はこれを使用します。「」を参照してくださいthe section called “レジストラの検索”)
2. 情報を表示するドメインの名前を入力し、[Search (検索)] を選択します。

ドメイン名登録の削除

最上位ドメイン (TLD) では、必要がなくなった登録を削除できます。レジストリで登録を削除できる場合、このトピックの手順を実行します。

次の点に注意してください。

登録料は返金されません

登録が期限切れになる前にドメイン名登録を削除した場合でも、登録料は AWS から払い戻しされません。

ドメインの登録を削除できる TLD

ドメインの登録を削除できるかどうか判断するには、「Amazon Route 53 に登録できる最上位ドメイン」を参照してください。TLD のセクションに「ドメイン登録の削除」サブセクションが含まれていない場合は、ドメインを削除できます。ドメインを削除する前に、ドメインロックが無効になっていることを確認してください。ドメインロックの無効化の詳細については、「」を参照してください。DisableDomainTransferLock。

ドメイン登録を削除できない場合はどうなりますか?

ドメインのレジストリでドメイン名の登録を削除できない場合は、ドメインの有効期間が切れるのを待つ必要があります。ドメインが自動的に更新されないようにするには、ドメインの自動更新を無効にします。[有効期限] の日付を過ぎると、Route 53 はそのドメインの登録を自動的に削除します。自動更新の設定を変更する方法については、「ドメインの自動更新の有効化/無効化」を参照してください。

ドメインが削除される前に遅延し、再度登録を可能にする

大半のレジストリで、期限切れになったドメインをすぐに登録することはできません。一般的な遅延は、TLD により 1 か月から 3 か月です。詳細については、「Amazon Route 53 に登録できる最上位ドメイン」の TLD の「ドメインの更新と復元の期限」セクションを参照してください。

> **Important**
>
> AWS アカウント間でドメインを移管したり、別のレジストラにドメインを移管したりする場合は、ドメインを削除せず、再登録を期待します。代わりに、該当する次のドキュメントを参照してください。
>
> - ドメインを別の AWS アカウントに転送する
> - Amazon Route 53 から別のレジストラへのドメインの移行

ドメイン名登録を削除するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [Registered Domains] をクリックします。
3. ドメインの名前を選択します。

   co.uk,、.me.uk、.org.uk、.uk ドメインを削除する場合は、「.co.uk、.me.uk、.org.uk、.uk ドメイン名の登録を削除するには」を参照してください。
4. TLD レジストリでドメイン名登録を削除できる場合は、[ドメインを削除] を選択します。

   一部のドメインでは、Route 53 がドメインの登録者に E メールを送信して、登録者がドメインを削除したいことを確認する必要がある場合があります。E メールを受け取った場合、メールは次のメールアドレスの 1 つから送信されます。

   - noreply@registrar.amazon – Amazon Registrar によって登録された TLDs 用。

- noreply@domainnameverification.net または noreply@emailverification.info – 当社のレジストラアソシエイトである Gandi によって登録された TLDs の場合。

TLD のレジストラを調べる方法については、「Amazon Route 53 に登録できる最上位ドメイン」を参照してください。

5. 確認 E メールを受け取った場合、E メール内のリンクを選択し、ドメイン削除のリクエストを承認または拒否します。

> **Important**
>
> 登録者の連絡先は、E メールの指示にすぐに従うか、Route 53 は ICANN の要求に従って、1 日後にすぐに削除リクエストをキャンセルする必要があります。

ドメイン登録が削除されると、もう 1 通メールが送信されます。リクエストの現在のステータスを調べるには、「ドメイン登録のステータスの表示」を参照してください。

6. 削除されたドメインのホストされたゾーンのレコードを削除してから、ホストされたゾーンを削除します。ホストゾーンを削除すると、Route 53 では、ホストゾーンの月額料金が請求されなくなります。詳細については、次のドキュメントを参照してください。

   - レコードの削除
   - パブリックホストゾーンの削除
   - Route 53 料金表

7. ドメイン名登録の削除中に問題が発生した場合は、 AWS サポートに無料でお問い合わせください。詳細については、「ドメイン登録の問題に関する AWS サポートへのお問い合わせ」を参照してください。

.co.uk、.me.uk、.org.uk、.uk ドメイン名の登録を削除するには

.co.uk、.me.uk、.org.uk、.uk ドメインを削除する場合は、.uk ドメインのレジストリである Nominet でアカウントを作成します。詳細については、Nominet ウェブサイト、https://www.nominet.uk/domain-support/ の「ドメイン名のキャンセル」を参照してください。

> **Important**
>
> .uk ドメイン名を削除 (キャンセル) すると、数日以内に削除され、誰でも登録できるようになります。ドメインを移管するだけの場合は、削除しないでください。

プロセスの概要を次に示します。

1. Nominet ウェブサイトで、初めてログインするための指示に従ってください。https://secure.nominet.org.uk/auth/login.html を参照してください。Nominet は、パスワードの作成手順を記載した E メールを送信します。
2. Nominet から受信した E メールの指示に従ってください。
3. Nominet ウェブサイトにログインし、ドメイン名のキャンセル (削除) の手順に従ってください。

ドメイン登録の問題に関する AWS サポートへのお問い合わせ

AWS では、すべての AWS お客様に基本サポートプランを無料で提供しています。このプランには、ドメイン登録に関連する以下の問題のサポートが含まれています。

- Amazon Route 53 へのドメインの移管および Amazon Route 53 からのドメインの移管
- AWS アカウント間のドメインの移管
- 登録できるドメイン数などの Route 53 エンティティのクォータの引き上げ (「クォータ」を参照)
- ドメインの所有者の変更
- ドメイン所有者の連絡先情報の変更
- 確認および承認 E メールの再送信
- ドメインの更新
- 失効したドメインの復元
- Route 53 請求情報の取得
- .uk ドメインの認証情報の提供
- AWS アカウントを閉鎖した後のドメインの削除または自動更新の無効化

これらの問題やドメイン登録に関連するその他の問題について AWS サポートに問い合わせるには、該当する手順を実行します。

トピック

- AWS アカウントにサインインできる AWS 場合のサポートへのお問い合わせ
- AWS アカウントにサインインできない場合の AWS サポートへのお問い合わせ

AWS アカウントにサインインできる AWS 場合のサポートへのお問い合わせ

AWS アカウントにサインインできるときに AWS サポートに連絡するには、次の手順を実行します。

1. ドメインが現在登録されている AWS アカウントを使用して、 AWS サポートにサインインします。

   > **Important**
   >
   > ドメインが現在登録されているルートアカウントを使用してサインインする必要があります。この要件により、承認されていないユーザーがお客様のアカウントをハイジャックするのを防止します。

2. [Account and billing] (アカウントおよび請求) を選択します。
3. 次の値を指定します。

   内容

   デフォルト値の [Account and Billing Support] をそのまま使用します。

   サービス

   デフォルト値の [ドメイン] をそのまま使用します。

   Category

   デフォルト値の [登録の問題] をそのまま使用します。

   緊急度

   該当する重要度を選択します。

   件名

   問題の簡単な概要を入力します。

説明

問題についてより詳しく説明し、関連するドキュメントやスクリーンショットをアタッチします。

連絡方法

問い合わせ方法を選択します。Web. は、 AWS アカウントに関連付けられている E メールアドレスを使用してお客様に AWS 連絡します。

4. [Submit] を選択してください。

AWS アカウントにサインインできない場合の AWS サポートへのお問い合わせ

AWS アカウントにサインインできない場合に AWS サポートに連絡するには、次の手順を実行します。

1. 「I'm an AWS customer and I'm looking for billing or account support」ページに移動します。
2. フォームに入力します。
3. [Submit] を選択してください。

ドメイン請求レポートのダウンロード

複数のドメインを管理し、一定期間のドメインごとの料金を確認するには、ドメイン請求レポートをダウンロードできます。このレポートには、ドメイン登録に関わる以下を含むすべての料金が表示されます。

- ドメインの登録
- ドメインの登録の更新
- Amazon Route 53 へのドメイン移管
- ドメインの所有者の変更 (一部の TLD では、このオペレーションは無料です)

請求レポートには、将来の請求期間が示される場合があります。これは、ドメインの自動更新プロセスが、ドメインが失効する前の月に開始されるために発生します。したがって、例えば 8 月のレポートでは、その年の 9 月から、翌年の 9 月まで続く請求期間が示される場合があります。

コンソールを使用してレポートを実行する場合、次のオプションを選択できます。

- 過去 12 か月: レポートには、レポートを実行した日の 1 年前から当日までの料金が含まれます。例えば、6 月 3 日にレポートを実行した場合、前年の 6 月 3 日から当日までの料金が含まれます。
- 前年の各月: レポートには、指定した月の料金が含まれます。

レポートをプログラムにより実行した場合、2014 年 7 月 31 日以降の任意の日付範囲の料金を取得できます。これは、Route 53 がドメイン登録のサポートを開始した日付です。例えば、AWS CLI コマンドリファレンスの「請求書の表示」を参照してください。

請求レポートは CSV 形式で、その内容は ViewBilling API で説明されています。

ドメイン請求レポートをダウンロードするには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [Registered Domains] を選択します。
3. [Domain billing report] を選択します。
4. レポートの日付範囲を選択してから [Download domain report] を選択します。
5. プロンプトに従ってレポートを開くか、保存します。
6. ドメイン請求レポートのダウンロード中に問題が発生した場合は、 AWS サポートに無料でお問い合わせください。詳細については、「ドメイン登録の問題に関する AWS サポートへのお問い合わせ」を参照してください。

Amazon Route 53 に登録できる最上位ドメイン

> **Important**
>
> 以下の最上位ドメイン制限は、ドメイン登録にのみ適用されます。Route 53 DNS サービスは、選択した任意の最上位ドメインと任意のドメインレジストラで使用できます。このページの情報は、Route 53 に登録できるドメインにのみ関連しています。DNS サービスとしての Route 53 の詳細については、「ウェブサイトやウェブアプリケーションへのインターネットトラフィックのルーティング」を参照してください。

汎用の最上位ドメインおよび地理的な最上位ドメインの次の一覧は、Amazon Route 53 でドメインを登録するために使用できる最上位ドメイン (TLD) を示しています。

Route 53 によるドメインの登録

TLD レジストリでは、一部のドメイン名に対して特別料金またはプレミアム料金を設定しています。Route 53 を使用して、特別料金またはプレミアム料金が設定されたドメインを登録することはできません。以下のリストには、Route 53 を使用して登録できる TLD が含まれています。TLD が含まれていない場合は、Route 53 でドメインを登録することはできません。

Route 53 へのドメインの移管

次の一覧に TLD が含まれている場合は、Route 53 にドメインを移管できます。TLD が含まれていない場合は、Route 53 にドメインを移管することはできません。

一部を除き、TLD では、ドメインを移管するための認可コードを現在のレジストラより取得する必要があります。認可コードが必要かどうかを確認するには、TLD の「移管に必要な認可コード」セクションを参照してください。

ドメインの登録と転送の料金

ドメインの登録または Route 53 への転送のコストの詳細については、「Amazon Route 53 のドメイン登録価格」を参照してください。

DNS サービスとしての Route 53 の使用

ドメインの TLD が次の一覧に含まれていない場合でも、Route 53 をあらゆるドメインの DNS サービスとして使用できます。DNS サービスとしての Route 53 の詳細については、「ウェブサイトやウェブアプリケーションへのインターネットトラフィックのルーティング」を参照してください。Route 53 にドメインの DNS サービスを移管する方法については、「Amazon Route 53 を既存ドメインの DNS サービスとして使用する」を参照してください。

国際化ドメイン名

すべての TLD が国際化ドメイン名 (IDN)、つまり ASCII 文字 a-z、0-9、および - (ハイフン) 以外の文字を含むドメイン名をサポートしているわけではありません。各 TLD のリストは、その TLD が IDN をサポートしているかどうかを示しています。国際化ドメイン名の詳細については、「DNS ドメイン名の形式」を参照してください。

TLD への地理的ドメインの登録

地域別 TLD の登録ルールは国によって異なります。制限のない国、つまり、世界中のだれでも登録できる国もあれば、住所など、一定の制限を設けている国もあります。各地域別 TLD のリストには、制限事項が示されています。

サポートされている最上位ドメインのインデックス

トピック

- 汎用最上位ドメイン
- 地理的最上位ドメイン

汎用最上位ドメイン

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, .app, .art, .associates, .auction, .audio

B

.band, .bar, .bargains, .beer,.bet, .bid, .bike, .bingo, .bio, .biz, .black, .blue, .boo, .bot, .boutique, .build, .builders, .business, .buzz

C

.cab, .cafe, .camera, .camp, .capital, .cards, .care, .careers, .cash, .casino, .catering, .cc, .center, .ceo, .chat, .cheap, .christmas, .church, .city, .claims, .cleaning, .click, .clinic, .clothing, .cloud, .club, .coach, .codes, .coffee, .college, .com, .community, .company, .computer, .condos, .construction, .consulting, .contact, .contractors, .cool, .coupons, .credit, .creditcard, .cruises

D

.dad, .dance, .dating, .day, .deal, .deals, .degree, .delivery, .democrat, .dental, .design, .dev, .diamonds, .diet, .digital, .direct, .directory, .discount, .diy, .dog, .domains

E

.earth, .education, .email, .energy, .engineering, .enterprises, .equipment, .esq, .estate, .events, .exchange, .expert, .exposed, .express

F

.fail, .fan, .farm, .finance, .financial, .fish, .fit, .fitness, .flights, .florist, .flowers, .fm, .foo, .food, .football, .forsale, .フォーラム, .foundation, .free, .fun, .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, .health, .healthcare, .help, .hiv, .hockey, .holdings, .holiday, .host, .hosting, .hot, .house, .how

I

.im, .immo, .immobilien, .industries, .info, .ink, .institute, .insure, .international, .investments, .io, .irish

J

.jewelry, .juegos

K USD

.kaufen, .kim, .kitchen, .kiwi

L

.land, .law, .lease, .legal, .lgbt, .life, .lifestyle, .lighting, .limited, .limo, .link, .live, .living, .llc, .loan, .loans, .lol, .love, .ltd

M

.maison, .management, .marketing, .mba, .media, .memorial, .メニュー, .mobi, .moda, .moi, .money, .mortgage, .mov, .movie

N

.name, .net, .network, .news, .nexus, .ninja, .now

O

.one, .onl, .online, .org

P

.page, .partners, .parts, .phd, .photo, .photography, .photos, .pics, .pictures, .pink, .pizza, .place, .plumbing, .plus, .poker, .porn, .press, .pro, .productions, .prof, プロパティ, .property, .pub. .pw (パラオ)

Q

.qpon

R

.realty, .recipes, .red, .reise, .reisen, .rentals, .repair, .report, .republican, .rest, .restaurant, .reviews, .rip, .rocks, .rsvp, .run

S

.sale, .sarl, .school, .schule, .services, .sex, .sexy, .shiksha, .shoes, .shop, .shopping, .show, .singles, .site, .ski, .soccer, .social, .solar, .solutions, .software, .soy, .space, .spot, .store, .stream, .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, .vote, .voyage

WXYZ

.watch, .website, .wedding, .wiki, .win, .wine, .work, .works, .world, .wtf, .xxx, .xyz, .zip, .zone

地理的最上位ドメイン

アフリカ

.ac (アセンション島), .co.za (南アフリカ), .sh (セントヘレナ)

アメリカ大陸

.ai (アンギラ), .ca (カナダ), .cl (チリ), .co (コロンビア), .com.ar (アルゼンチン), .com.br (ブラジル), .com.mx (メキシコ), .mx (メキシコ), .us (米国), .vc (セントビンセントおよびグレナディーン諸島), .vg (英領バージン諸島)

アジア/オセアニア

.au (オーストラリア), .cc (ココス (キーリング) 諸島), .co.nz (ニュージーランド), .com.au (オーストラリア), .com.sg (シンガポール共和国), .fm (ミクロネシア連邦), .in (インド), .jp (日本), .io (英領インド洋地域), .my (マレーシア), .net.au (オーストラリア), .net.nz (ニュージーランド), .nz

(ニュージーランド), .org.nz (ニュージーランド), .pw (パラオ), .qa (カタール), .ru (ロシア連邦), .sg (シンガポール共和国)

欧州

.be (ベルギー), .berlin (ドイツのベルリン市), .ch (スイス), .co.uk (英国), .cz (チェコ共和国), .de (ドイツ), .es (スペイン), .eu (欧州連合), .fi (フィンランド), .fr (フランス), .gg (ガーンジー), .im (マン島), .it (イタリア), .me (モンテネグロ), .me.uk (英国), .nl (オランダ), .org.uk (英国), .ruhr (ドイツ西部のルール地域), .se (スウェーデン), .uk (英国), .wien (オーストリアのウィーン市)

汎用最上位ドメイン

汎用最上位ドメイン (gTLD) は、.com、.net、.org など、世界中で使用され認識されるグローバル拡張子です。また、.bike、.condos、.marketing などの、専門ドメインも含まれます。

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, .app, .art, .associates, .auction, .audio

B

.band, .bar, .bargains, .beer, .bet, .bid, .bike, .bingo, .bio, .biz, .black, .blue, .boo, .bot, .boutique, .build, .builders, .business, .buzz

C

.cab, .cafe, .camera, .camp, .capital, .cards, .care, .careers, .cash, .casino, .catering, .cc, .center, .ceo, .chat, .cheap, .church, .christmas, .city, .claims, .cleaning, .click, .clinic, .clothing, .cloud, .club, .coach, .codes, .coffee, .college, .com, .community, .company, .computer, .condos, .construction, .consulting, .contact, .contractors, .cool, .coupons, .credit, .creditcard, .cruises

D

.dad, .dance, .dating, .day, .deal, .deals, .degree, .delivery, .democrat, .dental, .design, .dev, .diamonds, .diet, .digital, .direct, .directory, .discount, .diy, .dog, .domains

E

.earth, .education, .email, .energy, .engineering, .enterprises, .equipment, .esq, .estate, .events, .exchange, .expert, .exposed, .express

F

.fail, .fan, .farm, .finance, .financial, .fish, .fit, .fitness, .flights, .florist, .flowers, .fm, .foo, .food, .football, .forsale, .フォーラム, .foundation, .free, .fun, .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, .health, .healthcare, .help, .hiv, .hockey, .holdings, .holiday, .host, .hosting, .hot, .house, .how

I

.im, .immo, .immobilien, .industries, .info, .ink, .institute, .insure, .international, .investments, .io, .irish

J

.jewelry, .juegos

K USD

.kaufen, .kim, .kitchen, .kiwi

L

.land, .law, .lease, .legal, .lgbt, .life, .lifestyle, .lighting, .limited, .limo, .link, .live, .living, .llc, .loan, .loans, .lol, .love, .ltd

M

.maison, .management, .marketing, .mba, .media, .memorial, .メニュー, .mobi, .moda, .moi, .money, .mortgage, .mov, .movie

N

.name, .net, .network, .news, .nexus, .ninja, .now

O

.one, .onl, .online, .org

P

.page, .partners, .parts, .phd, .photo, .photography, .photos, .pics, .pictures, .pink, .pizza, .place, .plumbing, .plus, .poker, .porn, .press, .pro, .productions, .prof, プロパティ, .property, .pub

Q

.qpon

R

.realty, .recipes, .red, .reise, .reisen, .rentals, .repair, .report, .republican, .rest, .restaurant, .reviews, .rip, .rocks, .rsvp, .run

S

.sale, .sarl, .school, .schule, .services, .sex, .sexy, .shiksha, .shoes, .shop, .shopping, .show, .singles, .site, .ski, .soccer, .social, .solar, .solutions, .software, .soy, .space, .spot, .store, .stream, .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, .vote, .voyage

WXYZ

.watch, .website, .wedding, .wiki, .win, .wine, .work, .works, .world, .wtf, .xxx, .xyz, .zip, .zone

.ac

「.ac (アセンション島)」を参照してください。

Return to index

.academy

学校や大学などの教育機関が使用します。また、教育機関に関連する採用担当者、アドバイザー、広告主、学生、教師、管理者も使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.accountants

会計や経理に関連する企業、団体、および個人が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.actor

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.adult

成人向けコンテンツをホストしているウェブサイトに使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.agency

代理人として識別される任意の企業またはグループが使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.airforce

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます

- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.apartments

不動産業者、地主、および貸家人が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.app

開発者、起業家、企業がアプリを紹介するための安全なドメインとして使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

制限

この TLD 上のすべてのウェブサイトに HTTPS が必要です。ドメインがブラウザで正しく動作するには、ウェブサイトに HTTPS を設定する必要があります。SSL 証明書を取得するためのリソースなど AWS、 で HTTPS を設定する方法の詳細については、「 とは AWS Certificate Manager」を参照してください。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.art

アート関連のウェブサイト、ポートフォリオ、ギャラリー、クリエイティブプロジェクトに使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.associates

タイトルに「アソシエイト」という言葉を含むビジネスや企業が使用します。また、組織の専門性を示すことを望む団体や業者が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.auction

オークションに関連するイベントやオークションベースの売買に使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

中国語、フランス語、ドイツ語、スペイン語、ラテン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.audio

> **Important**
>
> 現在は、Route 53 を使用して新しい .audio ドメインを登録したり、Route 53 に .audio ドメインを移管したりすることはできません。Route 53 に登録済みの .audio ドメインは引き続きサポートされます。

オーディオビジュアル業界や、放送、サウンド機器、オーディオ制作、およびオーディオストリーミングに関心のある人が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

キリル文字 (主にロシア語)、フランス語、ドイツ語、イタリア語、ポルトガル語、スペイン語に対してサポートされます。

移管に必要な認可コード

サポート外。.audio ドメインは Route 53 に移管できなくなりました。

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.band

音楽バンドとバンドイベントに関する情報を共有するために使用します。また、ファンベースとつながり、バンド関連商品を販売するためにミュージシャンが使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

中国語、フランス語、ドイツ語、スペイン語、ラテン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.bar

バー、パブ、ナイトライフ関連のビジネスや愛好家が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.bargains

販売および宣伝に関する情報のために使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.beer

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.bet

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート外。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます

- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.bid

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.bike

自転車店、オートバイ販売会社、修理工場など、サイクリストを対象とする企業またはグループが使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.bingo

オンラインゲームのウェブサイト、またはビンゴゲームに関する情報を共有するために使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.bio

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.biz

ビジネスまたは商用目的で使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

簡体字中国語、繁体字中国語、デンマーク語、フィンランド語、ドイツ語、ハンガリー語、日本語、韓国語、ラトビア語、リトアニア語、ノルウェー語、ポーランド語、ポルトガル語、スペイン語、スウェーデン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.black

黒が好きな人、または、黒をビジネスやブランドに関連付けたい人が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート外。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.blue

青色が好きな人、または、青色をビジネスまたはブランドに関連付けたい人が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート外。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.boo

恋、笑い、驚きなど、楽しい思い出深い安全なドメインとして使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

制限

この TLD 上のすべてのウェブサイトに HTTPS が必要です。ドメインがブラウザで正しく動作するには、ウェブサイトに HTTPS を設定する必要があります。SSL 証明書を取得するためのリソースなど AWS、 で HTTPS を設定する方法の詳細については、「 とは AWS Certificate Manager」を参照してください。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.bot

チャットボットおよび AI 関連の製品やサービスに使用されます。このドメイン拡張は、人工知能における自動システム、会話型インターフェイス、および新しいテクノロジーの性質を伝えるのに役立ちます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.boutique

ブティックや小規模専門店についての情報のために使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.build

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます

- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.builders

建設業界に関連する会社と個人が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.business

任意の業種の企業が使用します。.biz 拡張子の代わりとして使用できます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.buzz

最新のニュースとイベントに関する情報のために使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

スペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.cab

タクシー業界に関連する会社と個人が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.cafe

カフェのビジネスや、カフェ文化に興味を持っている人が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

中国語、フランス語、ドイツ語、スペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.camera

写真愛好家および写真を共有したい人が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.camp

公園およびレクリエーション部門、サマーキャンプ、ライターズワークショップ、フィットネスキャンプ、キャンプ愛好家が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.capital

金融資本や市町村の財源など、任意の種類の資本を示す全般的なカテゴリとして使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.cards

e カード、印刷された挨拶状、名刺、トランプなど、カードを専門とする企業が使用します。カードゲームのルールや戦略を説明したいゲーマーにも最適です。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.care

介護業界の企業や業者が使用します。また、慈善団体が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます

- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.careers

求人に関する情報のために使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.cash

金融関連の活動に従事している任意の組織、団体、またはユーザーが使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.casino

ギャンブル業界、またはギャンブルやカジノゲームに関する情報を共有したいと考えているゲーマーが使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.catering

ケータリングビジネス、または食品関連のイベントについての情報を共有する人が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.cc

「.cc (ココス (キーリング) 諸島)」を参照してください。

Return to index

.center

研究機関からコミュニティセンターまであらゆるものの汎用拡張子として使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.ceo

CEO および同等の役職に関する情報のために使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

ドイツ語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

サポート外。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.chat

任意の種類のオンラインチャットウェブサイトで使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.cheap

安価な製品を宣伝して販売する e コマースウェブサイトが使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.christmas

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます

- 有効期限切れの 43 日後まで Route 53 との遅延更新ができます
- 有効期限から 44 日後にドメインが Route 53 から削除されます
- 有効期限切れの 44 日後から 86 日後までの間、レジストリでの復元ができます
- 有効期限切れの 86 日後、ドメインがレジストリから削除されます

.church

任意の規模の教会または宗派が信徒とつながり、教会関連のイベントや活動に関する情報を公開するために使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます

- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.city

見どころ、人気の高い観光地点、地元の活動など、特定の市に関する情報を提供するために使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.claims

保険請求を処理したり、法的サービスを提供したりする企業が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.cleaning

清掃サービスを提供する企業や個人が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.click

クリック操作をウェブサイトと関連付ける (例えば、ウェブサイトでの商品のクリックを購入と関連付ける) 企業が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護

サポート対象。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

キリル文字 (主にロシア語)、フランス語、ドイツ語、イタリア語、ポルトガル語、スペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.clinic

ヘルスケア業界と医療関係機関が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.clothing

小売業者、デパート、デザイナー、仕立屋、アウトレットも含めて、ファッション業界の人が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.cloud

全般的な拡張子として使用されますが、クラウドコンピューティングテクノロジーとサービスを提供する会社に最適です。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート外。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.club

任意の種類のクラブまたは組織が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

スペイン語、日本語でサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.coach

スポーツの専門家、ライフスタイルの指導者、企業トレーナーなど、指導に興味を持っている人が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.codes

行動規範 (コードオブコンダクト)、建築コード、プログラミングコードなど、あらゆる種類のコードの汎用拡張子として使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます

- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.coffee

コーヒー業界の人が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.college

学校や大学などの教育機関が使用します。また、教育機関に関連する採用担当者、アドバイザー、広告主、学生、教師、管理者も使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

アラビア語、簡体字中国語および繁体字中国語、キリル、ギリシャ語、ヘブライ語、日本語、およびタイ語をサポート。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.com

商用ウェブサイトに使用します。これはインターネットで一番人気の拡張子です。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護

すべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.community

コミュニティ、クラブ、組織、または同じ興味を持つ人のグループが使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.company

あらゆる種類の企業の汎用拡張子として使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.computer

コンピュータに関する情報の汎用拡張子として使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.condos

マンション関係の個人と企業が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.construction

建設業者や請負業者など、建設業界の人が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.consulting

コンサルタントおよびコンサルティング業界関連が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

アラビア語、中国語、フランス語、キリル文字、デバナガリ、ドイツ語、ギリシャ語、ヘブライ語、日本語、韓国語、ラテン語、スペイン語、タミル語、タイ語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.contact

任意の規模の教会または宗派が信徒とつながり、教会関連のイベントや活動に関する情報を公開するために使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます

- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.contractors

建設業界の請負業者など、請負業者が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.cool

最新のトレンドにブランドを関連付けたい組織とグループが使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.coupons

オンラインクーポンやクーポンコードを提供する小売業者や製造元が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

中国語、フランス語、ドイツ語、スペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.credit

クレジット業界が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.creditcard

クレジットカードを発行する企業や銀行が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.cruises

船旅業界が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.dad

親権関連のコンテンツ、ブログ、パパへのマーケティングに使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

制限

この TLD 上のすべてのウェブサイトに HTTPS が必要です。ドメインがブラウザで正しく動作するには、ウェブサイトに HTTPS を設定する必要があります。SSL 証明書を取得するためのリソースなど AWS、 で HTTPS を設定する方法の詳細については、「 とは AWS Certificate Manager」を参照してください。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.dance

ダンサー、ダンス講師、ダンススクールが使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

中国語、フランス語、ドイツ語、ラテン語、スペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

サポート外。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.dating

デートのウェブサイトに使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.day

誕生日から結婚式、特別な日まで、重要な日に注意を向けるために使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

制限

この TLD 上のすべてのウェブサイトに HTTPS が必要です。ドメインがブラウザで正しく動作するには、ウェブサイトに HTTPS を設定する必要があります。SSL 証明書を取得するためのリソースなど AWS、 で HTTPS を設定する方法の詳細については、「 とは AWS Certificate Manager」を参照してください。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.deal

オファー、割引、特別オファーを提供するウェブサイトに使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.deals

オンラインのバーゲンやセールに関する情報を提供するために使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.degree

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます

- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.delivery

任意の種類の商品またはサービスを提供する企業が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.democrat

民主党に関する情報のために使用されます。また、選挙で選出される公職の立候補者、当選した公職者、政治好き、コンサルタント、アドバイザーも使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

中国語、フランス語、ドイツ語、ラテン語、スペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

サポート外。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.dental

歯科医療従事者や歯科用品業者が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.design

任意の規模の教会または宗派が信徒とつながり、教会関連のイベントや活動に関する情報を公開するために使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.dev

開発者とテクノロジーの安全なドメインとして使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

制限

この TLD 上のすべてのウェブサイトに HTTPS が必要です。ドメインがブラウザで正しく動作するには、ウェブサイトに HTTPS を設定する必要があります。SSL 証明書を取得するため

のリソースなど AWS、 で HTTPS を設定する方法の詳細については、「 とは AWS Certificate Manager」を参照してください。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.diamonds

ダイヤモンド愛好家、および、販売業者や再販業者、取引業者も含めてダイヤモンド業界の人が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.diet

> **Important**
>
> 現在は、Route 53 を使用して新しい .diet ドメインを登録したり、Route 53 に .diet ドメインを移管したりすることはできません。Route 53 に登録済みの .diet ドメインは引き続きサポートされます。

健康やフィットネスの専門家が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

キリル文字 (主にロシア語)、フランス語、ドイツ語、イタリア語、ポルトガル語、スペイン語に対してサポートされます。

移管に必要な認可コード

サポート外。.diet ドメインは Route 53 に移管できなくなりました。

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.digital

デジタル関係のすべてに使用しますが、技術系のビジネスに最適です。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.direct

全般的な拡張子として使用しますが、e コマースウェブサイトを通して顧客に商品を直接販売する業者に最適です。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.directory

メディア部門が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.discount

割引のウェブサイト、および格安価格で販売を行う企業が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.diy

do-it-yourself プロジェクト、工作、ホーム改善コンテンツに使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート外。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.dog

犬好きな人、および犬関連のサービスや商品を提供する業者が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

中国語、フランス語、ドイツ語、スペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.domains

ドメイン名に関する情報のために使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます

- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.earth

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.education

教育に関する情報のために使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.email

メールの奨励に関する情報のために使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.energy

全般的な拡張子として使用しますが、エネルギーまたは省エネルギー関連の業者に最適です。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.engineering

技術系企業と技術の専門家が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.enterprises

大企業やビジネスに関する情報のために使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.equipment

機器、機器の小売業者または製造業者、レンタルショップに関する情報のために使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.esq

資格や経験を紹介するために、弁護士や著名人が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

制限

この TLD 上のすべてのウェブサイトに HTTPS が必要です。ドメインがブラウザで正しく動作するには、ウェブサイトに HTTPS を設定する必要があります。SSL 証明書を取得するためのリソースなど AWS、 で HTTPS を設定する方法の詳細については、「 とは AWS Certificate Manager」を参照してください。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.estate

住宅および住宅部門に関する情報のために使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.events

あらゆる種類のイベントに関する情報のために使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.exchange

任意の種類の取引 (証券取引、物品取引、または単純な情報交換) に使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます

- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.expert

各種分野の専門知識を持つ人が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.exposed

写真、タブロイド、調査報道を含む、多様な主題のための汎用拡張子として使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.express

全般的な拡張子として使用しますが、商品やサービスの迅速な配送や提供を強調したい業者に最適です。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

中国語、フランス語、ドイツ語、スペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.fail

失敗をしたが、それをユーモラスに公開したい人が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.fan

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.farm

農民、農業エンジニアなど、農業業界の人が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.finance

財務部門が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.financial

財務部門が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.fish

全般的な拡張子として使用しますが、魚や釣りに関連するウェブサイトに最適です。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます

- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.fit

フィットネス、ヘルス、健康関連のウェブサイトやビジネスに使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.fitness

フィットネスやフィットネスサービスを宣伝するために使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.flights

旅行代理店、航空会社、および旅行業界に関連する人が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.florist

花屋が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.flowers

> **Important**
>
> 現在は、Route 53 を使用して新しい .flowers ドメインを登録したり、Route 53 に .flowers ドメインを移管したりすることはできません。Route 53 に登録済みの .flowers ドメインは引き続きサポートされます。

オンラインの花の販売や、花の成長や飼育に関する情報など、花に関連するすべてに使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

キリル文字 (主にロシア語)、フランス語、ドイツ語、イタリア語、ポルトガル語、スペイン語に対してサポートされます。

移管に必要な認可コード

サポート外。.flowers ドメインは Route 53 に移管できなくなりました。

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.fm

「.fm (ミクロネシア連邦)」を参照してください。

Return to index

.foo

デベロッパーの安全なドメインとして使用されます。.foo は、あらゆる用途に使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

制限

この TLD 上のすべてのウェブサイトに HTTPS が必要です。ドメインがブラウザで正しく動作するには、ウェブサイトに HTTPS を設定する必要があります。SSL 証明書を取得するためのリソースなど AWS、 で HTTPS を設定する方法の詳細については、「 とは AWS Certificate Manager」を参照してください。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.food

食品関連のビジネス、レシピ、料理のコンテンツに使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート外。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.football

サッカーに関係のある人が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.forsale

商品やサービスを販売するために使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

中国語、フランス語、ドイツ語、ラテン語、スペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.フォーラム

オンラインフォーラム、ディスカッションボード、コミュニティプラットフォームに使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.foundation

非営利組織、慈善団体、その他の財団が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.free

無料の製品、サービス、またはコンテンツを提供するウェブサイトに使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.fun

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.fund

資金調達に関連する全般的な拡張子として使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます

- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.furniture

家具の製造業者と販売者、および家具業界に関連のある人が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.futbol

サッカー (フットボール) に関する情報のために使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

中国語、フランス語、ドイツ語、ラテン語、スペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

サポート外。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.fyi

全般的な拡張子として使用しますが、あらゆる種類の情報を共有するために最適です。「FYI」は、「for your information (参考までに)」の頭文字です。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

中国語、フランス語、ドイツ語、スペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.gallery

画廊所有者が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.games

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.gift

ギフトの販売、またはギフト関連サービスを提供する企業または組織が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

キリル文字 (主にロシア語)、フランス語、ドイツ語、イタリア語、ポルトガル語、スペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.gifts

ギフトの販売、またはギフト関連サービスを提供する企業または組織が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.gives

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます

- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.glass

ガラス切り職人や窓枠取付業者など、ガラス業界の人が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます

- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.global

国際市場または国際ビジョンを持つ企業や団体が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

アラビア語、ベラルーシ語、ボスニア語、ブルガリア語、簡体字中国語、繁体字中国語、デンマーク語、ドイツ語、ヒンディー語、ハンガリー語、アイスランド語、韓国語、ラトビア語、リトアニア語、マケドニア語、モンテネグロ語、ポーランド語、ロシア語、セルビア語、スペイン語、スウェーデン語、ウクライナ語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます

- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.gmbh

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート

国際化ドメイン名

サポート

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.gold

全般的な拡張子として使用しますが、金または金関連商品を売買する企業に最適です。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

中国語、フランス語、ドイツ語、スペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.golf

ゴルフ専門のウェブサイトに使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

中国語、フランス語、ドイツ語、スペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.graphics

グラフィックス業界の人が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.gratis

販売促進アイテム、ダウンロード、クーポンなどの無料商品を提供するウェブサイトに使用します。「Gratis」は、スペイン語で「無料」を意味します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.green

節約、エコロジー、環境、環境に優しいライフスタイルを扱うウェブサイトに使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート外。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.gripe

苦情や批評を共有するために使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.group

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます

- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.guide

全般的な拡張子として使用しますが、旅行先、サービス、および商品に特化したウェブサイトに最適です。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます

- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.guitars

> **Important**
>
> 現在は、Route 53 を使用して新しい .guitars ドメインを登録したり、Route 53 に .guitars ドメインを移管したりすることはできません。Route 53 に登録済みの .guitars ドメインは引き続きサポートされます。

ギター愛好家が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

キリル文字 (主にロシア語)、フランス語、ドイツ語、イタリア語、ポルトガル語、スペイン語に対してサポートされます。

移管に必要な認可コード

サポート外。.guitars ドメインは Route 53 に移管できなくなりました。

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます

- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.guru

各種主題についての知識を共有したい人が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.haus

不動産および建築業界が使用します。「Haus」は、「家」を意味するドイツ語です。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

中国語、フランス語、ドイツ語、ラテン語、スペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.health

健康、医療、健康関連のウェブサイトや組織に使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.healthcare

ヘルスケア部門が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.help

全般的な拡張子として使用しますが、オンラインヘルプと情報を提供するウェブサイトに最適です。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

キリル文字 (主にロシア語)、フランス語、ドイツ語、イタリア語、ポルトガル語、スペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.hiv

HIV の撲滅を扱うウェブサイトに使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

キリル文字 (主にロシア語)、フランス語、ドイツ語、イタリア語、ポルトガル語、スペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.hockey

ホッケー専門のウェブサイトに使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

中国語、フランス語、ドイツ語、スペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.holdings

フィナンシャルアドバイザーや株式仲買人、投資関係で働く人が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.holiday

旅行業界の人、および、パーティの企画や特別な行事に関係する個人と企業が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.host

ウェブホスティングプラットフォームやサービスを提供する企業が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

アラビア語、簡体字中国語、繁体字中国語、ギリシャ語、ヘブライ語、韓国語、タイ語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます

- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.hosting

> **Important**
>
> 現在は、Route 53 を使用して新しい .hosting ドメインを登録したり、Route 53 に .hosting ドメインを移管したりすることはできません。Route 53 に登録済みの .hosting ドメインは引き続きサポートされます。

ホスティングのウェブサイトまたはホスティング業界が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

中国語、フランス語、ドイツ語、スペイン語に対してサポートされます。

移管に必要な認可コード

サポート外。.hosting ドメインは Route 53 に移管できなくなりました。

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.hot

トレンドのトピック、人気のあるコンテンツ、または時間的制約のあるオファーを含むウェブサイトに使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます

- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.house

不動産業者および住宅の購入者と販売者が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.how

「方法」から「方法」まですべてを探索するために、思想家、ティンカー、ナレッジシーカーが使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

制限

この TLD 上のすべてのウェブサイトに HTTPS が必要です。ドメインがブラウザで正しく動作するには、ウェブサイトに HTTPS を設定する必要があります。SSL 証明書を取得するためのリソースなど AWS、 で HTTPS を設定する方法の詳細については、「 とは AWS Certificate Manager」を参照してください。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます

- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.im

「.im (マン島)」を参照してください。

Return to index

.immo

不動産部門が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます

- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.immobilien

不動産に関する情報のために使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

中国語、フランス語、ドイツ語、スペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

サポート外。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.industries

業界として識別されることを希望する企業や商業エンタープライズが使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.info

情報を広めるために使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.ink

入れ墨の愛好家、または、印刷や出版業界などインクに関連する業界が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

アラビア語、ラテン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.institute

任意の組織またはグループ、特に研究および教育機関が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.insure

保険会社および保険代理店が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.international

国際的なチェーン展開をしている企業、世界を旅する個人、または国際的な影響力を持つ慈善団体が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.investments

全般的な拡張子として使用しますが、投資機会を宣伝するために最適です。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.io

「.io (英領インド洋地域)」を参照してください。

Return to index

.irish

アイルランドの文化と組織を宣伝するために使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

アラビア語、簡体字中国語、繁体字中国語、フランス語、ドイツ語、ギリシャ語、ヘブライ語、日本語、韓国語、スペイン語、タミル語、タイ語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.jewelry

宝石販売店および買付業者が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

中国語、フランス語、ドイツ語、スペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます

- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.juegos

> **Important**
>
> 現在は、Route 53 を使用して新しい .juegos ドメインを登録したり、Route 53 に .juegos ドメインを移管したりすることはできません。Route 53 に登録済みの .juegos ドメインは引き続きサポートされます。

あらゆる種類のゲームのウェブサイトに使用します。「Juegos」は、「ゲーム」を意味するスペイン単語です。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

キリル文字 (主にロシア語)、フランス語、ドイツ語、イタリア語、ポルトガル語、スペイン語に対してサポートされます。

移管に必要な認可コード

サポート外。.juegos ドメインは Route 53 に移管できなくなりました。

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.kaufen

e コマースに関する情報のために使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

中国語、フランス語、ドイツ語、ラテン語、スペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

サポート外。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます

- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.kim

姓または名前が Kim である人が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.kitchen

台所用品の小売業者、コック、食べ物ブロガー、食品業界の人が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.kiwi

ニュージーランドのキウィ文化をサポートしたい会社と個人が使用します。また、2010 年と 2011 年に地震による被害を受けたクライストチャーチの再建を支援する慈善事業のプラットフォームとしても使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

マオリ語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.land

農民、不動産業者、商用デベロッパー、および土地に興味を持つ人が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.law

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.lease

不動産業者、地主、および貸家人が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.legal

法律の専門家が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.lgbt

女性同性愛者、男性同性愛者、両性愛者、および性別越境者のコミュニティが使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート外。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.life

全般的な拡張子として使用しますが、さまざまな企業、団体、個人に適しています。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます

- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.lifestyle

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート外。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.lighting

写真家、デザイナー、建築家、エンジニアなど、照明に興味を持つ人が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.limited

全般的な拡張子として使用しますが、さまざまな企業、団体、個人に適しています。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.limo

運転手、リムジン会社、レンタカー業者が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.link

オンラインショートカットリンクの作成に関する情報のために使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護

Uniregistry とは、.LINK ドメイン向けのレジストリのことです。Uniregistry ポリシーがあるため、レジストリレベルで WHOIS を実行すると、「REDACTED FOR PRIVACY」と表示されます。プライバシー保護機能を削除しても、レジストラレベルの Amazon Registrar ルックアップに表示される情報にのみ影響します。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

キリル文字 (主にロシア語)、フランス語、ドイツ語、イタリア語、ポルトガル語、スペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.live

全般的な拡張子として使用しますが、さまざまな企業、団体、個人に適しています。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

中国語、フランス語、ドイツ語、ラテン語、スペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.living

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート外。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.llc

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます

- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.loan

貸付機関、借主、および信用情報機関が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

デンマーク語、ドイツ語、ノルウェー語、スウェーデン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.loans

貸付機関、借主、および信用情報機関が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.lol

ユーモアとコメディのウェブサイトに使用します。「LOL」は「laugh out loud (大笑いする)」の頭文字です。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

キリル文字、フランス語、ドイツ語、イタリア語、ポルトガル語、スペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.love

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.ltd

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.maison

不動産部門が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.management

ビジネスの世界と会社管理に関する情報のために使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます

- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.marketing

さまざまな目的のためにマーケティング部門が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.mba

経営学修士 (MBA) に関する情報を提供するウェブサイトに使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

中国語、フランス語、ドイツ語、スペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.media

メディアおよびエンターテインメント部門で使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.memorial

出来事や人に敬意を払う記念組織が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.メニュー

レストラン、カフェ、食品サービス企業がメニューを紹介するために使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.mobi

ウェブサイトを携帯電話でアクセスできるようにしたい会社と個人が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート外。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.moda

ファッションに関する情報のために使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

中国語、フランス語、ドイツ語、ラテン語、スペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

サポート外。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.moi

フランス語「me」 フランス語のコンテンツを Francophone エンドユーザーに通知するために使用されます。フランス語の個人ブログ、CVs、ポートフォリオ、趣味や興味のあるサイトに適しています。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

サポート対象。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.money

金銭および金銭関連の活動を専門とするウェブサイトに使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます

- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.mortgage

担保業界が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

中国語、フランス語、ドイツ語、ラテン語、スペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます

- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.mov

写真やその他の移動物を移動するために使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

制限

この TLD 上のすべてのウェブサイトに HTTPS が必要です。ドメインがブラウザで正しく動作するには、ウェブサイトに HTTPS を設定する必要があります。SSL 証明書を取得するためのリソースなど AWS、 で HTTPS を設定する方法の詳細については、「 とは AWS Certificate Manager」を参照してください。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます

- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.movie

映画や映画制作に関する情報を提供するウェブサイトに使用します。専門家とファンの両方に適しています。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

中国語、フランス語、ドイツ語、スペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます

- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.name

個別にウェブでの存在感を出したい方が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

制限

.name TLD のレジストリである Verisign では、セカンドレベルドメイン (name.name) とサードレベルドメイン (firstname .lastname .name) を登録できます。Route 53 は、ドメインの登録と、既存ドメインの Route 53 への移管のどちらの場合も、セカンドレベルドメインのみをサポートします。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます

- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.net

あらゆる種類のウェブサイトに使用します。.net 拡張子は network (ネットワーク) の省略表現です。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護

すべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.network

ネットワーク業界の人、またはネットワーキングを通じてつながりを持ちたい人が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.news

最新の出来事や、ジャーナリズムと通信に関連する情報など、報道価値がある情報を配布するために使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

中国語、フランス語、ドイツ語、ラテン語、スペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.nexus

オンラインで行っていることに合わせてすべてをまとめる安全なハブとして使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

制限

この TLD 上のすべてのウェブサイトに HTTPS が必要です。ドメインがブラウザで正しく動作するには、ウェブサイトに HTTPS を設定する必要があります。SSL 証明書を取得するためのリソースなど AWS、 で HTTPS を設定する方法の詳細については、「 とは AWS Certificate Manager」を参照してください。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.ninja

忍者の能力と自分を関連付けたい個人と企業が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

中国語、フランス語、ドイツ語、ラテン語、スペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.now

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.one

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート外。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.onl

.onl 拡張子は、online (オンライン) の省略表現であり、スペイン語では非営利組織を表す略語でもあります。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.online

.onl 拡張子は、online (オンライン) の省略表現であり、スペイン語では非営利組織を表す略語でもあります。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.org

あらゆる種類の組織が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護

すべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます

- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.page

シンプルで安全なオンラインプレゼンスを構築するために使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

制限

この TLD 上のすべてのウェブサイトに HTTPS が必要です。ドメインがブラウザで正しく動作するには、ウェブサイトに HTTPS を設定する必要があります。SSL 証明書を取得するためのリソースなど AWS、 で HTTPS を設定する方法の詳細については、「 とは AWS Certificate Manager」を参照してください。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます

- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.partners

法律事務所、投資家、およびさまざまな企業が使用します。また、人間関係を築くソーシャル Web サイトにも使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます

- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.parts

全般的な拡張子として使用しますが、部品の製造業者、販売業者、および買付業者に最適です。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.phd

博士号を持つすべての人が、出版物や成果を紹介するために使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

制限

この TLD 上のすべてのウェブサイトに HTTPS が必要です。ドメインがブラウザで正しく動作するには、ウェブサイトに HTTPS を設定する必要があります。SSL 証明書を取得するためのリソースなど AWS、 で HTTPS を設定する方法の詳細については、「 とは AWS Certificate Manager」を参照してください。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.photo

写真家や写真に関心を持つ人が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

キリル文字 (主にロシア語)、フランス語、ドイツ語、イタリア語、ポルトガル語、スペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.photography

写真家や写真に関心を持つ人が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.photos

写真家や写真に関心を持つ人が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.pics

写真家や写真に関心を持つ人が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

キリル文字 (主にロシア語)、フランス語、ドイツ語、イタリア語、ポルトガル語、スペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.pictures

写真、芸術、およびメディアに関心を持つ人が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.pink

ピンク色が好きな人、または、ピンク色をビジネスまたはブランドに関連付けたい人が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.pizza

ピザレストランとピザが好きな人が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.place

全般的な拡張子として使用しますが、住宅や旅行部門に最適です。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.plumbing

配管業界の人が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます

- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.plus

全般的な拡張子として使用しますが、大き目のサイズの服、アドオンソフトウェア、"追加" の機能または寸法を提供する商品に最適です。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

中国語、フランス語、ドイツ語、スペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.poker

ポーカーで遊ぶ人やゲームウェブサイトで使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート外。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.porn

成人向けウェブサイトに使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.press

成人向けウェブサイトに使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.pro

ライセンスまたは資格を持つ専門家や、専門家の団体が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート外。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.productions

コマーシャルやラジオ広告、ミュージックビデオを作成するスタジオや制作会社が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.prof

教員が、教員の認証情報、研究、出版物を紹介するために使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

制限

この TLD 上のすべてのウェブサイトに HTTPS が必要です。ドメインがブラウザで正しく動作するには、ウェブサイトに HTTPS を設定する必要があります。SSL 証明書を取得するためのリソースなど AWS、 で HTTPS を設定する方法の詳細については、「 とは AWS Certificate Manager」を参照してください。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

プロパティ

不動産または知的財産を含む、任意の種類の財産に関する情報に使用します。また、販売または賃貸する住宅、建物、土地を持つ人が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.property

不動産または知的財産を含む、任意の種類の財産に関する情報に使用します。また、販売または賃貸する住宅、建物、土地を持つ人が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

キリル文字 (主にロシア語)、フランス語、ドイツ語、イタリア語、ポルトガル語、スペイン語に対してサポートされます。

移管に必要な認可コード

サポート外。.property ドメインは Route 53 に移管できなくなりました。

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.pub

出版、広告、または醸造ビジネスの人が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

中国語、フランス語、ドイツ語、ラテン語、スペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.qpon

クーポンとプロモーションコードのために使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

スペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.realty

不動産業者、ブローカー、およびプロパティ関連企業が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます

- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.recipes

レシピを共有する人が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.red

赤色が好きな人、または、赤色をビジネスまたはブランドに関連付けたい人が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.reise

旅行に関連するウェブサイトに使用します。「Reise」は、「行動開始」または「旅行に出る」という意味のドイツ語です。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

中国語、フランス語、ドイツ語、スペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.reisen

旅行に関連するウェブサイトに使用します。「Reisen」は、ドイツ語で「旅行する」という意味です。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.rentals

あらゆる種類のレンタルに使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.repair

修理サービス、または、あらゆる種類の品目の修理方法を教えたい人が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.report

全般的な拡張子として使用しますが、ビジネスレポート、コミュニティの出版物、書籍のレポート、またはニュースのレポートに最適です。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.republican

共和党に関する情報のために使用されます。また、選挙で選出される公職の立候補者、当選した公職者、政治好き、コンサルタント、アドバイザーも使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

中国語、フランス語、ドイツ語、ラテン語、スペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.rest

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます

- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.restaurant

レストラン業界が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.reviews

自分の意見を表明し、他人のコメントを読みたい人が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

中国語、フランス語、ドイツ語、ラテン語、スペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

サポート外。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.rip

逝去と追悼を専門とするウェブサイトに使用します。「RIP」は「rest in peace (安らかに眠れ)」の頭文字です。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

中国語、フランス語、ドイツ語、ラテン語、スペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.rocks

全般的な拡張子として使用しますが、ミュージシャン、地質学者、宝飾関係、クライマーなど、「ロック」な関係者に最適です。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

中国語、フランス語、ドイツ語、ラテン語、スペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.rsvp

結婚式から資金集め、ビジネス会議まで、イベントや予約に使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

制限

この TLD 上のすべてのウェブサイトに HTTPS が必要です。ドメインがブラウザで正しく動作するには、ウェブサイトに HTTPS を設定する必要があります。SSL 証明書を取得するため

のリソースなど AWS、 で HTTPS を設定する方法の詳細については、「 とは AWS Certificate Manager」を参照してください。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.run

全般的な拡張子として使用しますが、フィットネスやスポーツ業界に最適です。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

中国語、フランス語、ドイツ語、スペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.sale

e コマースのウェブサイトで使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

中国語、フランス語、ドイツ語、ラテン語、スペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.sarl

通常はフランスにある有限会社が使用します。「SARL」は「Société à Responsabilité Limité (フランス法における有限会社)」の頭字語です。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.school

教育、教育機関、および学校関連活動に関する情報に使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.schule

ドイツの教育、教育機関、および学校関連活動に関する情報に使用します。「Schule」は、「学校」を意味するドイツ語です。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.services

任意の種類のサービスに特化したウェブサイトに使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.sex

成人向けコンテンツに使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます

- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.sexy

性的なコンテンツに使用されます。また、最も人気のあるエキサイティングなブランド、製品、情報、ウェブサイトを記述するのにも使用されます。

Return to index

> **Important**
>
> 現在は、Route 53 を使用して新しい .sexy ドメインを登録したり、Route 53 に .sexyドメインを移管したりすることはできません。Route 53 に登録済みの .sexyドメインは引き続きサポートされます。

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

キリル文字 (主にロシア語)、フランス語、ドイツ語、イタリア語、ポルトガル語、スペイン語に対してサポートされます。

移管に必要な認可コード

サポート外。.sexyドメインは Route 53 に移管できなくなりました。

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.shiksha

教育機関が使用します。「Shiksha」は学校を表すインドの言葉です。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます

- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.shoes

靴の小売業者、デザイナー、製造業者、またはファッションブロガーが使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.shop

オンラインおよびbrick-and-mortarの小売企業、サービスプロバイダーに使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.shopping

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.show

全般的な拡張子として使用しますが、エンターテインメント業界に最適です。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

中国語、フランス語、ドイツ語、スペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.singles

つながりをつくりたい人を対象とした出会い系サービス、リゾートなどの企業が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.site

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.ski

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.soccer

サッカー専門のウェブサイトに使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

中国語、フランス語、ドイツ語、スペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます

- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.social

ソーシャルメディア、フォーラム、オンライン会話に関する情報のために使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

中国語、フランス語、ドイツ語、ラテン語、スペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.solar

太陽系または太陽エネルギーに関する情報のために使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.solutions

あらゆる種類のコンサルタント、セルフサービス、アドバイザーが使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.software

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.soy

米国ヒスパニック市場のデジタルニーズ、ブランド、パブリッシャー、コンシューマーに使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

制限

この TLD 上のすべてのウェブサイトに HTTPS が必要です。ドメインがブラウザで正しく動作するには、ウェブサイトに HTTPS を設定する必要があります。SSL 証明書を取得するためのリソースなど AWS、 で HTTPS を設定する方法の詳細については、「 とは AWS Certificate Manager」を参照してください。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.space

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.spot

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.store

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます

- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.stream

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.studio

全般的な拡張子として使用しますが、不動産、芸術、またはエンターテインメント業界の人に最適です。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

中国語、フランス語、ドイツ語、ラテン語、スペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.style

全般的な拡張子として使用しますが、最新のトレンド (特にファッション、デザイン、建築、芸術) を専門とするウェブサイトに最適です。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.sucks

全般的な拡張子として使用しますが、ネガティブな体験を共有したい方や詐欺、詐称、欠陥商品について他者に警告を発したい方に最適です。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート外。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.supplies

商品をオンラインで販売するビジネスで使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.supply

商品をオンラインで販売するビジネスで使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.support

顧客、製品、システムのサポートや感情的、金銭的、精神的なサポートも含めて、あらゆる種類のサポートを提供する企業、グループまたは慈善団体が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.surgery

外科手術、医薬品、およびヘルスケアに関する情報に使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.systems

技術サービスを提供する人とテクノロジー業界が主として使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.tattoo

入れ墨の愛好家および入れ墨業界が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

キリル文字 (主にロシア語)、フランス語、ドイツ語、イタリア語、ポルトガル語、スペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます

- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.tax

税金、確定申告書作成、および税法に関する情報に使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.taxi

タクシー、運転手、およびシャトルバス会社が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

中国語、フランス語、ドイツ語、スペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.team

チームとして識別されることを希望する企業や組織が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

中国語、フランス語、ドイツ語、スペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.tech

テクノロジーの愛好家および、会社、サービス、製造元でテクノロジーを専門とする人が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.technology

テクノロジーの愛好家および、会社、サービス、製造元でテクノロジーを専門とする人が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.tennis

テニスに関連する情報に使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.theater

劇場、演劇、およびミュージカルを専門とするウェブサイトに使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

中国語、フランス語、ドイツ語、スペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.tienda

スペイン語を話す消費者とつながりたい小売企業が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.tips

事実上あらゆる話題について知識と助言を共有したい人が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.tires

タイヤの製造元、販売業者、または買付業者が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます

- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.today

現在のイベント、ニュース、天候、娯楽などに関する情報のために使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.tools

任意の種類の工具に関する情報に使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.tours

全般的な拡張子として使用しますが、旅行会社に最適です。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

中国語、フランス語、ドイツ語、スペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.town

市町村の場所、文化、およびコミュニティを宣伝するために使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.toys

玩具業界が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.trade

全般的な拡張子として使用しますが、コマースウェブサイトや取引サービスに最適です。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

デンマーク語、ドイツ語、ノルウェー語、スウェーデン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.training

トレーナー、コーチ、教育者が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.tv

テレビとメディアに関する情報のために使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

制限

なし。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート外。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.university

大学またはその他の教育組織が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.uno

スペイン語、ポルトガル語、イタリア語のコミュニティに関する情報のために使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

スペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.vacations

旅行業界と観光業界が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます

- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.vegas

ラスベガス市およびラスベガスのライフスタイルを宣伝するために使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート外。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.ventures

起業家、新興企業、ベンチャーキャピタル、投資銀行、金融業者が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.vg

「.vg (英領バージン諸島)」を参照してください。

Return to index

.viajes

旅行代理店、添乗員、旅行ブログ、ツアー会社、レンタルサービス、旅行ブロガー、旅行小売業者が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.video

メディアおよびビデオ産業が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

中国語、フランス語、ドイツ語、ラテン語、スペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.villas

販売または賃貸する別荘を待つ不動産業者と不動産所有者が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.vision

全般的な拡張子として使用されますが、検眼士や眼科医など、視力の専門家に最適です。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.vote

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.voyage

旅行代理店、添乗員、旅行ブログ、ツアー会社、レンタルサービス、旅行ブロガー、旅行小売業者が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.watch

ストリーミングウェブサイト、ウェブテレビ、ビデオ、または時計に関する情報のために使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.website

ウェブサイトの開発、宣伝、改善と経験に関する情報のために使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

アラビア語、簡体字中国語、繁体字中国語、ギリシャ語、ヘブライ語、日本語、韓国語、タイ語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます

- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.wedding

Return to index

登録および更新のリース期間

1 ~ 10 年。

制限

なし。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

中国語、フランス語、ドイツ語、スペイン語でサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.wiki

オンラインドキュメントに関する情報のために使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

アラビア語、ラテン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.win

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.wine

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護

サポート対象。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.work

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.works

仕事、職、雇用サービスに関する情報のために企業、組織、個人が使用します。この拡張子は、.com、.net、.org 拡張子の代わりとして使用できます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.world

世界的な題材に関する情報を提供したい人が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます

- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.wtf

人気のある頭文字 (俗語ですが) 「WTF」で識別されることを希望する人が使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.xxx

成人向けコンテンツをホストしているウェブサイトに使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.xyz

任意の目的で、全般的な拡張子として使用します。

Return to index

登録および更新のリース期間

1 ~ 10 年。

制限

.xyz ドメインのレジストリである Generation XYZ では、一部のドメイン名をプレミアムドメイン名とみなします。プレミアム .xyz ドメインを Route 53 に登録または移管することはできません。詳細については、Generation XYZ ウェブサイトを参照してください。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.zip

モノを結び付けたり、非常に速く移動したりするために使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

制限

この TLD 上のすべてのウェブサイトに HTTPS が必要です。ドメインがブラウザで正しく動作するには、ウェブサイトに HTTPS を設定する必要があります。SSL 証明書を取得するためのリソースなど AWS、 で HTTPS を設定する方法の詳細については、「 とは AWS Certificate Manager」を参照してください。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.zone

タイムゾーン、気候ゾーン、スポーツゾーンなど、あらゆる種類のゾーンに関する情報のために使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

フランス語およびスペイン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

地理的最上位ドメイン

以下のドメイン拡張子は、地域別にグループ分けした、国コード最上位ドメイン (ccTLD) と呼ばれる正式な国別拡張子です。例を挙げれば、.be (ベルギー)、.in (インド)、.mx (メキシコ) です。ccTLD の登録ルールは国によって異なります。制限のない国、つまり、世界中のだれでも登録できる国もあれば、住所など、一定の制限を設けている国もあります。各 ccTLD のリストには、制限事項が示されています。

> **Important**
>
> .cc と .tv を除くすべての ccTLD を Route 53 に移管する場合、所有者連絡先の更新は行われず、レジストリの所有者連絡先データが使用されます。移管が完了すると、連絡先情報を更新できます。詳細については、「ドメインの連絡先情報と所有者の更新」を参照してください。

Return to index

アフリカ

.ac (アセンション島), .co.za (南アフリカ), .sh (セントヘレナ)

アメリカ大陸

.ai (アンギラ), .ca (カナダ), .cl (チリ), .co (コロンビア), .com.ar (アルゼンチン), .com.br (ブラジル), .com.mx (メキシコ), .mx (メキシコ), .us (米国), .vc (セントビンセントおよびグレナディーン諸島), .vg (英領バージン諸島)

アジア/オセアニア

.au (オーストラリア), .cc (ココス (キーリング) 諸島), .co.nz (ニュージーランド), .com.au (オーストラリア), .com.sg (シンガポール共和国), .fm (ミクロネシア連邦), .in (インド), .jp (日本), .io (英領インド洋地域), .my (マレーシア), .net.au (オーストラリア), .net.nz (ニュージーランド), .nz (ニュージーランド), .org.nz (ニュージーランド), .pw (パラオ), .qa (カタール), .ru (ロシア連邦), .sg (シンガポール共和国)

欧州

.be (ベルギー), .berlin (ドイツのベルリン市), .ch (スイス), .co.uk (英国), .cz (チェコ共和国), .de (ドイツ), .es (スペイン), .eu (欧州連合), .fi (フィンランド), .fr (フランス), .gg (ガーンジー), .im (マン島), .it (イタリア), .me (モンテネグロ), .me.uk (英国), .nl (オランダ), .org.uk (英国), .ruhr (ドイツ西部のルール地域), .se (スウェーデン), .uk (英国), .wien (オーストリアのウィーン市)

アフリカ

Amazon Route 53 にドメインを登録するには、アフリカの次のトップレベルドメイン (TLD) を使用できます。

, ,

Return to index

.ac (アセンション島)

Return to index

高等教育機関でも、汎用 TLD として使用されます。

登録および更新のリース期間

1 年間。

制限

公開されており、制約はありません。

プライバシー保護

レジストリによって決定されます。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 80 日後、ドメインがレジストリから削除されます

.co.za (南アフリカ)

Return to index

登録および更新のリース期間

1 年間。

制限

.za 拡張子で使用できるのはセカンドレベルドメインのみです。Route 53 はセカンドレベルドメインの .co.za をサポートします。

公開されていますが、いくつか制約があります。

- 登録できるのは特定可能な法的存在 (個人と法人) です。
- ドメイン名は登録手続き中にゾーンチェックに合格する必要があります。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート外。

移管に必要な認可コード

いいえ

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れの 1 日前まで更新ができます
- Route 53 との遅延更新はできません
- 有効期限切れの 1 日前に、ドメインが Route 53: から削除されます
- 有効期限切れ後 1 日から 9 日までの間に、レジストリでの復元ができます
- 有効期限切れの 9 日後に、ドメインがレジストリから削除されます

.sh (セントヘレナ)

Return to index

登録および更新のリース期間

1 ~ 10 年。

制限

公開されており、制約はありません。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 80 日後、ドメインがレジストリから削除されます

アメリカ大陸

Amazon Route 53 にドメインを登録するには、アメリカの次のトップレベルドメイン (TLD) を使用できます。

, , , , , , , , , ,

Return to index

.ai (アンギラ)

Return to index

登録および更新のリース期間

登録: 2 ~ 10 年。更新: 2 ~ 9 年。

制限事項

公開されており、制約はありません。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート外。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- Route 53 での遅延更新が可能: 有効期限の 45 日後まで
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.ca (カナダ)

Return to index

ドメイン名のバリアント (アクセントマークがある (à)、またはない (a)) は、自動的に登録者に予約され、管理バンドルの一部になります。バンドル内のドメインをアクティブ化するには、登録者がドメインの登録リクエストを行う必要があります。バンドル内のすべてのドメインは、同じ登録者と同じレジストラによって登録される必要があります。また、移管を完了するには、登録者は、バンドル内のすべてのドメインの移管リクエストを送信する必要があります。

TLD レジストリからの確認メール

.ca ドメインを登録すると、登録規約の承認手続きへのリンクが記載されたメールが届きます。手続きは 7 日以内に完了する必要があります。そうしないと、ドメインは登録されません。

登録および更新のリース期間

1 ~ 10 年。

制限

公開されていますが、いくつか制約があります。

- 登録できるのはカナダとつながりのある個人または組織です。「Canadian Presence Requirements for Registrants」に要件が説明されています。
- 登録者の連絡先: ドメイン所有者の完全で正確な法的に正式な名称を指定する必要があります。
- 管理者と技術担当者の連絡先: 連絡先のタイプとして [Person] を指定し、カナダに住んでいる個人の連絡先情報を指定する必要があります。
- 登録手続きの際に次のような法的タイプの 1 つを選択する必要があります。
  - ABO: カナダ先住民族 (個人またはグループ)
  - ASS: カナダの法人格のない団体
  - CCO: カナダの法人、またはカナダの州や準州
  - CCT: カナダ市民
  - EDU: カナダの教育機関
  - GOV: カナダの政府または政府機関
  - HOP: カナダの病院
  - INB: インドのインディアン法で認知されたインディアンバンド
  - LAM: カナダの図書館、アーカイブ、または博物館

- LGR: カナダ市民または永住者の法定代理人
- MAJ: 女王陛下/国王陛下
- OMK: カナダで登録された正式マーク
- PLT: カナダの政党
- PRT: カナダで登録されたパートナーシップ
- RES: カナダの永住者
- TDM: カナダで登録された商標 (カナダ以外の所有者タイプ)
- TRD: カナダの労働組合
- TRS: カナダで設立された信託

プライバシー保護

- 個人 – CIRA はプライバシー保護を自動的に個人に適用するため、すべての連絡先の、連絡先の名前、住所、電話番号、ファックス番号、E メールアドレスは非表示になります。プライバシー保護オプションは、レジストラ Whois にのみ適用されます。
- 会社、協会、公共団体 - 登録レベルではサポート外。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- ドメインがレジストリから削除されます。有効期限は可変です。AWS Support へのお問い合わせ

ドメイン登録の削除

.ca ドメインのレジストリはドメイン登録を削除することができません。代わりに、自動更新を無効にして、ドメインの有効期限が切れるまで待つ必要があります。詳細については、「ドメイン名登録の削除」を参照してください。

.cl (チリ)

> **Important**
>
> 現在は、Route 53 を使用して新しい .cl ドメインを登録したり、Route 53 に .cl ドメインを移管したりすることはできません。Route 53 に登録済みの .cl ドメインは引き続きサポートされます。

Return to index

更新期間

2 年間。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート外。RetrieveDomainAuthCode APIアクションへのアクセスを制限して、不正な転送を防ぐことをお勧めします。(この Route 53 API へのアクセスを制限すると、Route 53 コンソール、 AWS SDK、およびその他のプログラムによる手法を使用して認可コードを生成できるユーザーも制限されます) 詳細については、「Amazon Route 53 での Identity and Access Management」を参照してください。

移管に必要な認可コード

サポート外。.cl ドメインは Route 53 に移管できなくなりました。

DNSSEC

サポート外。

ドメインの更新と復元の期限

- 更新ができます。AWS Support にお問い合わせください。

- Route 53 との遅延更新ができます。AWS Support にお問い合わせください。
- ドメインが Route 53 から削除されます。AWS Support にお問い合わせください。
- レジストリでの復元ができます。AWS Support にお問い合わせください。
- ドメインがレジストリから削除されます。AWS Support にお問い合わせください。

.co (コロンビア)

Return to index

登録および更新のリース期間

1 ~ 5 年。

制限事項

公開されており、制約はありません。

プライバシー保護 (適用対象: 個人)

すべての情報が非表示になります。

連絡先の種類が個人でない場合は、WHOIS により会社名と国が表示されます。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 29 日後まで Route 53 との遅延更新ができます
- 有効期限から 30 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 30 日から 45 日までの間、レジストリでの復元ができます

- 有効期限切れの 50 日後、ドメインがレジストリから削除されます

.com.ar (アルゼンチン)

> **Important**
>
> 現在は、Route 53 を使用して新しい .com.ar ドメインを登録したり、Route 53 に .com.ar ドメインを移管したりすることはできません。Route 53 に登録済みの .com.ar ドメインは引き続きサポートされます。

Return to index

更新期間

1 年間。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート外。不正な転送を防ぐには、登録者のメールアドレスと、所有権の変更を許可する Route 53 API へのアクセスを制限します。例えば、UpdateDomainContact。詳細については、「サービス承認リファレンス」の「Amazon Route 53 Domains のアクション、リソース、および条件キー」、および「ドメインレコード所有者のアクセス許可の例」を参照してください。

移管に必要な認可コード

サポート外。.com.ar ドメインは Route 53 に移管できなくなりました。

DNSSEC

サポート外。

ドメインの更新と復元の期限

- 更新ができます。AWS Support にお問い合わせください。
- Route 53 との遅延更新ができます。AWS Support にお問い合わせください。
- ドメインが Route 53 から削除されます。AWS Support にお問い合わせください。
- レジストリでの復元ができます。AWS Support にお問い合わせください。
- ドメインがレジストリから削除されます。AWS Support にお問い合わせください。

.com.br (ブラジル)

> **Important**
>
> 現在は、Route 53 を使用して新しい .com.br ドメインを登録したり、Route 53 に .com.br ドメインを移管したりすることはできません。Route 53 に登録済みの .com.br ドメインは引き続きサポートされます。

Return to index

更新期間

1 年間。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート対象。

移管に必要な認可コード

サポート外。.com.br ドメインは Route 53 に移管できなくなりました。

DNSSEC

サポート外。

ドメインの更新と復元の期限

- 有効期限の 30 日前から有効期限日までの間、更新ができます
- 有効期限切れの 119 日後まで Route 53 との遅延更新ができます
- 有効期限から 119 日後にドメインが Route 53 から削除されます
- レジストリでの復元はできません
- 有効期限切れの 119 日後、ドメインがレジストリから削除されます

.com.mx (メキシコ)

Return to index

登録および更新のリース期間

1 ~ 10 年。

制限

公開されており、制約はありません。

プライバシー保護

レジストリによって決定されます。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート外。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.mx (メキシコ)

Return to index

登録および更新のリース期間

1 ~ 10 年。

制限

公開されており、制約はありません。

プライバシー保護

レジストリによって決定されます。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート外。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.us (米国)

Return to index

登録および更新のリース期間

1 ~ 10 年。

制限

.us ドメインのレジストリでは、「Federal Communications Commission v. Pacifica Foundation No. 77-528」の「Appendix to Opinion of the Court」で明示されている、7 つの言葉をドメイン名に含むことはできません。

公開されており、1 つの制約があります。

- .us 拡張子は、米国に拠点を置くウェブサイトまたは活動向けです。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート外。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 29 日後まで Route 53 との遅延更新ができます
- 有効期限から 30 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 30 日から 60 日までの間、レジストリでの復元ができます
- 有効期限切れから 65 日後、ドメインがレジストリから削除されます

.vc (セントビンセントおよびグレナディーン諸島)

ベンチャーキャピタルや (主にイギリスの) 大学などが関係するドメインで、汎用 TLD としても使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

制限

公開されており、制約はありません。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

すべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート外。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 80 日後、ドメインがレジストリから削除されます

.vg (英領バージン諸島)

ビデオゲームが関係する組織でも、一般的な TLD としてよく使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

制限

公開されており、制約はありません。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート外。

移管に必要な認可コード

はい

DNSSEC

サポート外。

ドメインの更新と復元の期限

- 有効期限の 44 日後まで更新できます
- Route 53 との遅延更新はできます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れの 45 日後、ドメインがレジストリから削除されます
- 有効期限切れ後 45 日から 74 日までの間、レジストリでの復元ができます
- ドメインは有効期限から 80 日後に再び公開されます

アジア/オセアニア

Amazon Route 53 にドメインを登録するには、アジアおよびオセアニアの次のトップレベルドメイン (TLD) を使用できます。

, , , , , , , , , , , , , , , , ,

Return to index

.au (オーストラリア)

Return to index

TLD レジストリからの確認メール

当社のレジストラアソシエイトである Gandi が、DomainDirectors を通じて「.au」ドメインを再販売しています。ドメイン名を Route 53 に移転すると、DomainDirectors がドメインの登録者の連絡先にメールを送信して、連絡先情報の確認を依頼または移管リクエストを承認します。

登録および更新のリース期間

1 ~ 5 年。

制限

公開されていますが、いくつか制約があります。

- .au ドメインを使用できるのは、オーストラリアに登録されている法人、共同事業者、個人事業主、オーストラリアで事業が許可されている外国企業、オーストラリアで登録された商標の所有者または申請者です。個人は .au ドメインを登録できません。登録者の連絡先は会社である必要があります。
- 登録手続きの際に、以下を指定する必要があります。
  - 登録タイプ: ABN (オーストラリアビジネス番号)、ACN (オーストラリア会社番号)、またはドメイン名が商標に相当する場合は TM (商標)。
  - ID 番号: ABN (オーストラリアビジネス番号)、ACN (オーストラリア会社番号)、TM (商標) である場合があります。
  - 登録者名。これは、ドメインを登録する法人の名前です。この値は、指定された ABN (オーストラリア企業番号)、ACN (オーストラリア企業番号)、または TM (商標) の名前と完全に一致する必要があります。
  - 適格性タイプ。ドメイン名を登録する法人のタイプを指します。
  - このドメイン名の登録が許可されている理由 (ポリシーの理由):
    - ドメイン名は、登録者の会社名または商号、組織または関連付け名、または商標の頭字語または略語と一致します。(ポリシーの理由 1)
    - ドメイン名は割り当てルールを満たしていますが、発行者の会社名、取引名、組織名、関連付け名、商標の頭字語または略語ではありません。(ポリシーの理由 2)。.au の割り当てルールを表示するには、.au レジストリの「スケジュール A」を参照してください。
- 連絡先情報 (氏名、ABN、商標 (TM) 番号など) が間違っていたり一致しなかったりすると、登録、取引、更新に失敗します。既存のドメインの情報を修正するには、所有権の変更が必要になる場合があります。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート外。RetrieveDomainAuthCode APIアクションへのアクセスを制限して、不正な転送を防ぐことをお勧めします。(この Route 53 API へのアクセスを制限すると、Route 53 コン

ソール、 AWS SDK、およびその他のプログラムによる手法を使用して認可コードを生成できるユーザーも制限されます) 詳細については、「Amazon Route 53 での Identity and Access Management」を参照してください。

国際化ドメイン名

サポート外。

移管に必要な認可コード

はい。Route 53 コンソールに加えて、.au レジストリから転送コードを取得することもできます。

DNSSEC

ドメイン登録でサポートされています。キーを設定するときは、DNS セキュリティアルゴリズム 2 (DH) を選択する必要があります。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限の 60 日前から有効期限日までの間、更新ができます
- 有効期限切れの 29 日後まで Route 53 との遅延更新ができます
- 有効期限から 29 日後にドメインが Route 53 から削除されます
- レジストリでの復元はできません
- 有効期限切れから 30 日後、ドメインがレジストリから削除されます

ドメイン登録の削除

.au ドメインの登録ではドメイン登録を削除することができません。代わりに、自動更新を無効にして、ドメインの有効期限が切れるまで待つ必要があります。詳細については、「ドメイン名登録の削除」を参照してください。

所有権の変更

Route 53 コンソールを使用して所有者を変更します。「ドメインの連絡先情報の更新」を参照してください。次に、以下のプロセスを完了させて所有権の変更を完了します:

1. 古い登録者と新しい登録者の両方が、transfers@1api.net から E メールで受信したリンクを、リストされている E メールアドレスに選択する必要があります。14 日以内にプロセスが完了しない場合、再度開始する必要があります。

2. 応答が確認された後、レジストリ内の所有者の変更はそれ以上確認することなく、短時間で処理されます。

.cc (ココス (キーリング) 諸島)

Return to index

コンサルティング会社やサイクリングクラブなどの名前に "cc" がついている組織でも、汎用 TLD としてよく使用されます。この拡張子は ".com" に代わるよくある表現です。

登録および更新のリース期間

1 ~ 10 年。

制限

公開されており、制約はありません。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

- 非表示 - 住所、電話番号、FAX 番号、メールアドレス
- 表示 - 連絡先名と組織名

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート外。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 30 日から 60 日までの間、レジストリでの復元ができます
- 有効期限切れから 65 日後、ドメインがレジストリから削除されます

.co.nz (ニュージーランド)

Return to index

登録および更新のリース期間

1 ~ 10 年。

制限

公開されていますが、いくつか制約があります。

- 個人は 18 歳以上でなくてはいけません。
- 組織は登録されている必要があります。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート外。RetrieveDomainAuthCode APIアクションへのアクセスを制限して、不正な転送を防ぐことをお勧めします。(この Route 53 API へのアクセスを制限すると、Route 53 コンソール、 AWS SDK、およびその他のプログラムによる手法を使用して認可コードを生成できるユーザーも制限されます) 詳細については、「Amazon Route 53 での Identity and Access Management」を参照してください。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 44 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 44 日から 134 日までの間、レジストリでの復元ができます
- 有効期限切れの 134 日後、ドメインがレジストリから削除されます

.com.au (オーストラリア)

Return to index

TLD レジストリからの確認メール

当社のレジストラアソシエイトである Gandi が、DomainDirectors を通じて「.com.au」ドメインを再販売しています。ドメイン名を Route 53 に移転すると、DomainDirectors がドメインの登録者の連絡先にメールを送信して、連絡先情報の確認を依頼または移管リクエストを承認します。

登録および更新のリース期間

1 ~ 5 年。

制限

公開されていますが、いくつか制約があります。

- .com.au ドメインと .net.au ドメインを使用できるのは、オーストラリアに登録されている共同事業者と個人事業主、オーストラリアで事業が許可されている外国企業、オーストラリアで登録された商標の所有者または申請者です。個人が .com.au または .net.au ドメインを登録することはできません。登録者の連絡先は会社である必要があります。
- ドメイン名は、 (該当するオーストラリアの機関に登録された) お客様の名称、またはお客様の登録商標 (または商標の省略形か頭字語) と同一である必要があります。
- ドメイン名はお客様の活動を示す必要があります。例えば、販売する製品や提供するサービスを示す必要があります。
- 登録手続きの際に、以下の情報を指定する必要があります。
  - 登録タイプ: ABN (オーストラリアビジネス番号)、ACN (オーストラリア会社番号)、またはドメイン名が商標に相当する場合は TM (商標)。
  - ID 番号: ABN (オーストラリアビジネス番号)、ACN (オーストラリア会社番号)、またはドメイン名が商標に相当する場合は TM (商標) である場合があります。
  - 登録者名。これは、ドメインを登録する法人の名前です。この値は、指定された名前と完全に一致する必要があります。
  - 適格性タイプ。これは、このドメイン名を登録する法人のタイプを指します。
  - このドメイン名の登録が許可されている理由 (ポリシーの理由):
    - ドメイン名は、登録者の会社名または商号、組織または関連付け名、または商標の頭字語または略語と一致します。(ポリシーの理由 1)
    - ドメイン名は割り当てルールを満たしていますが、発行者の会社名、取引名、組織名、関連付け名、商標の頭字語または略語ではありません。(ポリシーの理由 2)。.com.au の割

り当てルールを確認するには、.com.au レジストリの「SCHEDULE C」を参照してください。

- 連絡先情報 (氏名、ABN、商標 (TM) 番号など) が間違っていたり一致しなかったりすると、登録、取引、更新に失敗します。既存のドメインの情報を修正するには、所有権の変更が必要になる場合があります。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート外。RetrieveDomainAuthCode APIアクションへのアクセスを制限して、不正な転送を防ぐことをお勧めします。(この Route 53 API へのアクセスを制限すると、Route 53 コンソール、 AWS SDK、およびその他のプログラムによる手法を使用して認可コードを生成できるユーザーも制限されます) 詳細については、「Amazon Route 53 での Identity and Access Management」を参照してください。

国際化ドメイン名

サポート外。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。キーを設定するときは、DNS セキュリティアルゴリズム 2 (DH) を選択する必要があります。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限の 60 日前から有効期限日までの間、更新ができます
- 有効期限切れの 29 日後まで Route 53 との遅延更新ができます
- 有効期限から 29 日後にドメインが Route 53 から削除されます
- レジストリでの復元はできません
- 有効期限切れから 30 日後、ドメインがレジストリから削除されます

ドメイン登録の削除

.com.au ドメインのレジストリはドメイン登録を削除することができません。代わりに、自動更新を無効にして、ドメインの有効期限が切れるまで待つ必要があります。詳細については、「ドメイン名登録の削除」を参照してください。

所有権の変更

プログラムまたは Route 53 コンソールを使用して所有者を変更します。「ドメインの連絡先情報の更新」を参照してください。次に、以下のプロセスを完了させて所有権の変更を完了します:

1. 古い登録者と新しい登録者の両方が、transfers@1api.net から E メールで受信したリンクを、リストされている E メールアドレスに選択する必要があります。14 日以内にプロセスが完了しない場合、再度開始する必要があります。

2. 応答が確認された後、レジストリ内の所有者の変更はそれ以上確認することなく、短時間で処理されます。

.com.sg (シンガポール共和国)

> **Important**
>
> 現在は、Route 53 を使用して新しい .com.sg ドメインを登録したり、Route 53 に .com.sg ドメインを移管したりすることはできません。Route 53 に登録済みの .com.sg ドメインは引き続きサポートされます。

Return to index

更新期間

1 年または 2 年

ドメイン登録の削除

.com.sg ドメインのレジストリはドメイン登録を削除することができません。代わりに、自動更新を無効にして、ドメインの有効期限が切れるまで待つ必要があります。詳細については、「ドメイン名登録の削除」を参照してください。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート対象。

移管に必要な認可コード

サポート外。.com.sg ドメインは Route 53 に移管できなくなりました。

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 29 日後まで Route 53 との遅延更新ができます
- 有効期限から 30 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 30 日から 60 日までの間、レジストリでの復元ができます
- 有効期限切れから 60 日後、ドメインがレジストリから削除されます

.fm (ミクロネシア連邦)

オンラインメディアと放送が関係する組織でも、汎用 TLD としてよく使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

制限

公開されており、制約はありません。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

サポート外。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 44 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 44 日から 79 日までの間、レジストリでの復元ができます
- 有効期限切れから 84 日後、ドメインがレジストリから削除されます

.in (インド)

Return to index

> **Important**
>
> ドメインのステータスが serverHold の場合は、.IN レジストリ (NIXI - National Internet Exchange of India) に直接問い合わせて解決する必要があります。NIXI では、ステータスを解除するために連絡先情報の検証が必要になる場合があります。その場合、写真付き ID と住所の証明を提供する必要があります。
> NIXI へのお問い合わせは、support@nixi.in までご連絡ください。

登録および更新のリース期間

1 ~ 10 年。

制限

公開されており、制約はありません。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート外。

移管に必要な認可コード

はい

DNSSEC

サポート外。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 29 日後まで Route 53 との遅延更新ができます
- 有効期限から 30 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 30 日から 60 日までの間、レジストリでの復元ができます
- 有効期限切れから 65 日後、ドメインがレジストリから削除されます

.jp (日本)

Return to index

登録および更新のリース期間

1 年間。

制限

公開されており、1 つの制約があります。

- .jp ドメイン名は日本の個人または会社のみが登録できます。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート外。RetrieveDomainAuthCode APIアクションへのアクセスを制限して、不正な転送を防ぐことをお勧めします。(この Route 53 API へのアクセスを制限すると、Route 53 コンソール、 AWS SDK、およびその他のプログラムによる手法を使用して認可コードを生成できるユーザーも制限されます) 詳細については、「Amazon Route 53 での Identity and Access Management」を参照してください。

国際化ドメイン名

日本語に対してサポートされます。

移管に必要な認可コード

はい。

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 更新可能: 有効期限の 16 日前まで
- Route 53 との遅延更新はできません
- 有効期限の 6 日前、ドメインが Route 53: から削除されます
- レジストリでの復元ができます。AWS Support にお問い合わせください。
- ドメインがレジストリから削除されます。AWS Support にお問い合わせください。

> **Note**
>
> 現在、.co.jp、.or.jp などの汎用以外の JP ドメインを登録することはできません。

.io (英領インド洋地域)

オンラインサービスやオンラインゲームなどのコンピューター関連組織でも、汎用 TLD としてよく使用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

制限

公開されており、制約はありません。

プライバシー保護

州 / 地域および国を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

.io ドメインのレジストリでは、プライバシー保護の有効化や無効化など、一部のオペレーションに対して認可コードをワンタイムパスワードとしても使用します。パスワードが必要なオペレーションを複数実行する場合は、オペレーションごとに異なる認可コードを生成する必要があります。

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れの 90 日後、ドメインがレジストリから削除されます

.my (マレーシア)

> **Important**
>
> 2024 年 8 月以降、イスラエルの居住者は .my ドメインを登録できません。この制限は、イスラエルのロケーションへの住所の変更を含む、新しい登録と変更の両方に適用されます。

Return to index

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート外。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.net.au (オーストラリア)

Return to index

TLD レジストリからの確認メール

当社のレジストラアソシエイトである Gandi は、DomainDirectors を通じて「.net.au」ドメインを再販売しています。ドメイン名を Route 53 に移転すると、DomainDirectors がドメインの登録者の連絡先にメールを送信して、連絡先情報の確認を依頼または移転リクエストを承認します。

登録および更新のリース期間

1 ~ 5 年。

制限

公開されていますが、いくつか制約があります。

- .com.au ドメインと .net.au ドメインを使用できるのは、オーストラリアに登録されている法人、共同事業者、個人事業主、オーストラリアで事業が許可されている外国企業、オーストラリアで登録された商標の所有者または申請者です。
- ドメイン名は、該当するオーストラリアの機関に登録されたお客様の名称、またはお客様の登録商標 (またはその省略形か頭字語) と同一である必要があります。
- ドメイン名はお客様の活動を示す必要があります。例えば、販売する製品や提供するサービスを示す必要があります。
- 登録手続きの際に、以下を指定する必要があります。
  - 登録タイプ: ABN (オーストラリアビジネス番号)、ACN (オーストラリア会社番号)、またはドメイン名が商標に相当する場合は TM (商標)。
  - ID 番号: ABN (オーストラリアビジネス番号)、ACN (オーストラリア会社番号)、またはドメイン名が商標に相当する場合は TM (商標) である場合があります。
  - 登録者名。これは、ドメインを登録する法人の名前です。この値は、指定された名前と完全に一致する必要があります。
  - 適格性タイプ。これは、このドメイン名を登録する法人のタイプを指します。
  - このドメイン名の登録が許可されている理由 (ポリシーの理由):
    - ドメイン名は、登録者の会社名または商号、組織または関連付け名、または商標の頭字語または略語と一致します。(ポリシーの理由 1)
    - ドメイン名は割り当てルールを満たしていますが、発行者の会社名、取引名、組織名、関連付け名、商標の頭字語または略語ではありません。(ポリシーの理由 2)。.net.au の割り当てルールを表示するには、net.au レジストリの「SCHEDULE E」を参照してください。
- 連絡先情報 (氏名、ABN、商標 (TM) 番号など) が間違っていたり一致しなかったりすると、登録、取引、更新に失敗します。既存のドメインの情報を修正するには、所有権の変更が必要になる場合があります。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート外。RetrieveDomainAuthCode APIアクションへのアクセスを制限して、不正な転送を防ぐことをお勧めします。(この Route 53 API へのアクセスを制限すると、Route 53 コン

ソール、 AWS SDK、およびその他のプログラムによる手法を使用して認可コードを生成できるユーザーも制限されます) 詳細については、「Amazon Route 53 での Identity and Access Management」を参照してください。

国際化ドメイン名

サポート外。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。キーを設定するときは、DNS セキュリティアルゴリズム 2 (DH) を選択する必要があります。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限の 60 日前から有効期限日までの間、更新ができます
- 有効期限切れの 29 日後まで Route 53 との遅延更新ができます
- 有効期限から 29 日後にドメインが Route 53 から削除されます
- レジストリでの復元はできません
- 有効期限切れから 30 日後、ドメインがレジストリから削除されます

ドメイン登録の削除

.net.au ドメインのレジストリはドメイン登録を削除することができません。代わりに、自動更新を無効にして、ドメインの有効期限が切れるまで待つ必要があります。詳細については、「ドメイン名登録の削除」を参照してください。

所有権の変更

プログラムまたは Route 53 コンソールを使用して所有者を変更します。「ドメインの連絡先情報の更新」を参照してください。次に、以下のプロセスを完了させて所有権の変更を完了します:

1. 古い登録者と新しい登録者の両方が、transfers@1api.net から E メールで受信したリンクを、リストされている E メールアドレスに選択する必要があります。14 日以内にプロセスが完了しない場合、再度開始する必要があります。

2. 応答が確認された後、レジストリ内の所有者の変更はそれ以上確認することなく、短時間で処理されます。

.net.nz (ニュージーランド)

Return to index

登録および更新のリース期間

1 ~ 10 年。

制限

公開されていますが、いくつか制約があります。

- 個人は 18 歳以上でなくてはいけません。
- 組織は登録されている必要があります。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート外。RetrieveDomainAuthCode APIアクションへのアクセスを制限して、不正な転送を防ぐことをお勧めします。(この Route 53 API へのアクセスを制限すると、Route 53 コンソール、 AWS SDK、およびその他のプログラムによる手法を使用して認可コードを生成できるユーザーも制限されます) 詳細については、「Amazon Route 53 での Identity and Access Management」を参照してください。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 44 日後にドメインが Route 53 から削除されます

- 有効期限切れ後 44 日から 134 日までの間、レジストリでの復元ができます
- 有効期限切れの 134 日後、ドメインがレジストリから削除されます

.nz (ニュージーランド)

Return to index

登録および更新のリース期間

1 ~ 10 年。

制限

公開されていますが、いくつか制約があります。

- 個人は 18 歳以上でなくてはいけません。
- 組織は登録されている必要があります。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート外。RetrieveDomainAuthCode APIアクションへのアクセスを制限して、不正な転送を防ぐことをお勧めします。(この Route 53 API へのアクセスを制限すると、Route 53 コンソール、 AWS SDK、およびその他のプログラムによる手法を使用して認可コードを生成できるユーザーも制限されます) 詳細については、「Amazon Route 53 での Identity and Access Management」を参照してください。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます

- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 44 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 44 日から 134 日までの間、レジストリでの復元ができます
- 有効期限切れの 134 日後、ドメインがレジストリから削除されます

.org.nz (ニュージーランド)

Return to index

登録および更新のリース期間

1 ~ 10 年。

制限

公開されていますが、いくつか制約があります。

- 個人は 18 歳以上でなくてはいけません。
- 組織は登録されている必要があります。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート外。RetrieveDomainAuthCode APIアクションへのアクセスを制限して、不正な転送を防ぐことをお勧めします。(この Route 53 API へのアクセスを制限すると、Route 53 コンソール、 AWS SDK、およびその他のプログラムによる手法を使用して認可コードを生成できるユーザーも制限されます) 詳細については、「Amazon Route 53 での Identity and Access Management」を参照してください。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 44 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 44 日から 134 日までの間、レジストリでの復元ができます
- 有効期限切れの 134 日後、ドメインがレジストリから削除されます

.pw (パラオ)

Return to index

.pw は、もともと西太平洋のオセアニアのミクロネシア準リージョンにある島国であるパラオの居住者のために予約されましたが、現在は「Professional Web」を表すために一般的に使用され、誰でも利用できます。

登録および更新のリース期間

1 ~ 10 年。

プライバシー保護 (連絡先タイプ Person、Company、Association、Public Body のすべてに適用されます)

組織名を除くすべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます

- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 75 日後、ドメインがレジストリから削除されます

.qa (カタール)

> **Important**
>
> 現在は、Route 53 を使用して新しい .qa ドメインを登録したり、Route 53 に .qa ドメインを移管したりすることはできません。Route 53 に登録済みの .qa ドメインは引き続きサポートされます。

Return to index

更新期間

1 ~ 5 年。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート外。RetrieveDomainAuthCode APIアクションへのアクセスを制限して、不正な転送を防ぐことをお勧めします。(この Route 53 API へのアクセスを制限すると、Route 53 コンソール、 AWS SDK、およびその他のプログラムによる手法を使用して認可コードを生成できるユーザーも制限されます) 詳細については、「Amazon Route 53 での Identity and Access Management」を参照してください。

移管に必要な認可コード

サポート外。.qa ドメインは Route 53 に移管できなくなりました。

DNSSEC

サポート外。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます

- 有効期限切れの 29 日後まで Route 53 との遅延更新ができます
- 有効期限から 30 日後にドメインが Route 53 から削除されます
- レジストリでの復元はできません
- 有効期限切れから 31 日後、ドメインがレジストリから削除されます

.ru (ロシア連邦)

> **Important**
>
> Route 53 を使用して新しい .ru ドメインを登録したり、.ru ドメインを Route 53 に転送したり、既存の .ru ドメインを Route 53 で更新したりすることはできなくなりました。Route 53 で既存の .ru ドメインがある場合は、サービスの中断を避けるために、すぐに .ru をサポートするレジストラに転送します。

Return to index

登録および更新のリース期間

1 年間。

> **Note**
>
> .ru ドメインのレジストリは、ドメインの有効期限が切れる日にドメインの有効期限を更新します。WHOIS クエリでは、Route 53 でドメインを更新した時期に関係なく、その日付までのドメインの古い有効期限が表示されます。

制限

公開されていますが、いくつか制約があります。

- 個人は、パスポート番号または政府が発行する ID 番号の入力が必要になる可能性があります。
- 外国企業は、会社 ID または会社登録の入力が必要になる可能性があります。

プライバシー保護

レジストリによって決定されます。

不正な移管を防ぐためのドメインロック

サポート外。RetrieveDomainAuthCode APIアクションへのアクセスを制限して、不正な転送を防ぐことをお勧めします。(この Route 53 API へのアクセスを制限すると、Route 53 コンソール、 AWS SDK、およびその他のプログラムによる手法を使用して認可コードを生成できるユーザーも制限されます) 詳細については、「Amazon Route 53 での Identity and Access Management」を参照してください。

国際化ドメイン名

サポート外。

移管に必要な認可コード

サポート外。.ru ドメインは Route 53 に移管できなくなりました。

DNSSEC

サポート外。

ドメインの更新と復元の期限

サポート外。Route 53 で .ru ドメインを更新または復元することはできなくなりました。

ドメイン登録の削除

.ru ドメインのレジストリはドメイン登録を削除することができません。代わりに、自動更新を無効にして、ドメインの有効期限が切れるまで待つ必要があります。詳細については、「ドメイン名登録の削除」を参照してください。

.sg (シンガポール共和国)

> **Important**
>
> 現在は、Route 53 を使用して新しい .sg ドメインを登録したり、Route 53 に .sg ドメインを移管したりすることはできません。Route 53 に登録済みの .sg ドメインは引き続きサポートされます。

Return to index

更新期間

1 年または 2 年

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート対象。

移管に必要な認可コード

サポート外。.sg ドメインは Route 53 に移管できなくなりました。

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 29 日後まで Route 53 との遅延更新ができます
- 有効期限から 30 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 30 日から 60 日までの間、レジストリでの復元ができます
- 有効期限切れから 60 日後、ドメインがレジストリから削除されます

ドメイン登録の削除

.sg ドメインのレジストリはドメイン登録を削除することができません。代わりに、自動更新を無効にして、ドメインの有効期限が切れるまで待つ必要があります。詳しくは、ドメイン名登録の削除 を参照してください。

欧州

Amazon Route 53 にドメインを登録するには、ヨーロッパの次のトップレベルドメイン (TLD) を使用できます。

, ,

Return to index

.be (ベルギー)

Return to index

登録および更新のリース期間

1 年間。

制限

公開されており、制約はありません。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい。移管コードは DNS ベルギーのウェブサイトから取得できます。

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- Route 53 との遅延更新はできません
- 有効期限日にドメインが Route 53 から削除されます
- 有効期限の 40 日後まで、レジストリでの復元ができます
- 有効期限切れから 40 日後、ドメインがレジストリから削除されます

.berlin (ドイツのベルリン市)

Return to index

登録および更新のリース期間

1 ~ 10 年。

制限

公開されていますが、いくつか制約があります。

- 所有者、管理者、または技術担当者の連絡先はベルリンの住所にする必要があり、管理者の連絡先は個人である必要があります。
- 登録後 12 か月以内に .berlin ドメインをアクティブにして使用する必要があります (ウェブサイト、リダイレクト、またはメールアドレスに適用されます)。
- .berlin ドメインでウェブサイトを公開する場合、または、.berlin ドメインが別のウェブサイトにリダイレクトされる場合、そのウェブサイトのコンテンツはベルリン関連である必要があります。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

ラテン語、キリル文字に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 80 日後、ドメインがレジストリから削除されます

.ch (スイス)

Return to index

登録および更新のリース期間

1 年間。

制限

公開されており、制約はありません。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート外。RetrieveDomainAuthCode APIアクションへのアクセスを制限して、不正な転送を防ぐことをお勧めします。(この Route 53 API へのアクセスを制限すると、Route 53 コンソール、 AWS SDK、およびその他のプログラムによる手法を使用して認可コードを生成できるユーザーも制限されます) 詳細については、「Amazon Route 53 での Identity and Access Management」を参照してください。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 9 日後まで Route 53 との遅延更新ができます
- 有効期限から 9 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 9 日から 49 日までの間、レジストリでの復元ができます
- 有効期限から 49 日後、ドメインがレジストリから削除されます

.co.uk (英国)

Return to index

登録および更新のリース期間

1 ~ 10 年。

制限

公開されており、制約はありません。

プライバシー保護

すべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート

国際化ドメイン名

サポート外。

移管に必要な認可コード

.co.uk ドメインを Route 53 に移管する場合は、認可コードを取得する必要はありません。代わりに、現在のドメインレジストラが用意している方法を使って、ドメインの IPS タグの値を GANDI (すべて大文字) に更新します (IPS タグは .uk ドメイン名のレジストリである Nominet が必要としています)。レジストラが IPS タグの値を変更しない場合は、Nominet にお問い合わせください。

> **Note**
>
> .co.uk ドメインを登録すると、Route 53 は自動的にドメインの IPS タグを GANDI に設定します。

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限の 180 日前から 有効期限切れの 30 日後までの間、更新ができます
- 有効期限切れ後 30 日から 90 日までの間、Route 53 との遅延更新ができます
- 有効期限から 90 日後にドメインが Route 53 から削除されます

- レジストリでの復元はできません
- 有効期限から 92 日後、ドメインはレジストリから削除されます

ドメイン登録の削除

.co.uk ドメインのレジストリはドメイン登録を削除することができません。代わりに、自動更新を無効にして、ドメインの有効期限が切れるまで待つ必要があります。詳細については、「ドメイン名登録の削除」を参照してください。

.cz (チェコ共和国)

Return to index

登録および更新のリース期間

1 ~ 10 年。

制限

公開されており、制約はありません。

プライバシー保護

サポートされていませんが、E メールアドレスと電話番号はすべての連絡先で非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート外。

移管に必要な認可コード

はい

現在のレジストラが認可コードを提供していない場合は、`https://www.nic.cz/whois/send-password/` にアクセスし、CZ ドメインレジストリから登録者の E メールアドレスに送信されるようにリクエストします。

DNSSEC

サポート外。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 58 日後まで Route 53 との遅延更新ができます
- 有効期限から 59 日後にドメインが Route 53 から削除されます
- レジストリでの復元はできません
- 有効期限切れから 60 日後、ドメインがレジストリから削除されます

.de (ドイツ)

Return to index

登録および更新のリース期間

1 年間。

制限

公開されていますが、いくつか制約があります。

- お客様がドイツに住んでいるか、または、管理者の連絡先 (物理的な個人) がドイツに住んでいて、私書箱以外の住所になっている必要があります。
- 登録時に、ドメイン名の DNS (A、MX、CNAME) が正しく設定され、レジストリのゾーンチェックに合格する必要があります。2 つの異なる C クラスのサーバーが 3 台必要です。
- Route 53 以外の DNS サービスを使用している場合は、ドメインのネームサーバーがチェックに合格して、正しく設定されていることを確認する必要があります。ドメインのネームサーバーがチェックに合格するかどうか、https://www.denic.de/en/service/tools/nast/ をご覧ください。
- レジストリ検証要件を満たす連絡先情報を入力する必要があります。連絡先の詳細が無効であるか正しくフォーマットされていないと、ドメインの更新が失敗する可能性があります。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート外。RetrieveDomainAuthCode APIアクションへのアクセスを制限して、不正な転送を防ぐことをお勧めします。(この Route 53 API へのアクセスを制限すると、Route 53 コンソール、 AWS SDK、およびその他のプログラムによる手法を使用して認可コードを生成で

きるユーザーも制限されます) 詳細については、「Amazon Route 53 での Identity and Access Management」を参照してください。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- Route 53 との遅延更新はできません
- 有効期限日にドメインが Route 53 から削除されます
- レジストリでの復元ができます。AWS Support にお問い合わせください。
- ドメインがレジストリから削除されます。AWS Support にお問い合わせください。

.es (スペイン)

Return to index

ドメインの購入または移管

> **Important**
>
> 現在は、新しく .es ドメイン名を購入するか、.es ドメインを Route 53 に移管できます。登録者連絡先の連絡先のタイプに制限はありません。管理者/技術者/請求の連絡先タイプは個人である必要があります。

登録および更新のリース期間

1 ~ 5 年。

制限

スペインに興味があるかスペインとつながりのある人が使用できます。

2016 年以降、.ES ドメイン登録者は登録者の連絡先メールアドレスを提供する必要があります。この情報を提供していない場合は、ドメインを Route 53 に移管する前に、現在のレジストラで情報を提供する必要があります。

次の情報が必要になります。

- *AAAA0-ESNIC-F0* に類似する ESNIC 識別子。
- ESNIC 識別子がわからない場合は、現在のレジストラから取得できます。レジストラについては、https://www.dominios.es/en を参照してください。

レジストラのパスワードを覚えているかどうかに応じて、次のいずれかの手順に従って登録者のメールを更新できます。

- パスワードを覚えている場合は、ESNIC ID とパスワードを使用して https://www.nic.es/sgnd/login.action にサインインします。

  サインインした後、レジストリページの [編集] タブを選択して、登録者の E メール連絡先を編集できます。
- パスワードを忘れた場合は、https://www.nic.es/sgnd/peticion/editCorreo.action?request_locale=en にアクセスしてください。

  ESNIC 識別子、新しい有効な登録者の E メール連絡先をフォームに記入します。次に、[eID/電子証明書なしで処理] を選択してフォームを検証し、要求されたアイデンティティドキュメントをアップロードします。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

.es レジストリは time-to-live 付きの認可コードを管理し、有効期限が切れる可能性があります。認証コードを更新するには、ドメインから移管ロック (clientTransferProhibited) ステータスを削除します (存在する場合)。ドメインに移管ロックがない場合は、まず認証コードをオンにしてからオフにすることで、認証コードを更新できます。

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限の 6 日前まで更新ができます
- Route 53 との遅延更新はできません
- 有効期限の 6 日前、ドメインが Route 53: から削除されます
- 有効期限の 6 日前から有効期限切れの 4 日後までの間、レジストリでの復元ができます
- 有効期限切れの 4 日後、ドメインがレジストリから削除されます

.eu (欧州連合)

Return to index

登録および更新のリース期間

1 ~ 10 年。

制限

公開されており、1 つの制約があります。

- 欧州経済地域 (EEA) の 30 の加盟国のいずれかから、正しい郵便住所を提供する必要があります。また、欧州連合 (EU) の 27 の加盟国のいずれかの市民である場合は、EU の国籍を指定する必要があります。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート外。RetrieveDomainAuthCode APIアクションへのアクセスを制限して、不正な転送を防ぐことをお勧めします。(この Route 53 API へのアクセスを制限すると、Route 53 コンソール、 AWS SDK、およびその他のプログラムによる手法を使用して認可コードを生成できるユーザーも制限されます) 詳細については、「Amazon Route 53 での Identity and Access Management」を参照してください。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

レジストリ https://my.eurid.eu/ の「My.eu」パネルを使用して認可コードを生成することもできます。

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- Route 53 との遅延更新はできません
- 有効期限日にドメインが Route 53 から削除されます
- 有効期限の 40 日後まで、レジストリでの復元ができます
- 有効期限切れから 40 日後、ドメインがレジストリから削除されます

WHOIS 検索

既存の .eu ドメインの詳細については、「https://whois.eurid.eu/en/」をご覧ください。

.fi (フィンランド)

Return to index

登録および更新のリース期間

1 ~ 5 年。

制限

公開されていますが、いくつか制約があります。

- .fi 拡張子は、フィンランドに居住地がありフィンランド ID 番号を持つ個人と、フィンランドに登録されている法人または私企業が使用できます。
- 登録者の連絡先住所がフィンランドにある場合、登録者が個人である場合はフィンランドの ID 番号、登録者が会社である場合はフィンランドの会社番号がそれぞれ必要です。また、登録時に次の情報を提供する必要があります:
  - 連絡先が、フィンランドの個人または法人に基づいているかどうか。
  - 法人の名称に基づいている場合は、その名称が記録されている登記簿の識別名。

- 法人の名称に基づいている場合は、その名称が記録された登記簿の記録番号。
- フィンランドの法人の識別番号。
- フィンランドの個人の識別番号。
- 登録者がフィンランド以外の企業の場合は、ビジネス番号を VAT_Number として指定する必要があります。

- 登録者の住所がフィンランドにない場合、フィンランドの ID や会社番号は必要ありません。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート外。RetrieveDomainAuthCode APIアクションへのアクセスを制限して、不正な転送を防ぐことをお勧めします。(この Route 53 API へのアクセスを制限すると、Route 53 コンソール、 AWS SDK、およびその他のプログラムによる手法を使用して認可コードを生成できるユーザーも制限されます) 詳細については、「Amazon Route 53 での Identity and Access Management」を参照してください。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 29 日後まで Route 53 との遅延更新ができます
- 有効期限から 30 日後にドメインが Route 53 から削除されます
- レジストリでの復元はできません
- ドメインはレジストリから削除されません

ドメイン登録の削除

ドメインを削除する詳細については、「ドメイン名登録の削除」を参照してください。

.fr (フランス)

Return to index

登録および更新のリース期間

1 ~ 10 年。

制限

公開されていますが、いくつか制約があります。

- 個人は 18 歳以上で、その生年月日を入力する必要があります。
- 組織は欧州経済地域またはスイスに拠点を置く必要があります。
- 組織は、すべての会社識別フィールド (VAT 番号、SIREN、WALDEC、DUNS など) に入力する必要があります。これは、AFNIC が後日、確認作業を行う場合に作業が容易になるためです。
- 同じ適格条件が管理者の連絡先にも適用されます。
- 名称と期間は AFNIC の事前レビューを受け (Naming Charter Article 2.4)、以下の追加条件に従います。
  - 以前に予約または禁止されていたドメイン名は、正当な権利を持つことを証明し、誠実に行動する申請者が使用できます。
  - ville、mairie、agglo、cc、cg、cr で始まる名称は、AFNIC の命名規則に従います。

プライバシー保護

レジストリによって決定されます。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 27 日後まで Route 53 との遅延更新ができます
- 有効期限から 28 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 28 日から 58 日までの間、レジストリでの復元ができます
- 有効期限から 58 日後、ドメインがレジストリから削除されます

.gg (ガーンジー)

Return to index

登録および更新のリース期間

1 年間。

制限

公開されており、制約はありません。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 29 日後まで Route 53 との遅延更新ができます

- 有効期限から 30 日後にドメインが Route 53 から削除されます
- 有効期限切れ後の 30 日から 35 日までの間、レジストリでの復元ができます
- 有効期限から 35 日後、ドメインがレジストリから削除されます

.im (マン島)

インスタントメッセージサービスやパーソナルブランド ("I am") を開発したい個人でも、汎用 TLD としてよく使用します。

Return to index

登録および更新のリース期間

1 年または 2 年

制限

公開されており、制約はありません。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート外。

移管に必要な認可コード

はい

DNSSEC

サポート外。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 29 日後まで Route 53 との遅延更新ができます
- 有効期限から 30 日後にドメインが Route 53 から削除されます
- レジストリでの復元はできません

- 有効期限切れから 30 日後、ドメインがレジストリから削除されます

.it (イタリア)

Return to index

登録および更新のリース期間

1 年間。

制限

公開されていますが、いくつか制約があります。

- 個人または組織は、欧州連合内に登録住所を持つ必要があります。
- お客様の本国がイタリアである場合は、会計コードを入力する必要があります。本国が欧州連合内にある場合は、身分証明書番号 (ID 番号) を入力する必要があります。
- ドメインのネームサーバーは DNS チェックに合格する必要があります。変更リクエストを送信する前に、「https://dns-check.nic.it/」でネームサーバーをチェックすることをおすすめします。ドメイン名が技術的要件に従っていない (例えば、運用ネームサーバーに関連付けられていない) 場合 や、それが 30 日以内に修正されない場合、そのドメイン名はレジストリから削除されます。ドメインが削除された場合は技術要件に適合しないため、削除されたドメインに対する返金はお支払いできません。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート外。RetrieveDomainAuthCode APIアクションへのアクセスを制限して、不正な転送を防ぐことをお勧めします。(この Route 53 API へのアクセスを制限すると、Route 53 コンソール、 AWS SDK、およびその他のプログラムによる手法を使用して認可コードを生成できるユーザーも制限されます) 詳細については、「Amazon Route 53 での Identity and Access Management」を参照してください。

国際化ドメイン名

サポート対象。

移管に必要な認可コード

はい

DNSSEC

サポート外。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 13 日後まで、Route 53 との遅延更新ができます
- 有効期限から 49 日後、ドメインがレジストリから削除されます
- 有効期限切れ後 14 日から 44 日までの間、レジストリでの復元ができます
- ドメインがレジストリから削除されます。AWS Support にお問い合わせください。

.me (モンテネグロ)

Return to index

登録および更新のリース期間

1 ~ 10 年。

制限

.me ドメインのレジストリである Domain.me では、2 文字のドメイン名とそれよりも長い一部のドメイン名は、プレミアムドメイン名と見なされます。プレミアム .me ドメインを Route 53 に登録または移管することはできません。プレミアム .me ドメイン名の詳細については、domain.me ウェブサイトを参照してください。

プライバシー保護

すべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

アラビア語、ベラルーシ語、ボスニア語、ブルガリア語、簡体字中国語、繁体字中国語、クロアチア語、デンマーク語、フランス語、ドイツ語、ヒンディー語、ハンガリー語、アイスランド語、イタリア語、韓国語、ラトビア語、リトアニア語、モンゴル語、モンテネグロ語、ポーランド語、ポルトガル語、ロシア語、セルビア語、スペイン語、スウェーデン語、トルコ語、ウクライナ語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 29 日後まで Route 53 との遅延更新ができます
- 有効期限から 30 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 30 日から 60 日までの間、レジストリでの復元ができます
- 有効期限切れから 65 日後、ドメインがレジストリから削除されます

.me.uk (英国)

Return to index

登録および更新のリース期間

1 ~ 10 年。

制限

公開されており、制約はありません。

プライバシー保護

すべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート

国際化ドメイン名

サポート外。

移管に必要な認可コード

.me.uk ドメインを Route 53 に移管する場合は、認可コードを取得する必要はありません。代わりに、現在のドメインレジストラが用意している方法を使って、ドメインの IPS タグの値を GANDI (すべて大文字) に更新します (IPS タグは .uk ドメイン名のレジストリである Nominet が

必要としています)。レジストラが IPS タグの値を変更しない場合は、Nominet にお問い合わせください。

> **Note**
>
> .me.uk ドメインを登録すると、Route 53 は自動的にドメインの IPS タグを GANDI に設定します。

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限の 180 日前から 有効期限切れの 30 日後までの間、更新ができます
- 有効期限切れ後 30 日から 90 日までの間、Route 53 との遅延更新ができます
- 有効期限から 90 日後にドメインが Route 53 から削除されます
- レジストリでの復元はできません
- 有効期限から 92 日後、ドメインはレジストリから削除されます

ドメイン登録の削除

.me.uk ドメインのレジストリはドメイン登録を削除することができません。代わりに、自動更新を無効にして、ドメインの有効期限が切れるまで待つ必要があります。詳細については、「ドメイン名登録の削除」を参照してください

.nl (オランダ)

Return to index

登録および更新のリース期間

1 年間。

制限

公開されていますが、いくつか制約があります。

- 所有者または管理者の連絡先として、オランダの有効な住所を指定する必要があります。地元に存在している必要があります。

- オランダに有効な住所がない場合は、レジストリの SIDN が居住地住所手順に従って、居住地住所をお客様に提供します。
- ドメイン名は、.nl を除く 3～63 文字にする必要があります。

プライバシー保護

レジストリによって決定されます。

不正な移管を防ぐためのドメインロック

サポート外。RetrieveDomainAuthCode APIアクションへのアクセスを制限して、不正な転送を防ぐことをお勧めします。(この Route 53 API へのアクセスを制限すると、Route 53 コンソール、 AWS SDK、およびその他のプログラムによる手法を使用して認可コードを生成できるユーザーも制限されます) 詳細については、「Amazon Route 53 での Identity and Access Management」を参照してください。

国際化ドメイン名

サポート外。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限の 1 日前まで更新ができます
- Route 53 との遅延更新はできません
- 有効期限切れの 1 日前に、ドメインが Route 53: から削除されます
- 有効期限の 1 日前から有効期限切れの 39 日後までの間、レジストリでの復元ができます
- 有効期限から 39 日後、ドメインがレジストリから削除されます

.org.uk (英国)

Return to index

登録および更新のリース期間

1 ～ 10 年。

制限

公開されており、制約はありません。

プライバシー保護

すべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート

国際化ドメイン名

サポート外。

移管に必要な認可コード

.org.uk ドメインを Route 53 に移管する場合は、認可コードを取得する必要はありません。代わりに、現在のドメインレジストラが用意している方法を使って、ドメインの IPS タグの値を GANDI (すべて大文字) に更新します (IPS タグは .uk ドメイン名のレジストリである Nominet が必要としています)。レジストラが IPS タグの値を変更しない場合は、Nominet にお問い合わせください。

> **Note**
>
> .org.uk ドメインを登録すると、Route 53 は自動的にドメインの IPS タグを GANDI に設定します。

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限の 180 日前から 有効期限切れの 30 日後までの間、更新ができます
- 有効期限切れ後 30 日から 90 日までの間、Route 53 との遅延更新ができます
- 有効期限から 90 日後にドメインが Route 53 から削除されます
- レジストリでの復元はできません
- 有効期限から 92 日後、ドメインはレジストリから削除されます

ドメイン登録の削除

.org.uk ドメインのレジストリはドメイン登録を削除することができません。代わりに、自動更新を無効にして、ドメインの有効期限が切れるまで待つ必要があります。詳細については、「ドメイン名登録の削除」を参照してください。

.ruhr (ドイツ西部のルール地域)

Return to index

.ruhr 拡張子はルール地域 (ドイツ西部) 用です。

登録および更新のリース期間

1 ~ 10 年。

制限

公開されており、1 つの制約があります。

- 管理者の連絡先はドイツに住所を持つ個人である必要があります。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

サポート対象 (ä、ö、ü、ß)。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます

- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- ドメインがレジストリから削除されます。AWS Support にお問い合わせください。

.se (スウェーデン)

Return to index

登録および更新のリース期間

1 ~ 10 年。

制限

公開されていますが、いくつか制約があります。

- スウェーデンに拠点がある場合は、有効なスウェーデン ID 番号を指定する必要があります。ID 番号の形式は YYMMDD-NNNN です。
- スウェーデン外部に拠点がある場合は、徴税 ID 番号など、有効な ID 番号を入力する必要があります。

追加の検証要求

2025 年 10 月 1 日現在、.se ドメイン登録では、レジストリの新しい NIS 2.0 要件に準拠するために追加の ID 検証が必要です。.se ドメインを登録すると、検証ドキュメントをリクエストするためにご連絡します。必要なドキュメントを提供し、検証が完了するまで、ドメイン登録は保留中のままになります。ドキュメントを送信するには、 AWS サポートにお問い合わせください。

.se レジストリは、既存のドメインを定期的に監査し、最近登録されたドメインに対して、またはドメインに特定の変更 (ドメイン所有者や連絡先情報の更新など) を行ったときに、追加の検証をリクエストする場合があります。ドメインが serverHold ステータスの場合、これは、ドメインを完全にアクティブ化する前にレジストリの検証が必要であることを意味します。

提供する必要があるドキュメント:

- 個人の場合: 3 か月未満の政府発行の ID ドキュメント (ID カードやパスポートなど) および住所を証明できるもの。
- 会社または組織の場合: 会社または組織の登録証明書、および登録証明書と異なる場合は住所を証明できるもの。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート外。RetrieveDomainAuthCode APIアクションへのアクセスを制限して、不正な転送を防ぐことをお勧めします。(この Route 53 API へのアクセスを制限すると、Route 53 コンソール、 AWS SDK、およびその他のプログラムによる手法を使用して認可コードを生成できるユーザーも制限されます) 詳細については、「Amazon Route 53 での Identity and Access Management」を参照してください。

国際化ドメイン名

ラテン語、スウェーデン語、およびイディッシュ語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限の 1 日前まで更新ができます
- Route 53 との遅延更新はできません
- 有効期限切れの 1 日前に、ドメインが Route 53 から削除されます
- 有効期限の 1 日前から有効期限切れの 59 日後までの間、レジストリでの復元ができます
- 有効期限から 64 日後、ドメインがレジストリから削除されます

.uk (英国)

Return to index

登録および更新のリース期間

1 ~ 10 年。

制限

公開されており、制約はありません。

プライバシー保護

すべての情報が非表示になります。

不正な移管を防ぐためのドメインロック

サポート

国際化ドメイン名

サポート外。

移管に必要な認可コード

uk ドメインを Route 53 に移管する場合は、認可コードを取得する必要はありません。代わりに、現在のドメインレジストラが用意している方法を使って、ドメインの IPS タグの値を GANDI (すべて大文字) に更新します (IPS タグは .uk ドメイン名のレジストリである Nominet が必要としています)。レジストラが IPS タグの値を変更しない場合は、Nominet にお問い合わせください。

> **Note**
>
> .uk ドメインを登録すると、Route 53 は自動的にドメインの IPS タグを GANDI に設定します。

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限の 180 日前から 有効期限切れの 30 日後までの間、更新ができます
- 有効期限切れ後 30 日から 90 日までの間、Route 53 との遅延更新ができます
- 有効期限から 90 日後にドメインが Route 53 から削除されます
- レジストリでの復元はできません
- 有効期限から 92 日後、ドメインはレジストリから削除されます

ドメイン登録の削除

.uk ドメインのレジストリはドメイン登録を削除することができません。代わりに、自動更新を無効にして、ドメインの有効期限が切れるまで待つ必要があります。詳細については、「ドメイン名登録の削除」を参照してください。

.wien (オーストリアのウィーン市)

Return to index

登録および更新のリース期間

1 ~ 10 年。

制限

公開されていますが、いくつか制約があります。

- オーストリアのウィーン市と経済的、文化的、旅行者的、歴史的、社会的などの密接な関係があることを示す必要があります。
- .wien ドメイン名は、登録期間全体を通して、上記の条件に関連した用途で使用する必要があります。

プライバシー保護

サポート外。

不正な移管を防ぐためのドメインロック

サポート対象。

国際化ドメイン名

ラテン語に対してサポートされます。

移管に必要な認可コード

はい

DNSSEC

ドメイン登録でサポートされています。詳細については、「ドメインの DNSSEC の設定」を参照してください。

ドメインの更新と復元の期限

- 有効期限切れまで更新ができます
- 有効期限切れの 44 日後まで Route 53 との遅延更新ができます
- 有効期限から 45 日後にドメインが Route 53 から削除されます
- 有効期限切れ後 45 日から 75 日までの間、レジストリでの復元ができます
- 有効期限切れから 80 日後、ドメインがレジストリから削除されます

DNS サービスとしての Amazon Route 53 の設定

Amazon Route 53 は、example.com などのドメインに対して DNS サービスとして使用できます。Route 53 は、www.example.com などのドメイン名を 192.0.2.1 などの IP アドレスに変換することで、インターネットトラフィックをウェブサイトにルーティングします。コンピュータは、これらの IP アドレスを使用して相互に接続します。誰かがブラウザにドメイン名を入力するか、E メールを送信すると、DNS クエリは Route 53 に送信されます。ウェブサーバーの IP アドレスなど、適切な値で応答します。

> ⚠ DNS ホスティングとドメイン登録
>
> この章では、DNS ホスティングにのみ Route 53 を使用する方法について説明します。ドメインは現在のレジストラに登録されたままです。更新に対する支払いを継続します。Route 53 は、DNS 設定と DNS クエリのみを処理します。
> ドメインを Route 53 にも移管する場合は (Route 53 をレジストラと DNS サービスの両方にする)、ドメイン移管の移管前チェックリスト「」および「」を参照してくださいドメイン登録の Amazon Route 53 への移管。

この章では、インターネットトラフィックを適切な場所にルーティングするように Route 53 を設定する方法について説明します。また、別のプロバイダーから Route 53 に DNS サービスを移動する方法と、Route 53 を新しいドメインの DNS サービスとして使用する方法についても説明します。

トピック

- Amazon Route 53 を既存ドメインの DNS サービスとして使用する
- 新しいドメインの DNS ルーティングの設定
- リソースへのトラフィックのルーティング
- ホストゾーンの使用
- レコードを使用する
- Amazon Route 53 での DNSSEC 署名の設定
- AWS Cloud Map を使用してレコードとヘルスチェックを作成する
- DNS の制約と動作
- 関連トピック

Amazon Route 53 を既存ドメインの DNS サービスとして使用する

Route 53 に 1 つ以上のドメイン登録を移管していて、現在のレジストラが有料 DNS サービスを提供していない場合は、ドメインを移管する前に DNS サービスを移行する必要があります。そうしないと、ドメインを移管するときにレジストラは DNS サービスの提供を停止します。関連するウェブサイトとウェブアプリケーションは、インターネット上で使用できなくなります。(DNS サービスを別の DNS サービスプロバイダーに移行することもできます。 Route 53 に登録されているドメインの DNS サービスプロバイダーとして Route 53 を使用する必要はありません。)

プロセスは、現在ドメインを使用しているかどうかによって異なります。

- ドメインが現在トラフィックを受信している場合 (ユーザーがドメイン名を使用してウェブサイトを閲覧したり、ウェブアプリケーションにアクセスしている場合など) は、「Route 53 を使用中のドメインの DNS サービスにする」を参照してください。
- ドメインにトラフィックがない場合 (またはトラフィックをほとんど受け取っていない場合) は、「Route 53 を非アクティブドメインの DNS サービスにする」を参照してください。

どちらのオプションでも、移行プロセス全体でドメインを利用可能にしておく必要があります。ただし、万一問題が発生した場合は、最初のオプションですぐにロールバックできます。2 番目のオプションの場合、ドメインを数日間利用できなくなる可能性があります。

の専門家に接続する場合は AWS、「 販売サポート」を参照してください。

Route 53 を使用中のドメインの DNS サービスにする

既にトラフィックを受信しているドメインの DNS サービスを Amazon Route 53 に移行できます。たとえば、ユーザーが既にウェブサイトを参照したり、ドメイン上のウェブアプリケーションにアクセスしたりする場合があります。サービスを中断することなく移行するには、このトピックの手順に従います。

トピック

- ステップ 1: 現在の DNS サービスプロバイダから現在の DNS 設定を取得する (オプション、ただし推奨)
- ステップ 2: ホストゾーンを作成する
- ステップ 3: レコードを作成する
- ステップ 4: TTL の設定を下げる

- ステップ 5: (DNSSEC を構成している場合) 親ゾーンから DS レコードを削除する
- ステップ 6: 古い TTL の有効期限切れを待つ
- ステップ 7: NS レコードを更新して、Route 53 ネームサーバーを使用する
- ステップ 8: ドメインのトラフィックの監視
- ステップ 9: NS レコードの TTL を高い値に戻す
- ステップ 10: ドメイン登録を Amazon Route 53 に移管する
- ステップ 11: DNSSEC 署名を再度有効にする (必要な場合)

ステップ 1: 現在の DNS サービスプロバイダから現在の DNS 設定を取得する (オプション、ただし推奨)

DNS サービスを他のプロバイダから Route 53 に移行した後に、現在の DNS 設定を Route 53 で再現できます。まず、ドメインと同じ名前のホストゾーンを Route 53 に作成し、そのホストゾーンにレコードを作成します。各レコードは、ドメイン名またはサブドメイン名のトラフィックをルーティングする方法を示します。たとえば、誰かがウェブブラウザにドメイン名を入力すると、トラフィックをデータセンターのウェブサーバー、Amazon EC2 インスタンス、CloudFront ディストリビューション、またはその他の場所に移動しますか?

このプロセスは、現在の DNS 設定の複雑さによって異なります。

- 現在の DNS 設定が単純な場合 – 少数のサブドメインへのインターネットトラフィックを、ウェブサーバーや Amazon S3 バケットなどの少数のリソースにルーティングする場合は、Route 53 コンソールから手動でレコードをいくつか作成します。
- 現在の DNS 設定がより複雑で、現在の設定を再現するだけの場合 – 現在の DNS サービスプロバイダーからゾーンファイルを取得して Route 53 にインポートできれば、移行を簡素化できます。(すべての DNS サービスプロバイダがゾーンファイルを提供しているわけではありません。) ゾーンファイルをインポートすると、Route 53 はホストゾーンに対応するレコードを作成して既存の設定を再現します。

  ゾーンファイルまたはレコードリストを取得する方法を、現在の DNS サービスプロバイダのカスタマーサポートに問い合わせてみてください。必要なゾーンファイルのフォーマットの詳細については、「ゾーンファイルをインポートしてレコードを作成する」を参照してください。
- 現在の DNS 設定がより複雑で、Route 53 ルーティング機能に関心がある場合 – 次のドキュメントを参照して、他の DNS サービスプロバイダーでは利用できない Route 53 機能を使用するかどうかを確認してください。その場合は、レコードを手動で作成することも、ゾーンファイルをインポートして後でレコードを作成または更新することもできます。

- エイリアスレコードと非エイリアスレコードの選択 では、CloudFront ディストリビューションや Amazon S3 バケットなどの一部の AWS リソースに無料でトラフィックをルーティングする Route 53 エイリアスレコードの利点について説明します。 Amazon S3
- ルーティングポリシーの選択 では、Route 53 ルーティングオプションについて説明します。たとえば、ユーザーの場所、ユーザーとリソース間のレイテンシー、リソースの状態、指定した重みに基づくルーティングなどです。

> **Note**
>
> また、ゾーンファイルをインポートした後で設定を変更して、エイリアスレコードと複雑なルーティングポリシーを利用することもできます。

ゾーンファイルを取得できない場合や、Route 53 のレコードを手動で作成する場合に、移行の必要性が考えられるレコードは次のとおりです。

- A (アドレス) レコード – このレコードは、ドメイン名またはサブドメイン名を、対応するリソースの IPv4 アドレス (192.0.2.3 など) に関連付けます
- AAAA (アドレス) レコード – このレコードは、ドメイン名またはサブドメイン名を、対応するリソースの IPv6 アドレス (2001:0db8:85a3:0000:0000:abcd:0001:2345 など) に関連付けます
- メールサーバー (MX) レコード – このレコードは、トラフィックをメールサーバーにルーティングします
- CNAME レコード – このレコードは、あるドメイン名 (example.net) のトラフィックを別のドメイン名 (example.com) に再ルーティングします
- サポートされているその他の DNS レコードタイプに対応するレコード – サポートされているレコードタイプの一覧については、「サポートされる DNS レコードタイプ」を参照してください。

ステップ 2: ホストゾーンを作成する

ドメインのトラフィックをどのようにルーティングするかを Amazon Route 53 に指示するには、ドメインと同じ名前のホストゾーンを作成し、そのホストゾーンにレコードを作成します。

> **Important**
>
> ホストゾーンは、管理権限を持つドメインに対してのみ作成できます。通常、これはドメインを所有していることを指しますが、ドメインの登録者向けにアプリケーションを開発している場合にも当てはまります。

ホストゾーンを作成すると、Route 53 はそのゾーンに対して、1 つのネームサーバー (NS) レコードと、1 つの Start of Authority (SOA) レコードを自動的に作成します。NS レコードは、Route 53 がホストゾーンに関連付けた 4 つのネームサーバーを識別します。Route 53 をドメインの DNS サービスにするには、これら 4 つのネームサーバーを使用するようにドメインの登録を更新します。

> **Important**
>
> ホストゾーンに追加のネームサーバー (NS) レコードまたは Start of Authority (SOA) レコードを作成しないでください。また、既存の NS レコードと SOA レコードを削除しないでください。

ホストゾーンを作成するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. Route 53 を初めて使用する場合は、[DNS management (DNS 管理)] の [Get started (今すぐ始め)] を選択した後、[Create Hosted Zone (ホストゾーンの作成)] を選択します。

   既に Route 53 を利用している場合は、ナビゲーションペインで [Hosted zones (ホストゾーン)] を選択した上で、[Create Hosted Zone (ホストゾーンの作成)] を選択します。
3. [Create hosted zone] (ホストゾーンの作成) ペインで、ドメイン名とコメント (必要に応じて) を入力します。設定の詳細については、右側のヘルプパネルを開き参照してください。

   a ~ z、0 ~ 9、- (ハイフン) 以外の文字を指定する方法、および国際化されたドメイン名を指定する方法については、「DNS ドメイン名の形式」を参照してください。
4. [Type] (タイプ) では、デフォルト値の [Public hosted zone] (パブリックホストゾーン) をそのまま使用します。
5. [ホストゾーンの作成] を選択します。

ステップ 3: レコードを作成する

ホストゾーンを作成した後、ドメイン (example.com) またはサブドメイン (www.example.com) のトラフィックをルーティングする場所を定義するレコードをホストゾーンに作成します。例えば、example.com と www.example.com のトラフィックを、Amazon EC2 インスタンス上にあるウェブサーバーにルーティングする場合は、example.com という名前のレコードと www.example.com という名前のレコードを 2 つ作成します。各レコードでは、EC2 インスタンスの IP アドレスを指定します。

レコードはさまざまな方法で作成できます。

ゾーンファイルをインポートする

「ステップ 1: 現在の DNS サービスプロバイダから現在の DNS 設定を取得する (オプション、ただし推奨)」で現在の DNS サービスからゾーンファイルを取得している場合には、これが最も簡単な方法となります。Amazon Route 53 では、エイリアスレコードを作成するタイミングや、加重やフェイルオーバーなどの特殊なルーティングタイプを使用するタイミングを予測できません。この理由から、インポートするゾーンファイルがある場合、Route 53 では、シンプルなルーティングポリシーを使用しながら標準的な DNS レコードが作成されます。

詳細については、「ゾーンファイルをインポートしてレコードを作成する」を参照してください。

コンソールで個別にレコードを作成する

ゾーンファイルを取得しておらず、シンプルなルーティングポリシーを持つレコードをいくつか作成して使用を開始する場合には、Route 53 コンソールでレコードを作成します。エイリアスレコードと非エイリアスレコードの両方を作成できます。

詳細については、以下のトピックを参照してください。

- ルーティングポリシーの選択
- エイリアスレコードと非エイリアスレコードの選択
- Amazon Route 53 コンソールを使用したレコードの作成

プログラムでレコードを作成する

レコードは、 AWS SDKs、、 AWS CLIまたは のいずれかを使用して作成できます AWS Tools for Windows PowerShell。詳細については、AWS ドキュメント を参照してください。

SDK を提供し AWS ないプログラミング言語を使用している場合は、Route 53 API を使用することもできます。詳細については、「Amazon Route 53 API リファレンス」を参照してください。

ステップ 4: TTL の設定を下げる

レコードの TTL (有効期限) 設定は、DNS リゾルバーがレコードをキャッシュし、キャッシュされた情報を使用する期間を指定します。TTL の有効期限が切れると、リゾルバーは最新の情報について別のクエリを DNS サービスプロバイダーに送信します。

NS レコードの一般的な TTL 設定は 172800 秒、つまり 2 日です。NS レコードには、DNS がドメインのトラフィックのルーティングに関する情報を取得するために使用できるネームサーバーが一覧表示されます。現在の DNS サービスプロバイダーと Amazon Route 53 の両方で NS レコードの TTL を下げると、DNS を Route 53 に移行する際に問題が発生した場合のドメインのダウンタイムが短縮されます。TTL を下げないと、何か問題が発生した場合、ドメインはインターネット上で最大 2 日間使用できなくなる可能性があります。

> **Note**
>
> 一部の完全なリゾルバーは、親権威サーバーの NS レコードの TTL をキャッシュする可能性があるため、親権威 DNS サーバーに登録された NS レコードの TTL も減らす必要があります。

次の NS レコードの TTL を変更することをお勧めします。

- 現在の DNS サービスプロバイダのホストゾーンにある NS レコード。(現在のプロバイダでは異なる用語を使用している場合もあります。)
- 「ステップ 2: ホストゾーンを作成する」で作成したホストゾーンの NS レコード。

現在の DNS サービスプロバイダで NS レコードの TTL 設定を下げるには

- ドメインの現在の DNS サービスプロバイダが提供するメソッドを使用して、ドメインのホストゾーンでの NS レコードの TTL を変更します。

Route 53 ホストゾーンの NS レコードの TTL 設定を下げるには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [Hosted Zones] を選択します。
3. ホストゾーンの名前を選択します。

4. NS レコードを選択してから、[Edit] (編集) を選択します。
5. [TTL (Seconds)] の値を変更します。60 秒から 900 秒 (15 分) の間の値を指定することをお勧めします。
6. [Save changes] (変更の保存) をクリックします。

ステップ 5: (DNSSEC を構成している場合) 親ゾーンから DS レコードを削除する

ドメインで DNSSEC を設定している場合は、ドメインを Route 53 に移行する前に、親ゾーンから Delegation Signer (DS) レコードを削除します。

Route 53 または別のレジストラが親ゾーンをホストしている場合は、それらのホストに対し DS レコードの削除を依頼します。

2 つのプロバイダー間で DNSSEC 署名を同時に有効にすることはできません。DNSSEC をオフにするには、DS または DNSKEYs を削除する必要があります。これにより、DNSSEC 検証をスキップするように DNS リゾルバーに一時的に通知されます。ステップ 11 では、Route 53 への移行が完了した後に DNSSEC 検証を再度有効にできます。

詳細については、「ドメインのパブリックキーの削除」を参照してください。

ステップ 6: 古い TTL の有効期限切れを待つ

ユーザーがウェブサイトを参照している場合やウェブアプリケーションにアクセスする場合など、ドメインが使用中の場合、DNS リゾルバーは現在の DNS サービスプロバイダーが提供するネームサーバーの名前をキャッシュします。数分前にその情報をキャッシュした DNS リゾルバーでは、この後ほぼ 2 日ほど保存されます。

Route 53 への DNS サービスの移行がすべて同時に行われるようにするには、TTL を下げてから 2 日間待ちます。2 日間の TTL の有効期限が切れ、リゾルバーがドメインのネームサーバーをリクエストすると、リゾルバーは で指定した現在のネームサーバーと新しい TTL を取得しますステップ 4: TTL の設定を下げる。

ステップ 7: NS レコードを更新して、Route 53 ネームサーバーを使用する

ドメインの DNS サービスとして Amazon Route 53 の使用を開始するには、レジストラまたは親ゾーンが提供する方法を使用して、NS レコード内の現在のネームサーバーを Route 53 ネームサーバーに置き換えます。

> **Note**
>
> Route 53 ネームサーバーを使用するように、現在の DNS サービスプロバイダーで NS レコードを更新するときは、ドメインの DNS 設定を更新します。(これは、ドメインの Route 53 ホストゾーンの NS レコードを更新するのに似ていますが、移行元の DNS サービスで設定を更新する点が異なります)。

レジストラまたは親ゾーンで NS レコードを更新して Route 53 ネームサーバーを使用するには

1. Route 53 コンソールで、 ホストゾーンのネームサーバーを取得します。

   a. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。

   b. ナビゲーションペインで [Hosted zones] を選択します。

   c. [Hosted Zones] (ホストゾーン) ページで、該当するホストゾーンの名前を選択します。

   d. [Hosted zone details] (ホストゾーンの詳細) セクションの [Name servers] (ネームサーバー) で一覧表示されている、 4 つの名前を書き留めます。

2. ドメインの現在の DNS サービスが提供するメソッドを使用して、ホストゾーンの NS レコードを更新します。ドメインが Route 53 に登録されている場合は、「ドメインのネームサーバーおよびグルーレコードの追加あるいは変更」を参照してください。このプロセスは、現在の DNS サービスでネームサーバーの削除が可能かどうかによって異なります。

   ネームサーバーを削除できる場合

   - ホストゾーンの NS レコードで、現在のネームサーバーの名前をメモします。現在の DNS 設定を復元する必要がある場合は、これらが指定するサーバーになります。
   - NS レコードから現在のネームサーバーを削除します。
   - NS レコードを、この手順のステップ 1 で取得した 4 つすべての Route 53 ネームサーバーの名前に置き換えます。

   > **Note**
   >
   > 完了すると、NS レコード内のネームサーバーは 4 つの Route 53 ネームサーバーのみになります。

ネームサーバーを削除できない場合

- カスタムネームサーバーを使用するオプションを選択します。
- この手順のステップ 1 で取得した、4 つの Route 53 ネームサーバーをすべて追加します。

ステップ 8: ドメインのトラフィックの監視

ウェブサイトやアプリケーションのトラフィック、電子メールなど、ドメインのトラフィックを監視する。

- トラフィックが減速または停止した場合 – 以前の DNS サービスが提供するメソッドを使用して、ドメインのネームサーバーを以前のネームサーバーに戻します。これらは「レジストラまたは親ゾーンで NS レコードを更新して Route 53 ネームサーバーを使用するには」のステップ 7 でメモしたネームサーバーです。その後、何が悪かったのかを見極めます。
- トラフィックに影響がない場合 –「ステップ 9: NS レコードの TTL を高い値に戻す」に進みます。

ステップ 9: NS レコードの TTL を高い値に戻す

ドメインの Amazon Route 53 ホストゾーンで、NS レコードの TTL をより一般的な値、例えば 172800 秒 (2 日) に変更します。これにより、DNS リゾルバーがドメインのネームサーバーのクエリを送信するのを頻繁に待つ必要がないため、ユーザーのレイテンシーが向上します。

Route 53 ホストゾーン内で NS レコードの TTL を変更するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [Hosted Zones] を選択します。
3. ホストゾーンの名前を選択します。
4. ホストゾーンのレコードのリストで、NS レコードを選択します。
5. [編集] を選択します。
6. [TTL (Seconds)] を、DNS リゾルバーがドメインのネームサーバーの名前をキャッシュする秒数に変更します。172800 秒の値を推奨します。
7. [Save changes] (変更の保存) をクリックします。

ステップ 10: ドメイン登録を Amazon Route 53 に移管する

ドメインの DNS サービスの Amazon Route 53 への移行が完了したので、必要な場合には、ドメインの登録を Route 53 に移管します。詳細については、「ドメイン登録の Amazon Route 53 への移管」を参照してください。

ステップ 11: DNSSEC 署名を再度有効にする (必要な場合)

これでドメインの DNS サービスを Amazon Route 53 に移管したので、DNSSEC 署名を再度有効にすることができます。

DNSSEC 署名を有効にするには、次の 2 つの手順を実行します。

- ステップ 1: Route 53 の DNSSEC 署名を有効にし、 AWS Key Management Service () のカスタマーマネージドキーに基づいてキー署名キー (KSK) を作成するよう Route 53 にリクエストします AWS KMS。
- ステップ 2: 親ゾーンに委任署名者 (DS) レコードを追加して、ホストゾーンの信頼チェーンを作成します。これにより、DNS レスポンスを信頼できる暗号化署名で検証できます。

  手順については、「DNSSEC 署名を有効にし、信頼チェーンを確立します。」を参照してください。

Route 53 を非アクティブドメインの DNS サービスにする

トラフィックがない (またはトラフィックをほとんど受信していない) ドメイン用に、DNS サービスを Amazon Route 53 に移行する場合は、このセクションの手順を実行します。

トピック

- ステップ 1: 現在の DNS サービスプロバイダから現在の DNS 設定を取得する (非アクティブドメイン)
- ステップ 2: ホストゾーンを作成する (非アクティブドメイン)
- ステップ 3: レコードの作成 (非アクティブドメイン)
- ステップ 4: Amazon Route 53 ネームサーバーを使用するようにドメイン登録を更新する (非アクティブドメイン)

ステップ 1: 現在の DNS サービスプロバイダから現在の DNS 設定を取得する (非アクティブドメイン)

DNS サービスを他のプロバイダから Route 53 に移行する場合は、現在の DNS 設定を Route 53 に再現します。まず、ドメインと同じ名前のホストゾーンを Route 53 に作成し、そのホストゾーンにレコードを作成します。各レコードは、ドメイン名またはサブドメイン名のトラフィックをルーティングする方法を示します。たとえば、誰かがウェブブラウザにドメイン名を入力すると、トラフィックをデータセンターのウェブサーバー、Amazon EC2 インスタンス、CloudFront ディストリビューション、またはその他の場所に移動しますか?

このプロセスは、現在の DNS 設定の複雑さによって異なります。

- 現在の DNS 設定が単純な場合 – 少数のサブドメインへのインターネットトラフィックを、ウェブサーバーや Amazon S3 バケットなどの少数のリソースにルーティングする場合は、Route 53 コンソールから手動でレコードをいくつか作成します。
- 現在の DNS 設定がより複雑で、現在の設定を再現するだけの場合 – 現在の DNS サービスプロバイダーからゾーンファイルを取得して Route 53 にインポートできれば、移行を簡素化できます。(すべての DNS サービスプロバイダがゾーンファイルを提供しているわけではありません。) ゾーンファイルをインポートすると、Route 53 はホストゾーンに対応するレコードを作成して既存の設定を再現します。

  ゾーンファイルまたはレコードリストを取得する方法を、現在の DNS サービスプロバイダのカスタマーサポートに問い合わせてみてください。必要なゾーンファイルのフォーマットの詳細については、「ゾーンファイルをインポートしてレコードを作成する」を参照してください。
- 現在の DNS 設定がより複雑で、Route 53 ルーティング機能に関心がある場合 – 次のドキュメントを参照して、他の DNS サービスプロバイダーでは利用できない Route 53 機能を使用するかどうかを確認してください。その場合は、レコードを手動で作成することも、ゾーンファイルをインポートして後でレコードを作成または更新することもできます。
  - エイリアスレコードと非エイリアスレコードの選択 では、CloudFront ディストリビューションや Amazon S3 バケットなどの一部の AWS リソースに無料でトラフィックをルーティングする Route 53 エイリアスレコードの利点について説明します。 Amazon S3
  - ルーティングポリシーの選択 では、Route 53 ルーティングオプションについて説明します。たとえば、ユーザーの場所、ユーザーとリソース間のレイテンシー、リソースの状態、指定した重みに基づくルーティングなどです。

> **Note**
>
> また、ゾーンファイルをインポートした後で設定を変更して、エイリアスレコードと複雑なルーティングポリシーを利用することもできます。

ゾーンファイルを取得できない場合や、Route 53 のレコードを手動で作成する場合に、移行の必要性が考えられるレコードは次のとおりです。

- A (アドレス) レコード – このレコードは、ドメイン名またはサブドメイン名を、対応するリソースの IPv4 アドレス (192.0.2.3 など) に関連付けます
- AAAA (アドレス) レコード – このレコードは、ドメイン名またはサブドメイン名を、対応するリソースの IPv6 アドレス (2001:0db8:85a3:0000:0000:abcd:0001:2345 など) に関連付けます
- メールサーバー (MX) レコード – このレコードは、トラフィックをメールサーバーにルーティングします
- CNAME レコード – このレコードは、あるドメイン名 (example.net) のトラフィックを別のドメイン名 (example.com) に再ルーティングします
- サポートされているその他の DNS レコードタイプに対応するレコード – サポートされているレコードタイプの一覧については、「サポートされる DNS レコードタイプ」を参照してください。

ステップ 2: ホストゾーンを作成する (非アクティブドメイン)

ドメインのトラフィックをどのようにルーティングするかを Amazon Route 53 に指示するには、ドメインと同じ名前のホストゾーンを作成し、そのホストゾーンにレコードを作成します。

> **Important**
>
> ホストゾーンは、管理権限を持つドメインに対してのみ作成できます。通常、これはドメインを所有していることを指しますが、ドメインの登録者向けにアプリケーションを開発している場合にも当てはまります。

ホストゾーンを作成すると、Route 53 はそのゾーンに対して、1 つのネームサーバー (NS) レコードと、1 つの Start of Authority (SOA) レコードを自動的に作成します。NS レコードは、Route 53 がホストゾーンに関連付けた 4 つのネームサーバーを識別します。Route 53 をドメインの DNS サービスにするには、これら 4 つのネームサーバーを使用するようにドメインの登録を更新します。

> **Important**
>
> ホストゾーンに追加のネームサーバー (NS) レコードまたは Start of Authority (SOA) レコードを作成しないでください。また、既存の NS レコードと SOA レコードを削除しないでください。

ホストゾーンを作成するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. Route 53 を初めて使用する場合、[今すぐ始める] を選択します。

   既に Route 53 を利用している場合は、ナビゲーションペインの [Hosted zones (ホストゾーン)] を選択します。
3. [ホストゾーンの作成] を選択します。
4. [Create hosted zone] (ホストゾーンの作成) ペインで、ドメイン名とコメント (必要に応じて) を入力します。設定の詳細については、ラベルの上にマウスポインタを置いて、ツールヒントを表示してください。

   a ~ z、0 ~ 9、- (ハイフン) 以外の文字を指定する方法、および国際化されたドメイン名を指定する方法については、「DNS ドメイン名の形式」を参照してください。
5. [Record type] (レコードタイプ) では、デフォルト値の [Public hosted zone] (パブリックホストゾーン) をそのまま使用します。
6. [ホストゾーンの作成] を選択します。

ステップ 3: レコードの作成 (非アクティブドメイン)

ホストゾーンを作成した後、ドメイン (example.com) またはサブドメイン (www.example.com) のトラフィックをルーティングする場所を定義するレコードをホストゾーンに作成します。例えば、example.com と www.example.com のトラフィックを、Amazon EC2 インスタンス上にあるウェブサーバーにルーティングする場合は、example.com という名前のレコードと www.example.com という名前のレコードを 2 つ作成します。各レコードでは、EC2 インスタンスの IP アドレスを指定します。

レコードはさまざまな方法で作成できます。

ゾーンファイルをインポートする

「ステップ 1: 現在の DNS サービスプロバイダから現在の DNS 設定を取得する (非アクティブドメイン)」で現在の DNS サービスからゾーンファイルを取得している場合には、これが最も簡単な方法となります。Amazon Route 53 では、エイリアスレコードを作成するタイミングや、加重やフェイルオーバーなどの特殊なルーティングタイプを使用するタイミングを予測できません。この理由から、インポートするゾーンファイルがある場合、Route 53 では、シンプルなルーティングポリシーを使用しながら標準的な DNS レコードが作成されます。

詳細については、「ゾーンファイルをインポートしてレコードを作成する」を参照してください。

コンソールで個別にレコードを作成する

ゾーンファイルを取得しておらず、シンプルなルーティングポリシーを持つレコードをいくつか作成して使用を開始する場合には、Route 53 コンソールでレコードを作成します。エイリアスレコードと非エイリアスレコードの両方を作成できます。

詳細については、以下のトピックを参照してください。

- ルーティングポリシーの選択
- エイリアスレコードと非エイリアスレコードの選択
- Amazon Route 53 コンソールを使用したレコードの作成

プログラムでレコードを作成する

レコードは、 AWS SDKs、、 AWS CLIまたは のいずれかを使用して作成できます AWS Tools for Windows PowerShell。詳細については、AWS ドキュメント を参照してください。

SDK を提供し AWS ないプログラミング言語を使用している場合は、Route 53 API を使用することもできます。詳細については、「Amazon Route 53 API リファレンス」を参照してください。

ステップ 4: Amazon Route 53 ネームサーバーを使用するようにドメイン登録を更新する (非アクティブドメイン)

ドメイン用にレコードを作成し終えたら、ドメインの DNS サービスを Amazon Route 53 に変更します。ドメインレジストラで設定を更新するには、以下の手順を実行します。

ドメインのネームサーバーを更新するには

1. Route 53 コンソールで、Route 53 ホストゾーンのネームサーバーを取得します。

a. Route 53 コンソール (https://console.aws.amazon.com/route53/) を開きます。
b. ナビゲーションペインで [Hosted zones] を選択します。
c. [Hosted Zones (ホストゾーン)] ページで、ホストゾーンのラジオボタン (名前ではない) を選択し、[View details (詳細を表示)] を選択します。
d. ホストゾーンの詳細ページで、[Hosted zone details (ホストゾーンの詳細)] を選択します。
e. [Name Servers] (ネームサーバー) で一覧表示されている 4 つのサーバー名を書き留めます。

2. ドメインのレジストラが提供する方法を使用して、この手順のステップ 2 で取得した 4 つの Route 53 ネームサーバーを使用するようにドメインのネームサーバーを変更します。

   Route 53 に登録されているドメインに関しては、「ドメインのネームサーバーおよびグルーレコードの追加あるいは変更」を参照してください。

新しいドメインの DNS ルーティングの設定

インターネットトラフィックをウェブサイトまたはウェブアプリケーションにルーティングするには、ドメインの DNS ルーティングを設定します。手順は、ドメインを Route 53 から購入したか、別のレジストラから購入したかによって異なります。

Route 53 から購入したドメインの DNS を設定する

Route 53 にドメインを登録すると、Route 53 自体がドメインの DNS サービスになります。ドメインと同じ名前のホストゾーンを作成し、ゾーンに 4 つのネームサーバーを割り当て、それらのネームサーバーを使用するようにドメインを更新します。

別のレジストラから購入したドメインの DNS を設定する

たとえば、最上位ドメイン (TLD) が Route 53 によって提供されていないため、別のレジストラからドメインを購入する場合、次の 2 つのオプションがあります。

- DNS ホスティングにのみ Route 53 を使用する: 現在のレジストラを保持しますが、Route 53 に DNS の処理を許可します。以下の手順に従ってホストゾーンを作成し、レジストラのネームサーバーを更新します。
- ドメインを Route 53 に転送する: Route 53 をレジストラおよび DNS サービスにします。最初に行う操作については[ドメイン移管の移管前チェックリスト]「」を、転送手順[ドメイン登録の Amazon Route 53 への移管]については「」を参照してください。

Route 53 でサポートされている TLD の詳細については、「Amazon Route 53 に登録できる最上位ドメイン」を参照してください。

ホストゾーンを作成し、DNS を委任する

パブリックホストゾーンを作成し、ネームサーバーをレジストラに追加するには、次の手順に従います。

Route 53 ではないドメイン向けにホストゾーンを作成するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで、[ホストゾーン] を選択し、[ホストゾーンの作成] を選択します。
3. 名前には、 など、ホストゾーンを作成するドメインの名前を入力しexample.com、必要に応じて説明を追加し、パブリックホストゾーンを選択し、ホストゾーンの作成を選択します。
4. ホストゾーンを作成したら、4 つのネームサーバー (NS) レコードを書き留めます。各 は「ns-」で始まります。

   ドメインレジストラで、これらのネームサーバーを入力して、ドメインを Route 53 ホストゾーンにポイントします。

DNS トラフィックをルーティングする

ドメインのインターネットトラフィックをルーティングする方法を Route 53 に指示するには、ホストゾーンにレコードを作成します。たとえば、example.com のリクエストを Amazon EC2 インスタンスのウェブサーバーにルーティングする場合は、example.com ホストゾーンにレコードを作成し、そのインスタンスの Elastic IP アドレスを指定します。詳細については、以下の各トピックを参照してください。

- ホストゾーンでレコードを作成する方法については、「レコードを使用する」を参照してください。
- 選択した AWS リソースにトラフィックをルーティングする方法については、「」を参照してくださいAWS リソースへのインターネットトラフィックのルーティング。
- DNS の仕組みについては、「ウェブサイトやウェブアプリケーションへのインターネットトラフィックのルーティング」を参照してください。
- DNS 安静を確認するには、「Route 53 からの DNS 応答の確認」を参照してください。

リソースへのトラフィックのルーティング

ユーザーがウェブブラウザにドメインの名前を入力するなどしてウェブサイトやウェブアプリケーションをリクエストすると、Amazon Route 53 はAmazon S3バケットやデータセンターのウェブサーバーなどのリソースにユーザーをルーティングするのに役立ちます。リソースにトラフィックをルーティングするように Route 53 を設定するには、次の手順を実行します。

1. ホストゾーンの作成。パブリックホストゾーンまたはプライベートホストゾーンのいずれかを作成できます。

   パブリックホストゾーン

   インターネットトラフィックをリソースにルーティングする場合は、パブリックホストゾーンを作成します。例えば、顧客が EC2 インスタンスでホスティングしている会社のウェブサイトを表示できます。詳細については、「「パブリックホストゾーンの操作」」を参照してください。

   プライベートホストゾーン

   Amazon VPC 内でトラフィックをルーティングする場合は、プライベートホストゾーンを作成します。詳細については、「プライベートホストゾーンの使用」を参照してください。
2. ホストゾーンにレコードを作成します。レコードは、各ドメイン名またはサブドメイン名のトラフィックをどこへルーティングするかを定義します。例えば、www.example.com のトラフィックをデータセンターのウェブサーバーにルーティングするには、通常 example.com ホストゾーンに www.example.com レコードを作成します。

   詳細については、以下のトピックを参照してください。

   - レコードを使用する
   - サブドメインのトラフィックのルーティング
   - AWS リソースへのインターネットトラフィックのルーティング

サブドメインのトラフィックのルーティング

acme.example.com や zenith.example.com などのサブドメインのリソースにトラフィックをルーティングする場合、次の 2 つの方法があります。

ドメインのホストゾーンにレコードを作成します。

通常、サブドメインのトラフィックをルーティングするには、ドメインと同じ名前のホストゾーンにレコードを作成します。例えば、acme.example.com のインターネットトラフィックをデータセンターのウェブサーバーにルーティングするには、example.com ホストゾーンに acme.example.com という名前のレコードを作成します。詳細については、トピック「レコードを使用する」とそのサブトピックを参照してください。

サブドメインのホストゾーンを作成し、新しいホストゾーンでレコードを作成する

サブドメインのホストゾーンを作成することもできます。別のホストゾーンを使用してサブドメインのインターネットトラフィックをルーティングすることは、「サブドメインの責任をホストゾーンに委任する」または「サブドメインを他のネームサーバーに委任する」とも呼ばれます。使用方法に関する概要は次のとおりです。

1. トラフィックをルーティングするサブドメインと同じ名前のホストゾーン (acme.example.com など) を作成します。
2. 新しいホストゾーンに、サブドメイン (acme.example.com) とそのサブドメイン (backend.acme.example.com など) のトラフィックをどのようにルーティングするかを定義するレコードを作成します。
3. 新しいホストゾーンの作成時に、Route 53 がそのゾーンに割り当てるネームサーバーを取得します。
4. ドメインのホストゾーン (example.com) に新しい NS レコードを作成します。NS レコード名はサブドメイン名 (acme.example.com) でなければならず、ステップ 3 で取得した 4 つのネームサーバーをレコード値として指定します。

別のホストゾーンを使用してサブドメインのトラフィックをルーティングする場合、IAM のアクセス許可を使用してサブドメインのホストゾーンへのアクセスを制限できます 複数のサブドメインが異なるグループによって管理されている場合、サブドメインごとにホストゾーンを作成すると、ドメインのホストゾーン内のレコードにアクセスする必要があるユーザーの数を減らすことができます。

この委任プロセスを実装するには、次の IAM アクセス許可が必要です。Route 53 IAM ポリシーの詳細については、「」を参照してくださいAmazon Route 53 での Identity and Access Management。

親アカウント (example.com を所有)

ユーザーまたはロールには、親ドメインのホストゾーンのレコードを変更するアクセス許可が必要です。

子アカウント (acme.example.com を作成)

ユーザーまたはロールには、サブドメインホストゾーンを作成および管理するためのアクセス許可が必要です。

サブドメインに別個のホストゾーンを使用することで、ドメインとサブドメインに異なる DNS サービスを使用することもできます。詳細については、「親ドメインを移行しないで Amazon Route 53 をサブドメインの DNS サービスとして使用する」を参照してください。

この設定の各 DNS リゾルバーからの最初の DNS クエリに対するパフォーマンスの影響はわずかです。リゾルバーは、ルートドメインのホストゾーンから情報を取得し、サブドメインのホストゾーンから情報を取得する必要があります。サブドメインの最初の DNS クエリの後、リゾルバーは情報をキャッシュするため、TTL が期限切れになり、別のクライアントがそのリゾルバーからサブドメインをリクエストするまで、再度取得する必要はありません。詳細については、「TTL (秒)」セクションの「Amazon Route 53 レコードの作成時または編集時に指定する値」を参照してください。

トピック

- サブドメインのトラフィックをルーティングする別のホストゾーンの作成
- サブドメインの追加レベルのトラフィックのルーティング

サブドメインのトラフィックをルーティングする別のホストゾーンの作成

サブドメインのトラフィックをルーティングする方法の 1 つは、サブドメインのホストゾーンを作成し、新しいホストゾーンに、サブドメインのレコードを作成することです。(より一般的なオプションは、ドメインのホストゾーン内にサブドメインのレコードを作成することです)。

> **Note**
>
> この手順では、サブドメインを Route 53 に委任する方法を示します。代わりにそれらのサービスのネームサーバーを指す NS レコードを作成することで、サブドメインを他の DNS サービスに委任することもできます。

プロセスの概要を次に示します。

1. サブドメインのホストゾーンを作成します。詳細については、「サブドメインの新しいホストゾーンを作成する」を参照してください。

2. ホストゾーンに、サブドメインのレコードを追加します。サブドメインのホストゾーンに属するレコードがドメインのホストゾーンに含まれている場合は、これらのレコードをサブドメインのホストゾーンに複製します。詳細については、「サブドメインのホストゾーンでのレコードの作成」を参照してください。
3. ドメインのホストゾーンにサブドメインの NS レコードを作成します。これにより、サブドメインの責任を新しいホストゾーンのネームサーバーに委任します。サブドメインのホストゾーンに属するレコードがドメインのホストゾーンに含まれている場合は、これらのレコードをドメインのホストゾーンから削除します (ステップ 2 でサブドメインのホストゾーンに複製を作成しました)。詳細については、「ドメインのホストゾーンの更新」を参照してください。

サブドメインの新しいホストゾーンを作成する

Route 53 コンソールを使用してサブドメインのホストゾーンを作成するには、次の手順を実行します。

サブドメインのホストゾーンを作成するには (コンソール)

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. Route 53 を初めて使用する場合、[今すぐ始める] を選択します。

   既に Route 53 を利用している場合は、ナビゲーションペインの [Hosted zones (ホストゾーン)] を選択します。
3. [ホストゾーンの作成] を選択します。
4. 右側のペインでは、[acme.example.com] のようなサブドメイン名を入力します。オプションでコメントも入力できます。

   a ~ z、0 ~ 9、- (ハイフン) 以外の文字を指定する方法、および国際化されたドメイン名を指定する方法については、「DNS ドメイン名の形式」を参照してください。
5. [Type] (タイプ) では、デフォルト値の [Public hosted zone] (パブリックホストゾーン) をそのまま使用します。
6. 右ペインの下部にある [Create Hosted Zone] (ホストゾーンの作成) を選択します。

サブドメインのホストゾーンでのレコードの作成

Route 53 でサブドメイン (acme.example.com) とそのサブドメイン (backend.acme.example.com) のトラフィックをルーティングする方法を定義するには、サブドメインのホストゾーンにレコードを作成します。

サブドメインのホストゾーンにレコードを作成する場合は、以下の点に注意してください。

- サブドメインのホストゾーンに追加のネームサーバー (NS) レコードまたは Start of Authority (SOA) レコードを作成しないでください。また、既存の NS レコードと SOA レコードを削除しないでください。
- サブドメインのすべてのレコードは、当該サブドメインのホストゾーンに作成します。例えば、example.com ドメインと acme.example.com サブドメインの両方にホストゾーンがある場合、acme.example.com サブドメインのすべてのレコードは acme.example.com のホストゾーンに作成します。これには、backend.acme.example.com や beta.backend.acme.example.com などのレコードが含まれます。
- サブドメイン (acme.example.com) のホストゾーンに属するレコードがドメイン (example.com) のホストゾーンに既に含まれている場合は、これらのレコードをサブドメインのホストゾーンに複製します。このプロセスの最後のステップとして、後でドメインのホストゾーンから重複するレコードを削除します。

> **Important**
>
> サブドメインの一部のレコードが、ドメインのホストゾーンとサブドメインのホストゾーンの両方にあると、DNS の動作が一貫しなくなります。動作は、DNS リゾルバーがキャッシュしたネームサーバーによって異なります。ドメインホストゾーンのネームサーバー (example.com) またはサブドメインホストゾーンのネームサーバー (acme.example.com)。場合によっては、レコードは存在するが、DNS リゾルバーがクエリするホストゾーンには存在しないときに、Route 53 は NXDOMAIN (存在しないドメイン) を返します。

詳細については、「レコードを使用する」を参照してください。

ドメインのホストゾーンの更新

ホストゾーンを作成する際、Route 53 は、そのゾーンに対し 4 つのネームサーバーを自動的に割り当てます。ホストゾーンの NS レコードは、ドメインまたはサブドメインの DNS クエリに応答する

ネームサーバーを特定します。サブドメインのホストゾーンのレコードを使用してインターネットトラフィックをルーティングするには、ドメインのホストゾーン (example.com) に新しい NS レコードを作成します。サブドメイン (acme.example.com) の名前を付けます。NS レコードの値には、サブドメインのホストゾーンからネームサーバーの名前を指定します。

Route 53 が、DNS リゾルバーからサブドメイン acme.example.com (またはそのサブドメインの 1 つ) に対する DNS クエリを受け取ると、以下のことが発生します。

1. Route 53 は、ドメインのホストゾーン内で (example.com) を調べ、サブドメイン (acme.example.com) のための NS レコードを検出します。
2. Route 53 は、ドメイン (example.com) のホストゾーン内で、acme.example.com の NS レコードからネームサーバーを取得し、それを DNS リゾルバーに返します。
3. リゾルバーは、acme.example.com のクエリを acme.example.com ホストゾーンのネームサーバーに再送信します。
4. Route 53 は、acme.example.com ホストゾーンのレコードを使用してクエリに応答します。

サブドメインのホストゾーンを使用してサブドメインのトラフィックをルーティングし、ドメインのホストゾーンから重複レコードを削除するように Route 53 を設定するには、次の手順を実行します。

サブドメインのホストゾーンを使用するように Route 53 を設定するには (コンソール)

1. Route 53 コンソールで、サブドメインのホストゾーンのネームサーバーを取得します。
   a. ナビゲーションペインで [Hosted zones] を選択します。
   b. [Hosted Zones] (ホストゾーン) ページで、サブドメインのホストゾーンの名前を選択します。
   c. 右ペインにある [Hosted zones details] (ホストゾーンの詳細) セクションの [Name Servers] (ネームサーバー) に、一覧表示されている 4 つのサーバーの名前をコピーします。
2. サブドメインではなくドメイン (example.com) のホストゾーンの名前を選択します。
3. [Create record (レコードを作成)] を選択します。
4. [Simple routing (シンプルルーティング)]、[Next (次へ)] の順に選択します。
5. [Define simple record (シンプルなレコードを定義)] を選択します。
6. 次の値を指定します。

名前

サブドメインの名前を入力します (例: acme.example.com)。これは、作成したサブドメインホストゾーンの名前と完全に一致する必要があります。

値/トラフィックのルーティング先

[IP address or another value depending on the record type] (IP アドレスまたはレコードタイプに応じた別の値) を選択し、ステップ 1 でコピーしたネームサーバーの名前を貼り付けます。

レコードタイプ

[NS – Name servers for a hosted zone] (NS — ホストゾーンのネームサーバー) を選択します。

TTL (秒)

NS レコードの、より一般的な値 (172800 秒など) に変更します。

7. [Define simple record] (シンプルなレコードを定義)、[Create records] (レコードを作成) の順に選択します。
8. サブドメインのホストゾーンに再作成したレコードがドメインのホストゾーンに含まれている場合は、これらのレコードをドメインのホストゾーンから削除します。詳細については、「レコードの削除」を参照してください。

   完了すると、サブドメインのすべてのレコードがサブドメインのホストゾーンに含まれます。

サブドメインの追加レベルのトラフィックのルーティング

acme.example.com などのサブドメインのサブドメインにトラフィックをルーティングするのと同じ方法で、トラフィックを backend.acme.example.com などのサブドメインにルーティングします。ドメインのホストゾーンにレコードを作成するか、下位サブドメインのホストゾーンを作成し、その新しいホストゾーンにレコードを作成します。

下位レベルのサブドメイン用に別のホストゾーンを作成する場合は、ドメイン名に近いレベルのサブドメインのホストゾーンに下位レベルのサブドメインの NS レコードを作成します。これにより、トラフィックがリソースに正しくルーティングされます。例えば、次のサブドメインのトラフィックをルーティングするとします。

- subdomain1.example.com

- subdomain2.subdomain1.example.com

別のホストゾーンを使用して subdomain2.subdomain1.example.com のトラフィックをルーティングするには、次の操作を行います。

1. subdomain2.subdomain1.example.com という名前のホストゾーンを作成します。
2. subdomain2.subdomain1.example.com ホストゾーンにレコードを作成します。詳細については、「サブドメインのホストゾーンでのレコードの作成」を参照してください。
3. subdomain2.subdomain1.example.com ホストゾーンのネームサーバーの名前をコピーします。
4. subdomain1.example.com ホストゾーンで、subdomain2.subdomain1.example.com という NS レコードを作成し、subdomain2.subdomain1.example.com ホストゾーンのネームサーバーの名前に貼り付けます。

   さらに、subdomain1.example.com から重複するレコードを削除します。詳細については、「ドメインのホストゾーンの更新」を参照してください。

   この NS レコードの作成を完了すると、subdomain2.subdomain1.example.com のホストゾーンを使用した、subdomain2.subdomain1.example.com サブドメインへのトラフィックのルーティングが、Route 53 により開始されます。

ホストゾーンの使用

ホストゾーンは、レコードのコンテナです。レコードは、example.com などのドメインとそのサブドメイン (acme.example.com、zenith.example.com) のトラフィックをルーティングする方法に関する情報を保持します。ホストゾーンの名前はドメインと同じです。ユーザー定義変数には次の 2 種類があります。

- パブリックホストゾーンには、トラフィックをインターネットでどのようにルーティングするかを指定するレコードが含まれています。詳細については、「「パブリックホストゾーンの操作」」を参照してください。
- プライベートホストゾーンには、トラフィックを Amazon VPC でどのようにルーティングするかを指定するレコードが含まれています。詳細については、「プライベートホストゾーンの使用」を参照してください。

「パブリックホストゾーンの操作」

パブリックホストゾーンは、 やそのサブドメイン (example.com、acme.example.comzenith.example.com) など、ドメインのインターネット上のトラフィックをルーティングする方法に関する情報を保持するコンテナです。パブリックホストゾーンは、次の 2 つの方法で入手できます。

- Route 53 にドメインを登録すると、Route 53 は自動的にホストゾーンを作成します。
- 既存のドメインの DNS サービスを Route 53 に転送する場合は、まずドメインのホストゾーンを作成します。詳細については、「Amazon Route 53 を既存ドメインの DNS サービスとして使用する」を参照してください。

どちらの場合も、ホストゾーンにレコードを作成して、ドメインとサブドメインのトラフィックをルーティングします。例えば、www.example.com へのトラフィックを、CloudFront ディストリビューションや、データセンターのウェブサーバーにルーティングするためのレコードを作成することができます。レコードの詳細については、「レコードを使用する」を参照してください。

このトピックでは、Amazon Route 53 コンソールを使用してパブリックホストゾーンを作成、一覧表示、削除する方法を説明します。

> **Note**
>
> Amazon VPC サービスを使用して作成した 1 つ以上の VPC 内で、Route 53 プライベートホストゾーンを使用してトラフィックをルーティングすることもできます。詳細については、「プライベートホストゾーンの使用」を参照してください。

トピック

- パブリックホストゾーンを使用する場合の考慮事項
- パブリックホストゾーンの作成
- パブリックホストゾーンに対するネームサーバーの取得
- パブリックホストゾーンの一覧表示
- パブリックホストゾーンの DNS クエリメトリクスの表示
- パブリックホストゾーンの削除
- Route 53 からの DNS 応答の確認

- ホワイトラベルネームサーバーの設定
- Amazon Route 53 がパブリックホストゾーンに作成する NS レコードと SOA レコード
- パブリック DNS レコードを管理するための高速リカバリの有効化

パブリックホストゾーンを使用する場合の考慮事項

パブリックホストゾーンを使用する場合は、以下の点を考慮してください。

NS レコードと SOA レコード

ホストゾーンを作成すると、Amazon Route 53 はゾーンのネームサーバー (NS) レコードと認可開始 (SOA) レコードを作成します。NS レコードには、レジストラまたは DNS サービスに渡す 4 つのネームサーバーが一覧表示され、DNS クエリが Route 53 ネームサーバーに到達します。NS および SOA レコードの詳細については、「Amazon Route 53 がパブリックホストゾーンに作成する NS レコードと SOA レコード」を参照してください。

同じ名前を持つ複数のホストゾーン

同じ名前で複数のホストゾーンを作成し、それぞれに異なるレコードを追加できます。Route 53 はすべてのホストゾーンに 4 つのネームサーバーを割り当て、ネームサーバーはホストゾーンごとに異なります。レジストラのネームサーバーレコードを更新するときは、ドメインのクエリに応答するときに Route 53 が使用するレコードを含む、正しいホストゾーンに Route 53 ネームサーバーを使用するように注意してください。Route 53 が、同じ名前の他のホストゾーンのレコードに値を返すことは決してありません。

再利用可能な委託セット

デフォルトでは、Route 53 は作成する各ホストゾーンに 4 つのネームサーバー (委任セットと呼ばれます) の一意のセットを割り当てます。多くのホストゾーンを作成する場合は、 API を使用して再利用可能な委任セットを作成できます。(再利用可能な委託セットは Route 53 コンソールからは操作できません)。その後、 API を使用してホストゾーンを作成し、それぞれに同じ 4 つのネームサーバーを割り当てることができます。

再利用可能な委任セットにより、DNS サービスを Route 53 に移行することが容易になります。Route 53 が提供するすべてのドメインに同じ 4 つのネームサーバーを使用するようにレジストラに指示できます。詳細については、Amazon Route 53 API リファレンスの「CreateReusableDelegationSet」を参照してください。

パブリックホストゾーンの作成

パブリックホストゾーンは、 やそのサブドメイン (example.com、acme.example.comzenith.example.com) など、ドメインのインターネット上のトラフィックをルーティングする方法に関する情報を保持するコンテナです。ホストゾーンを作成したら、ドメインとサブドメインのトラフィックをルーティングするレコードを作成します。

> ⚠ 制限事項
>
> Route 53 でホストゾーンを作成するための以下の制限に注意してください。
>
> - ホストゾーンは、管理権限を持つドメインに対してのみ作成できます。通常、これはドメインを所有していることを指しますが、ドメインの登録者向けにアプリケーションを開発している場合にも当てはまります。
> - ホストゾーンは、ドメインとサブドメインに対してのみ作成できます。Route 53 は、.com などの最上位ドメイン (TLD) のホスティングをサポートしていません。

Route 53 コンソールを使用してパブリックホストゾーンを作成するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. Route 53 を初めて使用する場合は、[DNS management (DNS の管理)] で [Get started (今すぐ始める)] を選択します。

   既に Route 53 を利用している場合は、ナビゲーションペインの [Hosted zones (ホストゾーン)] を選択します。
3. [ホストゾーンの作成] を選択します。
4. [Create Hosted Zone (ホストゾーンの作成)] ペインに、そのトラフィックをルーティングするドメインの名前を入力します。オプションでコメントも入力できます。

   a ~ z、0 ~ 9、- (ハイフン) 以外の文字を指定する方法、および国際化されたドメイン名を指定する方法については、「DNS ドメイン名の形式」を参照してください。
5. [Type] は、デフォルト値である [Public Hosted Zone] のままにします。
6. [作成] を選択します。
7. ドメインとサブドメインのトラフィックをどのようにルーティングするかを指定するレコードを作成します。詳細については、「レコードを使用する」を参照してください。

8. 新しいホストゾーンのレコードを使用してドメインのトラフィックをルーティングする場合は、該当するトピックを参照してください。

   - Route 53 を、別のドメインレジストラに登録されているドメインの DNS サービスとして使用する場合は、「Amazon Route 53 を既存ドメインの DNS サービスとして使用する」を参照してください。
   - Route 53 に登録されているドメインに関しては、「ドメインのネームサーバーおよびグルーレコードの追加あるいは変更」を参照してください。

パブリックホストゾーンに対するネームサーバーの取得

ドメイン登録の DNS サービスを変更する場合は、パブリックホストゾーンのネームサーバーを取得します。DNS サービスを変更する方法については、「Amazon Route 53 を既存ドメインの DNS サービスとして使用する」を参照してください。

> **Note**
>
> 一部のレジストラでは、IP アドレスを使用してネームサーバーのみを指定できます。完全修飾ドメイン名は使用できません。レジストラに IP アドレスが必要な場合は、dig ユーティリティ (Mac、Unix、Linux の場合) または nslookup ユーティリティ (Windows の場合) を使用して、ネームサーバーの IP アドレスを取得できます。Route 53 でネームサーバーの IP アドレスが変更されることはほとんどありません。Route 53 で変更する必要がある場合は、事前に通知されます。

Route 53 コンソールを使用してホストゾーンのネームサーバーを取得するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [Hosted zones (ホストゾーン)] をクリックします。
3. [Hosted Zones (ホストゾーン)] ページで、ホストゾーンのラジオボタン (名前ではない) を選択し、[View details (詳細を表示)] を選択します。
4. ホストゾーンの詳細ページで、[Hosted zone details (ホストゾーンの詳細)] を選択します。
5. [Name Servers] (ネームサーバー) で一覧表示されている 4 つのサーバー名を書き留めます。

パブリックホストゾーンの一覧表示

Amazon Route 53 コンソールを使用して、現在の AWS アカウントで作成したすべてのホストゾーンを一覧表示できます。Route 53 API を使用してホストゾーンを一覧表示する方法については、Amazon Route 53 API リファレンスの「ListHostedZones」を参照してください。

Route 53 コンソールを使用して AWS アカウントに関連付けられたパブリックホストゾーンを一覧表示するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [Hosted zones] を選択します。このページには、現在サインインしている AWS アカウントに関連付けられているホストゾーンのリストが表示されます。
3. ホストゾーンをフィルタリングするには、表の上部にある検索バーを使用します。

   検索動作は、ホストゾーンに最大で 2,000 のレコードが含まれているか、または 2,000 を超えるレコードが含まれているかによって異なります。

   最大 2,000 のホストゾーン

   - 特定の値を持つレコードを表示するには、検索バーを選択し、ドロップダウンリストでプロパティを選択し、値を入力します。検索バーに値を直接入力し、Enter を押すこともできます。例えば、名前が **abc** で始まるホストゾーンを表示する場合は、この値を検索バーに入力した後で Enter キーを押します。
   - ホストゾーンタイプが共通なホストゾーンのみを表示するには、ドロップダウンリストから対象のタイプを選択し、タイプを入力します。

   2,000 を超えるホストゾーン

   - プロパティは、完全なドメイン名、すべてのプロパティ、およびタイプに基づいて検索できます。
   - 完全なドメイン名を使用して検索すると、検索結果が速く得られます。

パブリックホストゾーンの DNS クエリメトリクスの表示

Route 53 がパブリックホストゾーンまたは一連のパブリックホストゾーンに対して応答する DNS クエリの合計数を表示できます。メトリクスは CloudWatch に表示されるため、グラフを表示したり、期間を選択したり、他の方法でメトリクスをカスタマイズしたりできます。DNS クエリの数が選択

したレベルを上回ったり下回ったりしたときに、アラームを作成して通知を設定することもできます。

> **Note**
>
> Route 53 では、すべてのパブリックホストゾーンでの DNS クエリの数を CloudWatch に自動的に送信するため、何も設定しなくてもクエリメトリクスを表示できます。DNS クエリメトリクスには料金はかかりません。

どの DNS クエリがカウントされますか?

メトリクスには、DNS リゾルバーが Route 53 に転送するクエリのみが含まれます。DNS リゾルバーがクエリへのレスポンス (example.com のロードバランサーの IP アドレスなど) を既にキャッシュしている場合、そのレコードの TTL の有効期限が切れるまでキャッシュされたレスポンスを返し続けます。

ユーザーが使用するリゾルバーであるドメイン名 (example.com) またはサブドメイン名 (www.example.com) に対して送信される DNS クエリの数と、レコードの TTL によっては、DNS リゾルバーに送信される数千のクエリごとに 1 つのクエリのみが表示される場合があります。DNS の仕組みについては、「Amazon Route 53 によりドメインのトラフィックをルーティングする方法」を参照してください。

ホストゾーンのクエリメトリクスは、いつ CloudWatch に表示され始めますか ?

ホストゾーンを作成した後、そのホストゾーンが CloudWatch に表示されるまでに最大数時間の遅延が発生します。また、表示するデータが存在するように、ホストゾーンのレコードの DNS クエリを送信する必要があります。

メトリクスは米国東部 (バージニア北部) でのみ利用できます

コンソールでメトリクスを取得するには、リージョンに米国東部 (バージニア北部) を指定する必要があります。 AWS CLI を使用してメトリクスを取得するには、 AWS リージョンを指定しないままにするか、リージョン`us-east-1`として を指定する必要があります。他のリージョンを選択した場合、Route 53 メトリクスは使用できません。

DNS クエリの CloudWatch メトリクスとディメンション

DNS クエリの CloudWatch メトリクスとディメンションの詳細については、「Amazon CloudWatch を使用したホストゾーンのモニタリング」を参照してください。CloudWatch メトリクスの詳細については、Amazon CloudWatch ユーザーガイドの「Amazon CloudWatch メトリクスを使用する」を参照してください。

DNS クエリに関する詳細データの取得

Route 53 が応答する各 DNS クエリの詳細情報 (以下の値を含む) を取得するには、クエリログ記録を設定します。

- リクエストされたドメインまたはサブドメイン
- リクエストの日付と時刻
- DNS レコードタイプ (A や AAAA など)
- DNS クエリに応答した Route 53 エッジロケーション
- DNS レスポンスコード (`NoError` や `ServFail` など)

詳細については、「パブリック DNS クエリのログ記録」を参照してください。

DNS クエリメトリクスの取得方法

ホストゾーンを作成するとすぐに、Amazon Route 53 は、メトリクスとディメンションを CloudWatch に対し 1 分間隔で送信し始めます。次の手順を使用して、CloudWatch コンソールでメトリクスを表示するか、 AWS Command Line Interface () を使用してメトリクスを表示できますAWS CLI。

トピック

- CloudWatch コンソールでのパブリックホストゾーンの DNS クエリメトリクスの表示
- を使用した DNS クエリメトリクスの取得 AWS CLI

CloudWatch コンソールでのパブリックホストゾーンの DNS クエリメトリクスの表示

CloudWatch コンソールでパブリックホストゾーンの DNS クエリメトリクスを表示するには、以下の手順を実行します。

CloudWatch コンソールでパブリックホストゾーンの DNS クエリメトリクスを表示するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/cloudwatch/ で CloudWatch コンソールを開きます。
2. ナビゲーションペインで [Metrics (メトリクス)] を選択してください。
3. コンソールの右上隅にある AWS リージョンリストで、米国東部 (バージニア北部) を選択します。他の AWS リージョンを選択した場合、Route 53 メトリクスは使用できません。
4. [All metrics] タブで、[Route 53] を選択します。

5. [Hosted Zone Metrics (ホストゾーンのメトリクス)] を選択します。
6. メトリクス名 DNSQueries を持つ 1 つ以上のホストゾーンのチェックボックスをオンにします。
7. [グラフ化したメトリクス] タブで、該当する値を変更して、目的の形式でメトリクスを表示します。

   [統計] で、[Sum] または [SampleCount] を選択します。これらの統計はどちらも同じ値を表示します。

を使用した DNS クエリメトリクスの取得 AWS CLI

を使用して DNS クエリメトリクスを取得するには AWS CLI、get-metric-data コマンドを使用します。次の点に注意してください。

- コマンドのほとんどの値は、別の JSON ファイルで指定します。詳細については、「get-metric-data」を参照してください。
- コマンドは、JSON ファイル `Period` で指定した間隔ごとに 1 つの値を返します。`Period` は秒単位であるため、5 分の期間を指定し `60` に `Period` を指定すると、5 つの値が取得されます。5 分の期間を指定し、`300` に `Period` を指定した場合、1 つの値が取得されます。
- JSON ファイルでは、`Id` に任意の値を指定できます。
- AWS リージョンを指定しないままにするか、リージョン`us-east-1`として を指定します。他のリージョンを選択した場合、Route 53 メトリクスは使用できません。詳細については、AWS「 ユーザーガイド」の「 CLI の設定」を参照してください。 AWS Command Line Interface

以下は、2019 年 5 月 1 日の 4:01 から 4:07 までの 5 分間の DNS クエリメトリクスを取得するために使用する AWS CLI コマンドです。`metric-data-queries` パラメータは、コマンドに続くサンプル JSON ファイルを参照します。

```
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
```

サンプル JSON ファイルを次に示します。

```
[
    {
        "Id": "my_dns_queries_id",
        "MetricStat": {
```

```
            "Metric": {
                "Namespace": "AWS/Route53",
                "MetricName": "DNSQueries",
                "Dimensions": [
                    {
                        "Name": "HostedZoneId",
                        "Value": "Z1D633PJN98FT9"
                    }
                ]
            },
            "Period": 60,
            "Stat": "Sum"
        },
        "ReturnData": true
    }
]
```

このコマンドの出力は次のとおりです。次の点に注意してください。

- コマンドの開始時刻と終了時刻は、7 分間の期間 (2019-05-01T04:01:00Z から 2019-05-01T04:07:00Z) を対象としています。
- 戻り値は 6 つだけです。2019-05-01T04:05:00Z に値がないのは、その 1 分間に DNS クエリがなかったためです。
- JSON ファイルで指定された Period の値は 60 (秒) であるため、値は 1 分間隔で報告されます。

```
{
    "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"
            ]
        }
    ]
}
```

パブリックホストゾーンの削除

このセクションでは、Amazon Route 53 コンソールを使用してパブリックホストゾーンを削除する方法を説明します。

ホストゾーンは、デフォルトの SOA レコードと NS レコード以外のレコードがない場合にのみ削除できます。ホストゾーンに他のレコードがある場合は、最初に削除します。これにより、まだ使用中のレコードがあるホストゾーンを削除できなくなります。

トピック

- トラフィックがドメインにルーティングされないようにする
- 別のサービスによって作成されたパブリックホストゾーンを削除する
- Route 53 コンソールを使用してのパブリックホストゾーンの削除

トラフィックがドメインにルーティングされないようにする

ドメイン登録を維持するが、ウェブサイトまたはウェブアプリケーションへのインターネットトラフィックのルーティングを停止する場合は、ホストゾーンを削除するのではなく、ホストゾーンのレコードを削除することをお勧めします。

> **Important**
>
> ホストゾーンを削除した場合、元に戻すことはできません。新しいホストゾーンを作成し、ドメインのネームサーバーを更新する必要があります。有効にするには最大 48 時間かかる場合があります。また、ホストゾーンを削除すると、誰かがドメインをハイジャックし、ドメイン名を使用してトラフィックを自分のリソースにルーティングする可能性があります。サブドメインに独自のホストゾーンを付与し、その子ホストゾーンを削除する場合は、子ホストゾーンと同じ名前の NS レコードを削除して、親ホストゾーンも更新する必要があります。例えば、ホストゾーン acme.example.com を削除する場合は、example.com ホストゾー

ンの NS レコード acme.example.com も削除する必要があります。最初に NS レコードを削除し、その NS レコードの TTL が期限切れになるまで待ってから、子ホストゾーンを削除することをお勧めします。これにより、DNS リゾルバーに子ホストゾーンのネームサーバーがキャッシュされている間は、誰も子ホストゾーンをハイジャックできません。

ホストゾーンの月額料金を回避する場合は、ドメインの DNS サービスを無料の DNS サービスに移動できます。DNS サービスを移動するときは、ドメインのネームサーバーを更新する必要があります。ドメインが Route 53 に登録されている場合に、新しい DNS サービスのネームサーバーを使用して Route 53 ネームサーバーを置き換える方法については、「ドメインのネームサーバーおよびグルーレコードの追加あるいは変更」を参照してください。ドメインが別のレジストラに登録されている場合は、そのレジストラが提供する方法を使用してドメインのネームサーバーを更新します。詳細については、インターネットで「無料の DNS サービス」を検索してください。

別のサービスによって作成されたパブリックホストゾーンを削除する

別のサービスがホストゾーンを作成した場合、Route 53 コンソールを使用してホストゾーンを削除することはできません。代わりに、そのサービスに適したプロセスを使用してください。

- AWS Cloud Map – パブリック DNS 名前空間の作成時に AWS Cloud Map が作成したホストゾーンを削除するには、namespace を削除します。 はホストゾーンを自動的に AWS Cloud Map 削除します。詳細については、AWS Cloud Map デベロッパーガイドの名前空間の削除を参照してください。
- Amazon Elastic Container Service (Amazon ECS) Service Discovery – Service Discovery を使用してサービスを作成した際に Amazon ECS が作成したパブリックホストゾーンを削除するには、名前空間を使用している Amazon ECS サービスを削除した上で、その名前空間を削除します。詳細については、Amazon Elastic Container Service デベロッパーガイドの「サービスの削除」を参照してください。

Route 53 コンソールを使用してのパブリックホストゾーンの削除

Route 53 コンソールを使用してパブリックホストゾーンを削除するには、以下の手順を実行します。

Route 53 コンソールを使用してパブリックホストゾーンを削除するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。

2. ナビゲーションペインで [Hosted zones] (ホストゾーン) を選択した後に、削除するホストゾーンの強調表示されたリンクを選択します。
3. 削除するホストゾーンに NS と SOA のレコードのみが含まれていることを確認します。他のレコードが含まれている場合は、それらを削除します。また、DNSSEC 署名を無効にする必要があります。

   > **Note**
   >
   > これらの要件を満たさずにホストゾーンを削除しようとすると、Route 53 はエラーを返します。
   >
   > - DNSSEC 署名が有効になっている場合: 指定されたホストゾーンに DNSSEC キー署名キーが含まれているため、削除できません
   > - 他のリソースレコードセットが存在する場合 (デフォルトの SOA および NS レコードを除く): 指定されたホストゾーンには必須ではないリソースレコードセットが含まれているため、削除できません

   - ホストゾーンの詳細ページにある [Records] (レコード) リストで、[Type] (タイプ) 列の値が「NS」または「SOA」以外に設定されたレコードがある場合には、その行を選択し、次に [Delete] (削除) を選択します。

     複数の連続するレコードを選択するには、最初の行を選択し、[Shift] (シフト) キーを押したまま最後の行を選択します。複数の連続していないレコードを選択するには、最初の行を選択し、Ctrl キーを押したまま、残りの行を選択します。

     > **Note**
     >
     > ホストゾーンでサブドメインの NS レコードを作成した場合は、それらのレコードも削除します。

4. [Hosted Zones] (ホストゾーン) ページで、削除するホストゾーンの行を選択します。
5. [削除] を選択します。
6. 確認キーを入力し、[Delete (削除)] を選択します。
7. ドメインをインターネット上で利用できなくするには、DNS サービスを無料の DNS サービスに移管し、Route 53 のホストゾーンを削除することをお勧めします。これにより、今後の DNS クエリが誤ってルーティングされることを防ぐことができます。

ドメインが Route 53 に登録されている場合に、新しい DNS サービスのネームサーバーを使用して Route 53 ネームサーバーを置き換える方法については、「ドメインのネームサーバーおよびグルーレコードの追加あるいは変更」を参照してください。ドメインが他のレジストラに登録されている場合、レジストラが提供する方法を使用してドメインのネームサーバーを変更します。

> **Note**
>
> サブドメイン (acme.example.com) のホストゾーンを削除する場合は、ドメイン (example.com) のネームサーバーを変更する必要はありません。

Route 53 からの DNS 応答の確認

ドメインに Amazon Route 53 ホストゾーンを作成した場合は、コンソールの DNS チェックツールを使用して、DNS サービスとして Route 53 を使用するようにドメインを設定するときに、Route 53 が DNS クエリにどのように応答するかを確認できます。位置情報、地理的近接性、レイテンシーレコードの場合、特定の DNS リゾルバーまたはクライアント IP アドレスからのクエリをテストして、Route 53 が返すレスポンスを確認することもできます。

> **Important**
>
> このツールはドメインネームシステムにクエリを送信しません。ホストゾーンのレコードの設定にのみ基づいて応答します。このツールは、ホストゾーンがドメインのトラフィックをルーティングするために現在使用されているかどうかにかかわらず、同じ情報を返します。

DNS チェックツールは、パブリックホストゾーンにのみ使用できます。

> **Note**
>
> DNS チェックツールが、`dig` コマンドの応答セクションで想定される情報と同じ情報を返します。したがって、親ネームサーバーを指すサブドメインのネームサーバーをクエリしても、それらは返されません。

トピック

- チェックツールを使用した DNS クエリへの Amazon Route 53 の応答の確認
- チェックツールを使用した特定の IP アドレスからのクエリのシミュレート (位置情報およびレイテンシーレコードのみ)

チェックツールを使用した DNS クエリへの Amazon Route 53 の応答の確認

ツールを使用して、レコードに対する DNS クエリへの応答として Amazon Route 53 が返すレスポンスを確認できます。

チェックツールを使用して、Route 53 が DNS クエリにどうのように応答するかを確認するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [Hosted Zones] を選択します。
3. [Hosted Zones] ページで、ホストゾーンの名前を選択します。コンソールには、ホストゾーンのレコードのリストが表示されます。
4. [Check response from Route 53 (Route 53 からの応答を確認)] ページに直接移動するには、[Test record (レコードをテスト)] を選択します。
5. 次の値を指定します。
   - ホストゾーンの名前を除く、レコードの名前。たとえば、www.example.com をチェックするには、www と入力します。example.com をチェックするには、[レコード名] フィールドを空白のままにします。
   - チェックするレコードのタイプ (A や CNAME など)。
6. [Get Response] を選択します。
7. [Response returned by Route 53] セクションには、次の値が表示されます。

   DNS レスポンスコード

   クエリが有効であったかどうかを示すコード。最も一般的なレスポンスコードは、クエリが有効であったことを意味する NOERROR です。レスポンスが有効でない場合、Route 53 はその理由を示すレスポンスコードを返します。返されるレスポンスコードのリストについては、IANA ウェブサイトで「DNS RCODES」を参照してください。

   プロトコル

   Amazon Route 53 がクエリの応答に使用したプロトコル (UDP または TCP)。

Route 53 によって返されるレスポンス

Route 53 がウェブアプリケーションに返す値。値は次のいずれかです。

- 非エイリアスレコードの場合、レスポンスにはレコード内の値が含まれています。
- 同じ名前およびタイプの複数レコードの場合 (加重、レイテンシー、位置情報、フェイルオーバーを含む)、リクエストに基づいて、レスポンスには該当するレコードからの値が含まれています。
- 別のレコード以外の AWS リソースを参照するエイリアスレコードの場合、レスポンスにはリソースのタイプに応じて、 AWS リソースの IP アドレスまたはドメイン名が含まれます。
- 他のレコードを参照するエイリアスレコードの場合、レスポンスには参照されるレコードの値が含まれています。

チェックツールを使用した特定の IP アドレスからのクエリのシミュレート (位置情報およびレイテンシーレコードのみ)

レイテンシーまたは位置情報レコードを作成した場合、チェックツールを使用して DNS リゾルバーおよびクライアントの IP アドレスからのクエリをシミュレートできます。

チェックツールを使用して、指定された IP アドレスからのクエリをシミュレートするには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [Hosted Zones] を選択します。
3. [Hosted Zones] ページで、ホストゾーンの名前を選択します。コンソールには、ホストゾーンのレコードのリストが表示されます。
4. [Check response from Route 53] ページに直接移動するには、[Test record set] を選択します。

   特定のレコードの [Check response from Route 53] (Route 53 からのレスポンスを確認) ページに移動するには、そのレコードのチェックボックスを選択し、[Test record set] (レコードセットのテスト) を選択します。
5. まずレコードを選択せずに [レコードセットのテスト] を選択した場合、次の値を指定します。

   - ホストゾーンの名前を除く、レコードの名前。たとえば、www.example.com をチェックするには、www と入力します。example.com をチェックするには、[レコード名] フィールドを空白のままにします。

- チェックするレコードのタイプ (A や CNAME など)。

6. 適用可能な値を指定します。

   リゾルバー IP アドレス

   クライアントがリクエストに使用する DNS リゾルバーの場所をシミュレートする IPv4 または IPv6 アドレスを指定します。これは、レイテンシーおよび位置情報レコードのテストに役立ちます。この値を省略すると、ツールは AWS 米国東部 (バージニア北部) リージョン (us-east-1) の DNS リゾルバーの IP アドレスを使用します。

   EDNS0 クライアントサブネット IP

   リゾルバーが EDNS0 をサポートしている場合は、該当する地理的な場所の IP アドレスのクライアントサブネット IP (例: 192.0.2.0、2001:db8:85a3::8a2e:370:7334) を入力します。

   サブネットマスク

   [EDNS0 client subnet IP] に IP アドレスを指定した場合、オプションで、チェックツールが DNS クエリに含める IP アドレスのビット数を指定できます。例えば、EDNS0 クライアントサブネット IP に 192.0.2.44 を指定し、サブネットマスクに 24 を指定した場合には、チェックツールは 192.0.2.0/24 からのクエリをシミュレートします。デフォルト値は IPv4 アドレスの場合は 24 ビット、IPv6 アドレスの場合は 64 ビットです。

7. [Get Response] を選択します。

8. [Response returned by Route 53] セクションには、次の値が表示されます。

   Route 53 に送信された DNS クエリ

   クエリは、BIND 形式で、チェックツールが Route 53 に送信されたことを確認します。これは、ウェブアプリケーションがクエリの送信に使用するのと同じ形式です。3 つの値は通常、レコードの名前、IN (インターネットの場合)、レコードのタイプです。

   DNS レスポンスコード

   クエリが有効であったかどうかを示すコード。最も一般的なレスポンスコードは、クエリが有効であったことを意味する NOERROR です。レスポンスが有効でない場合、Route 53 はその理由を示すレスポンスコードを返します。返されるレスポンスコードのリストについては、IANA ウェブサイトで「DNS RCODES」を参照してください。

   プロトコル

   Amazon Route 53 がクエリの応答に使用したプロトコル (UDP または TCP)。

Route 53 によって返されるレスポンス

Route 53 がウェブアプリケーションに返す値。値は次のいずれかです。

- 非エイリアスレコードの場合、レスポンスにはレコード内の値が含まれています。
- 同じ名前およびタイプの複数レコードの場合 (加重、レイテンシー、位置情報、フェイルオーバーを含む)、リクエストに基づいて、レスポンスには該当するレコードからの値が含まれています。
- 別のレコード以外の AWS リソースを参照するエイリアスレコードの場合、レスポンスにはリソースのタイプに応じて、 AWS リソースの IP アドレスまたはドメイン名が含まれます。
- 他のレコードを参照するエイリアスレコードの場合、レスポンスには参照されるレコードの値が含まれています。

ホワイトラベルネームサーバーの設定

各 Amazon Route 53 ホストゾーンは、委任セットと呼ばれる 4 つのネームサーバーにリンクされています。デフォルトでは、これらのネームサーバーは ns-2048.awsdns-64.com のような名前です。ns1.example.com など、ネームサーバーをホストゾーンのドメイン名と一致するようにする場合は、ホワイトラベルネームサーバーを設定できます。これは、バニティネームサーバーまたはプライベートネームサーバーとも呼ばれます。

複数のドメインで再利用できる 4 つのホワイトラベルネームサーバーの組を設定する方法を次のステップで説明します。例えば、example.com、example.org、example.net というドメインを所有しているとします。このステップで example.com のホワイトラベルネームサーバーを設定し、それを example.org と example.net で再利用できます。

トピック

- ステップ 1: 再利用可能な Route 53 の委任セットを作成する
- ステップ 2: Amazon Route 53 ホストゾーンを作成または再作成し、NS レコードと SOA レコードの TTL を変更する
- ステップ 3: ホストゾーンにレコードを再作成する
- ステップ 4: IP アドレスを取得します
- ステップ 5: ホワイトラベルネームサーバーにレコードを作成する
- ステップ 6: NS と SOA レコードを更新します
- ステップ 7: グルーレコードを作成し、レジストラの名前サーバーを変更します。

- ステップ 8: ウェブサイトまたはアプリケーションのトラフィックをモニタリングします。
- ステップ 9: TTL を元の値に戻す
- ステップ 10: (オプション) 再帰的な DNS サービスへのお問い合わせ

ステップ 1: 再利用可能な Route 53 の委任セットを作成する

ホワイトラベルネームサーバーは、Route 53 の再利用可能な委任セットに関連付けられています。ホストゾーンと再利用可能な委任セットが同じ AWS アカウントによって作成された場合にのみ、ホストゾーンにホワイトラベルネームサーバーを使用できます。

再利用可能な委任セットを作成するには、Route 53 API、 CLI、またはいずれかの AWS SDKs AWS を使用できます。詳細については、次のドキュメントを参照してください。

- Route 53 API – Amazon Route 53 API リファレンスの「CreateReusableDelegationSet」を参照してください
- AWS CLI – AWS CLI コマンドリファレンスのcreate-reusable-delegation-set」を参照してください。
- AWS SDKs ドキュメントページの該当する SDK AWS ドキュメントを参照してください。

ステップ 2: Amazon Route 53 ホストゾーンを作成または再作成し、NS レコードと SOA レコードの TTL を変更する

Amazon Route 53 ホストゾーンを作成または再作成します。

- ホワイトラベルネームサーバーを使用するドメインの DNS サービスとして現在 Route 53 を使用していない場合 – ホストゾーンを作成し、以前のステップで作成した再利用可能な委託セットを各ホストゾーンに指定します。詳細については、Amazon Route 53 API リファレンスの「CreateHostedZone」を参照してください。
- ホワイトラベルネームサーバーを使用するドメインの DNS サービスとして Route 53 を使用している場合 – ホストゾーンを再作成し、前のステップで作成した再利用可能な委任セットにリンクする必要があります。

> **Important**
>
> 既存のホストゾーンのネームサーバーは変更できません。再利用可能な委任セットは、作成時にのみホストゾーンにリンクできます。

ホストゾーンを作成して、それに該当するドメインのリソースにアクセスを試みる前に、各ホストゾーンの次の TTL 値を変更します。

- ホストゾーンの NS レコードの TTL を 60 秒以下に変更します。
- ホストゾーンの SOA レコードの最小 TTL を 60 秒以下に変更します。これは SOA レコードの最後の値です。

ホワイトラベルネームサーバーの間違った IP アドレスをレジストラに付与すると、ウェブサイトは使用できなくなり、問題を修正した後も TTL でそのように維持されます。TTL を低く設定することで、ウェブサイトの停止時間を短縮できます。

ホストゾーンの作成と、ホストゾーンのネームサーバーに再利用可能な委任セットを指定する方法の詳細については、Amazon Route 53 API リファレンスの「CreateHostedZone」を参照してください。

ステップ 3: ホストゾーンにレコードを再作成する

ステップ 2 で作成したホストゾーンのレコードを作成する

- ドメインの DNS サービスを Amazon Route 53 に移行する場合 – 既存のレコードに関する情報をインポートしてレコードを作成することができます。詳細については、「ゾーンファイルをインポートしてレコードを作成する」を参照してください。
- ホワイトラベルネームサーバーを使用できるように既存のホストゾーンを置き換える場合 – 新しいホストゾーンで、現在のホストゾーンに表示されるレコードを再作成します。Route 53 には、ホストゾーンからレコードをエクスポートする方法が用意されていませんが、一部のサードパーティベンダーにはその機能があります。その後、Route 53 のインポート機能を使用して、ルーティングポリシーがシンプルな、非エイリアスレコードをインポートすることができます。ルーティングポリシーがシンプルでないエイリアスレコードまたはレコードをエクスポートして再インポートする方法はありません。

  Route 53 API を使用したレコード作成の詳細については、Amazon Route 53 API リファレンスの「CreateHostedZone」を参照してください。Route 53 コンソールを使用したレコード作成の詳細については、「レコードを使用する」を参照してください。

ステップ 4: IP アドレスを取得します

再利用可能な委託セット内のネームサーバーの IPv4 および IPv6 アドレスを取得して、次の表に入力します。

再利用可能な委託セットのネームサーバー名 (例: Ns-2048.awsdns-64.com)	IPv4 および IPv6 アドレス	ホワイトラベルネームサーバーに割り当てる名前 (例: ns1.example.com)
	IPv4: IPv6:	
	IPv4: IPv6:	
	IPv4: IPv6:	
	IPv4: IPv6:	

例えば、再利用可能な委託セットの 4 つのネームサーバーが次のようであるとします。

- ns-2048.awsdns-64.com
- ns-2049.awsdns-65.net
- ns-2050.awsdns-66.org
- ns-2051.awsdns-67.co.uk

4 つのネームサーバーのうち最初のサーバーの IP アドレスを取得するために実行する Linux および Windows コマンドを次に示します。

Linux での dig コマンド

```
% 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
```

Windows での nslookup コマンド

```
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
```

ステップ 5: ホワイトラベルネームサーバーにレコードを作成する

ホワイトラベルネームサーバーのドメイン名 (ns1.example.com など) と同じ名前 (example.com など) を持つホストゾーンで、8 つのレコードを作成します。

- 各ホワイトラベルネームサーバーの 1 つの A レコード
- 各ホワイトラベルネームサーバーの 1 つの AAAA レコード

> **Important**
>
> 同じホワイトラベルネームサーバーを複数のホストゾーンで使用する場合、他のホストゾーンではこのステップを実行しないでください。

レコードごとに、以下の値を指定します。以前のステップで記入した表を参照してください。

ルーティングポリシー

シンプルルーティングを指定します。

レコード名

ホワイトラベルネームサーバーの 1 つに割り当てる名前、例えば ns1.example.com です。プレフィックス (この例では ns1) としては、ドメイン名で有効な任意の値を使用できます。

値/トラフィックのルーティング先

再利用可能な委託セットにある 1 つの Route 53 ネームサーバーの、IPv4 または IPv6 アドレス。

> **Important**
>
> ホワイトラベルネームサーバーのレコードを作成するときに間違った IP アドレスを指定した場合、以降のステップを実行するときに、ウェブサイトまたはウェブアプリケーショ

ンをインターネットで利用できなくなります。IP アドレスをすぐに訂正した場合でも、ウェブサイトまたはウェブアプリケーションは、TTL の期間、利用できないままです。

レコードタイプ

IPv4 アドレスのレコードを作成する場合は A を指定します。

IPv6 アドレスのレコードを作成する場合は AAAA を指定します。

TTL (秒)

この値は、DNS リゾルバーが別の DNS クエリを Route 53 に転送する前に、このレコードの情報をキャッシュする時間です。このレコードに誤って正しくない値を指定した場合でも迅速に回復できるように、最初は 60 秒以下を指定することをお勧めします。

ステップ 6: NS と SOA レコードを更新します

ホワイトラベルネームサーバーに使用するホストゾーンの SOA レコードと NS レコードを更新します。ホストゾーンとそれに対応するドメインについてステップ 6 から ステップ 8 までを実行し、別のドメインとホストゾーンについても同じ作業を繰り返します。

> **Important**
> 作業は、ホワイトラベルネームサーバー (ns1.example.com など) と同じドメイン名 (example.com など) を持つ、Amazon Route 53 ホストゾーンから始めます。

1. Route 53 ネームサーバーの名前をホワイトラベルネームサーバーの 1 つの名前に置き換えて、SOA レコードを更新します。

   例

   Route 53 ネームサーバーの名前を置き換えます。

   ```
   ns-2048.awsdns-64.net. hostmaster.example.com. 1 7200 900 1209600 60
   ```

   ホワイトラベルネームサーバーの 1 つの名前を使用する。

   ```
   ns1.example.com. hostmaster.example.com. 1 7200 900 1209600 60
   ```

> **Note**
>
> 最後の値としての有効期限 (TTL) を ステップ 2: Amazon Route 53 ホストゾーンを作成または再作成し、NS レコードと SOA レコードの TTL を変更する で変更しました。

Route 53 コンソールを使用しながらのレコードの更新については、「レコードの編集」を参照してください。

2. NS レコードで、必要に応じて元のネームサーバーに戻せるように、ドメインの現在のネームサーバーの名前をメモします。
3. NS レコードを更新します。Route 53 ネームサーバーの名前を 4 つのホワイトラベルネームサーバーの名前、例えば `ns1.example.com`、`ns2.example.com`、`ns3.example.com`、および `ns4.example.com` に置き換えます。

ステップ 7: グルーレコードを作成し、レジストラの名前サーバーを変更します。

レジストラが用意している方法を使って、グルーレコードを作成し、レジストラのネームサーバーを変更します。

1. グルーレコードを追加します。
   - ホワイトラベルネームサーバーとドメイン名が同じドメインを更新する場合 – ステップ 4 で取得した値と名前および IP アドレスが一致する 4 件のグルーレコードを作成します。対応するグルーレコードにホワイトラベルネームサーバーの IPv4 および IPv6 アドレスの両方を含めてください。次に例を示します。

     ns1.example.com – IP アドレス = 192.0.2.117 および 2001:db8:85a3::8a2e:370:7334

     レジストラはグルーレコードを表すのにさまざまな用語を使っています。この作業は、新しいネームサーバーの登録などと言われていることもあります。
   - 別のドメインを更新する場合 – Route 53 が DNS サービスの場合、最初に前の箇条書きのステップを完了してから、ドメイン名と一致するグルーレコードを作成する必要があります。その後、この手順のステップ 2 にスキップします。
2. ドメインのネームサーバーをホワイトラベルネームサーバーの名前に変更します。

DNS サービスとして Amazon Route 53 を使用している場合は、「ドメインのネームサーバーおよびグルーレコードの追加あるいは変更」を参照してください。

ステップ 8: ウェブサイトまたはアプリケーションのトラフィックをモニタリングします。

ステップ 7 でグルーレコードを作成しネームサーバーを変更したウェブサイトまたはアプリケーションのトラフィックをモニタリングします。

- トラフィックが停止している場合 – レジストラから提供される方法を使って、ドメインのネームサーバーを以前の Route 53 ネームサーバーに戻します。これはステップ 6b でメモしたネームサーバーです。その後、何が悪かったのかを見極めます。
- トラフィックに影響がない場合 – 同じホワイトラベルネームサーバーを使用する残りのホストゾーンに対して、ステップ 6 ~ 8 を繰り返します。

ステップ 9: TTL を元の値に戻す

ホワイトラベルネームサーバーを使用するようになったすべてのホストゾーンについて、以下の値を変更します。

- ホストゾーンの NS レコードの TTL を、NS レコードでもっと一般的な値、例えば 172800 秒 (2 日) に変更します。
- ホストゾーンの SOA レコードの最小 TTL を、SOA レコードでもっと一般的な値、例えば 900 秒に変更します。これは SOA レコードの最後の値です。

ステップ 10: (オプション) 再帰的な DNS サービスへのお問い合わせ

オプション Amazon Route 53 の位置情報ルーティングを使用している場合は、EDNS0 の edns-client-subnet 拡張をサポートする再帰的 DNS サービスに連絡して、ホワイトラベルネームサーバーの名前を伝えます。こうすることで、この DNS サービスは、クエリが発信されたおおよその地理的場所に基づいて、最適な場所にある Route 53 に対し DNS クエリをルーティングし続けることができます。

Amazon Route 53 がパブリックホストゾーンに作成する NS レコードと SOA レコード

作成したパブリックホストゾーンごとに、Amazon Route 53 はネームサーバー (NS) レコードと Start of Authority (SOA) レコードを自動的に作成します。これらのレコードを変更する必要はほとんどありません。

トピック

- ネームサーバー (NS) レコード
- Start of Authority (SOA) レコード

ネームサーバー (NS) レコード

Amazon Route 53 によって、ホストゾーンと同じ名前のネームサーバー (NS) レコードが自動的に作成されます。これには、ホストゾーンの 4 つの正式なネームサーバーがリストされます。まれな状況を除き、このレコードのネームサーバーを追加、変更、または削除しないことをお勧めします。

次の例に、Route 53 ネームサーバーの名前の形式を示します (これらはサンプルとして提供されています。レジストラのネームサーバーレコードを更新する際には、これらを使用しないでください)。

- ns-2048.awsdns-64.com
- ns-2049.awsdns-65.net
- ns-2050.awsdns-66.org
- ns-2051.awsdns-67.co.uk

ホストゾーンのネームサーバーのリストを取得するには:

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [Hosted zones (ホストゾーン)] をクリックします。
3. [Hosted Zones (ホストゾーン)] ページで、ホストゾーンのラジオボタン (名前ではない) を選択し、[View details (詳細を表示)] を選択します。
4. ホストゾーンの詳細ページで、[Hosted zone details (ホストゾーンの詳細)] を選択します。
5. [Name Servers] (ネームサーバー) で一覧表示されている 4 つのサーバー名を書き留めます。

他の DNS サービスプロバイダから Route 53 への DNS サービスの移行方法については、「Amazon Route 53 を既存ドメインの DNS サービスとして使用する」を参照してください。

Start of Authority (SOA) レコード

Start of Authority (SOA) レコードは、ドメインに関する基本 DNS 情報を保持します。次に例を示します。

```
ns-2048.awsdns-64.net. hostmaster.example.com. 1 7200 900 1209600 86400
```

SOA レコードには以下の要素が含まれています。

- SOA レコードを作成した Route 53 ネームサーバー (例: `ns-2048.awsdns-64.net`)。
- 管理者の E メールアドレス。@ 記号はピリオドに置き換えられます (例: `hostmaster.example.com`)。デフォルト値は、監視されない amazon.com E メールアドレスです。
- ホストゾーンのレコードを更新するたびに に追加できるシリアル番号。Route 53 は単独で番号を変更しません。(シリアル番号はセカンダリ DNS をサポートする DNS サービスによって使用されます)。この例では、この値は 1 です。
- 変更を確認するためにプライマリ DNS サーバーの SOA レコードを問い合わせるまでに、セカンダリ DNS サーバーが待機するリフレッシュ時間 (秒数)。この例では、この値は `7200` です。
- 失敗したゾーン転送を再試行するまでに、セカンダリサーバーが待機する再試行間隔 (秒数)。通常は、再試行時間はリフレッシュ時間より短くなります。この例では、この値は `900` (15 分) です。
- セカンダリサーバーがゾーン転送を終了し続ける秒単位の時間。この時間が転送に成功せずに経過すると、セカンダリサーバーはデータを古すぎて信頼性が高くないと見なすため、クエリへの応答を停止します。この例では、この値は `1209600` (2 週間) です。
- 最小有効期限 (TTL)。この値は、再帰リゾルバーが Route 53 から次のレスポンスをキャッシュする期間を設定するのに役立ちます。

  NXDOMAIN

  DNS クエリで指定された名前 (example.com など) を持つレコードは、どのようなタイプのものも存在しません。また、DNS クエリで指定された名前 (zenith.example.com など) を持つ子のレコードも存在しません。

  NODATA

  DNS クエリで指定された名前を持つレコードが少なくとも 1 つありますが、いずれも DNS クエリで指定されたタイプ (A など) のレコードではありません。

  DNS リゾルバーで NXDOMAIN または NODATA をキャッシュすることは、ネガティブキャッシングと呼ばれます。

  ネガティブキャッシングの期間は、次の値にうち小さいほうです。

  - この値 – SOA レコードの最小 TTL。前述の例では、この値は `86400` (1 日) です。

- SOA レコードの TTL の値。デフォルト値は 900 秒です。この値の変更については、「レコードの編集」を参照してください。

Route 53 が NXDOMAIN または NODATA レスポンス (ネガティブレスポンス) で DNS クエリに応答する場合は、標準クエリの料金が課金されます (Amazon Route 53 料金表の「クエリ」を参照してください) 。ネガティブレスポンスのコストが懸念される場合は、1 つのオプションとして、SOA レコードの TTL、SOA レコードの最小 TTL (この値)、またはその両方を変更します。ホストゾーン全体の否定的なレスポンスに適用されるこれらの TTLs を上げると、良い影響と悪い影響の両方が生じる可能性があることに注意してください。

- インターネット上の DNS リゾルバーがレコードの不在をキャッシュする期間が長くなるため、Route 53 に転送されるクエリの数が減ります。これにより、DNS クエリに関する Route 53 料金が削減されます。
- ただし、有効なレコードを誤って削除して後で再作成すると、DNS リゾルバーがネガティブレスポンス (このレコードは存在しない) をキャッシュする期間が長くなります。これにより、顧客やユーザーが、対応するリソース (acme.example.com の Web サーバーなど) にアクセスできない時間が長くなります。

Route 53 で SOA レコードを検索するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [Hosted zones] を選択します。
3. レコードを表示するドメインのリンク名を選択します。
4. [Records] (レコード) セクションでは、すべてのレコードをリスト表示でき、その結果をフィルタリングして、SOA 値を検索することもできます。

パブリック DNS レコードを管理するための高速リカバリの有効化

パブリック DNS レコードを管理する Route 53 高速リカバリは、米国東部 (バージニア北部) リージョンが使用できなくなった場合に 60 分の目標復旧時間 (RTO) を達成するのに役立ちます。Route 53 パブリックホストゾーンでこの機能を有効にすると、 が米国東部 (バージニア北部) リージョンに障害 AWS があることを検出してから約 60 分以内に DNS の変更を再開できます。

> **Important**
>
> 高速復旧は、パブリックホストゾーンでのみ使用できます。プライベートホストゾーンはサポートされていません。

> **Note**
>
> Route 53 データプレーンからの DNS クエリ解決は、リージョンのサービスに障害が発生しても正常に動作し続けます。データプレーンとコントロールプレーンオペレーションの理解については、「Route 53 の耐障害性」を参照してください。

トピック

- パブリック DNS レコードの高速リカバリの仕組み
- フェイルオーバー後の DNS 変更の再送信
- 米国東部 (バージニア北部) リージョンへのフェイルバック
- その他の考慮事項
- パブリック DNS レコードを管理するための高速復旧を有効にする方法

パブリック DNS レコードの高速リカバリの仕組み

高速復旧が有効になっている場合、Route 53 はパブリックホストゾーンのコピーを米国西部 (オレゴン) リージョンに保持します。米国東部 (バージニア北部) リージョンが長時間使用できなくなった場合、Route 53 は 60 分以内にフェイルオーバーします。次に、有効なホストゾーンのコントロールプレーンリクエストを米国西部 (オレゴン) リージョンにルーティングします。その後、CLI、SDK、API を使用して DNS の変更を継続できます。フェイルオーバー中は一部の API メソッドのみが機能することに注意してください。詳細については、「その他の考慮事項」セクションを参照してください。リージョンが回復すると、Route 53 は米国東部 (バージニア北部) リージョンにフェイルバックします。

> **Note**
>
> 米国東部 (バージニア北部) リージョンで問題が発生する前に、高速復旧を有効にする必要があります。これを行うには、コンソール、CLI、SDK、または API を使用します (以下の「パ

ブリック DNS レコードを管理するための高速復旧を有効にする方法」セクションを参照してください) 。フェイルオーバーの開始後、高速復旧を有効にすることはできません。

フェイルオーバー後の DNS 変更の再送信

通常の条件下では、高速復旧によるパブリックホストゾーンへの変更は、米国東部 (バージニア北部) リージョンで受け入れられ、米国西部 (オレゴン) リージョンにコピーされます。ただし、米国東部 (バージニア北部) リージョンで停止が発生した場合、一部の変更は受け入れられますが、まだ米国西部 (オレゴン) リージョンにコピーされていない場合があります。これらの進行中の変更は、「ストランド変更」と呼ばれます。フェイルオーバーが完了したら、Route 53 は、DNS 作業を続行する前に、ストランドされた変更を再送信することをお勧めします。これを行うには、以下で説明するように API または AWS CloudFormation を使用します。

API を使用して DNS の変更を追跡および送信する

Route 53 API、 AWS CLI、または AWS SDKs を使用して DNS レコードを管理する場合は、ChangeResourceRecordSets API を使用して変更を送信し、GetChange API を使用して変更を追跡します。

ChangeResourceRecordSets を呼び出すと、Route 53 は変更の ID を返します (詳細については、ChangeInfo」を参照) 。その後、この ID を GetChange に渡してステータスを確認できます。INSYNC のステータスは、変更が米国西部 (オレゴン) リージョンにコピーされ、すべての Route 53 DNS サーバーに送信されたことを意味します。これらの変更に対してそれ以上何もする必要はありません。ただし、米国東部 (バージニア北部) リージョンの停止中に、GetChange が PENDING を返す場合があります。つまり、変更がコピーされていない可能性があります。この場合、フェイルオーバーが終了すると、GetChange は NoSuchChange を返します。つまり、Route 53 はその変更をコピーできませんでした。これらのストランドされた変更は無視して、新しい変更として再送信できます。フェイルオーバーは、Route 53 が AWS メッセージを Health Dashboard に投稿するときに行われます。

AWS CloudFormation を使用した変更の追跡と送信

AWS CloudFormation は、GetChange API を使用して DNS の変更のステータスを追跡します。更新は、変更が INSYNC になった後にのみマークされます。CloudFormation を使用して DNS レコードを管理している間に米国東部 (バージニア北部) リージョンが使用できなくなった場合、停止中にアクションは終了しません。Route 53 フェイルオーバーが完了したら、同じアクションを再試行して、CloudFormation が DNS の変更を再送信できるようにします。

米国東部 (バージニア北部) リージョンへのフェイルバック

Route 53 は、パブリックホストゾーンのコントロールプレーンの作業を、そのリージョンが回復した後に米国東部 (バージニア北部) リージョンにフェイルバックします。このプロセス中にストランドされた変更が作成されないため、フェイルバック中に DNS 変更を再送信する必要はありません。

その他の考慮事項

高速復旧機能について知っておくべきことが他にもいくつかあります。

1. フェイルオーバー中に、新しいホストゾーンの作成、ホストゾーンの削除、DNSSEC 署名の有効化、DNSSEC 署名の無効化を行うことはできません。
2. AWS PrivateLink リンクはフェイルオーバー後に機能しませんが、米国東部 (バージニア北部) リージョンへのフェイルバック後に再び機能します。
3. CloudFront の定額プランは現在サポートされていません。
4. 高速リカバリを使用するホストゾーンは削除できません。ホストゾーンを削除する前に、高速復旧をオフにする必要があります。
5. フェイルオーバー中、これらの API メソッドは高速リカバリを備えたパブリックホストゾーンでも機能します。他のすべての Route 53 API メソッドは、フェイルバックするまで機能しません。
   - `ChangeResourceRecordSets`
   - `GetChange`
   - `GetGeoLocation`
   - `GetHostedZone`
   - `GetHostedZoneCount`
   - `GetHostedZoneLimit`
   - `GetReusableDelegationSet`
   - `GetReusableDelegationSetLimit`
   - `ListGeoLocations`
   - `ListHostedZones`
   - `ListHostedZonesByName`
   - `ListResourceRecordSets`
   - `ListReusableDelegationSets`

パブリック DNS レコードを管理するための高速復旧を有効にする方法

Route 53 コンソール、API、CLI、または SDK を使用して、高速復旧を有効にできます。所要時間は、ホストゾーンのサイズやその他の要因によって異なります。プロセスに最大数時間かかることを計画します。ステータスは、ホストゾーンの高速復旧タブまたは GetHostedZone API で確認できます。プロセスの最後には、DNS の変更が受け入れられない期間が数分あります。その後、DNS の変更は通常どおり機能します。

Route 53 コンソールを使用して高速復旧を有効または無効にするには

1. Route 53 コンソール (https://console.aws.amazon.com/route53/) を開きます。
2. ナビゲーションペインで [Hosted zones] を選択します。
3. 高速復旧を有効にするパブリックホストゾーンを選択します。
4. 高速復旧タブで、有効化を選択します。
5. [Save changes] (変更の保存) をクリックします。
6. ホストゾーンのステータスをモニタリングします。ステータスは、セットアップ時の高速復旧の有効化と、完了時の有効化への変更を示しています。

上記の同じステップを使用して高速復旧を無効にすることができますが、代わりに Disable を選択します。

を有効にする CLI の例

```
aws route53 update-hosted-zone-features --enable-accelerated-recovery --hosted-zone-id
 Z123456789
```

を無効にする CLI の例

```
aws route53 update-hosted-zone-features --no-enable-accelerated-recovery --hosted-zone-
id Z123456789
```

プライベートホストゾーンの使用

プライベートホストゾーンは、Amazon VPC サービスで作成する 1 つ以上の VPC 内のドメインとそのサブドメインへの DNS クエリに対し、Amazon Route 53 がどのように応答するかに関する情報を保持するコンテナです。プライベートホストゾーンの動作は次のとおりです。

1. example.com などのプライベートホストゾーンを作成して、ホストゾーンに関連付ける VPC を指定します。ホストゾーンを作成すると、さらに多くの VPC をそのゾーンに関連付けることができます。
2. VPC 内および VPC 間でドメインとサブドメインへの DNS クエリに Route 53 が応答する方法を決定するホストゾーンに、レコードを作成します。例えば、プライベートホストゾーンに関連付けた VPC に、EC2 インスタンスで実行されるデータベースサーバーがあるとします。A または AAAA レコードを作成し (例: db.example.com)、データベースサーバーの IP アドレスを指定します。

   レコードの詳細については、「レコードを使用する」を参照してください。プライベートホストゾーンを使用する際の Amazon VPC の要件については、Amazon VPC ユーザーガイドの「プライベートホストゾーンの使用 」を参照してください。
3. アプリケーションが db.example.com への DNS クエリを送信すると、Route 53 は対応する IP アドレスを返します。プライベートホストゾーンから回答を取得するには、関連付けられた VPCs のいずれかで EC2 インスタンスを実行しているか、ハイブリッドセットアップからインバウンドエンドポイントを持っている必要があります。VPCs またはハイブリッドセットアップの外部からプライベートホストゾーンにクエリを実行すると、クエリはインターネット上で再帰的に解決されます。
4. アプリケーションは、Route 53 から取得した IP アドレスを使用して、データベースサーバーとの接続を確立します。

プライベートホストゾーンを作成すると以下のネームサーバーが使用されます。

- ns-0.awsdns-00.com
- ns-512.awsdns-00.net
- ns-1024.awsdns-00.org
- ns-1536.awsdns-00.co.uk

DNS プロトコルは、すべてのホストゾーンに NS レコードを設定する必要があるため、これらのネームサーバーが使用されます。これらのネームサーバーは予約済みであり、Route 53 パブリックホストゾーンでは使用されません。これらのゾーンは、プライベートホストゾーンで指定された VPC に接続されたインバウンドエンドポイントを使用して、ホストゾーンに関連付けられた VPC の VPCs Resolver を介してのみクエリできます。

ネームサーバーがインターネットに表示されていても、VPC Resolver はネームサーバーアドレスに接続しません。さらに、インターネット経由でネームサーバーへのクエリを直接実行しても、プライ

ベートホストゾーンの情報は返されません。代わりに、VPC リゾルバーは、VPC からホストゾーンへの関連付けに基づくプライベート名前空間内にクエリがあることを検出し、直接のプライベート接続を使用してプライベート DNS サーバーに到達します。

> **Note**
>
> プライベートホストゾーンの NS レコードセットは必要に応じて変更できますが、プライベートな DNS 解決は引き続き機能します。この方法は推奨できませんが、希望する場合は、パブリック DNS サーバーでは使用されない予約済みのドメイン名を使用してください。

インターネットでドメインへのトラフィックをルーティングする場合は、Route 53 のパブリックホストゾーンを使用します。詳細については、「「パブリックホストゾーンの操作」」を参照してください。

トピック

- プライベートホストゾーンを使用する場合の考慮事項
- プライベートホストゾーンの作成
- プライベートホストゾーンの一覧表示
- プライベートホストゾーンにさらに VPC を関連付ける
- Amazon VPC と、作成したプライベートホストゾーンを異なる AWS アカウントに関連付ける
- プライベートホストゾーンから VPC の関連付けを解除する
- プライベートホストゾーンの削除
- VPC アクセス許可

プライベートホストゾーンを使用する場合の考慮事項

プライベートホストゾーンを使用する場合は、以下の点を考慮してください。

- 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 VPC Resolver rules
- Delegating responsibility for a subdomain
- Custom DNS servers
- Required IAM permissions

Amazon VPC の設定

プライベートホストゾーンを使用するには、次の Amazon VPC 設定で `true` を指定する必要があります：

- `enableDnsHostnames`
- `enableDnsSupport`

詳細については「Amazon VPC ユーザーガイド」の「VPC の DNS 属性の表示と更新」を参照してください。

Route 53 ヘルスチェック

プライベートホストゾーンの Route 53 ヘルスチェックでは、フェイルオーバー、複数値レスポンス、加重、レイテンシー、位置情報、地理的近接性レコードのみへの関連付けが可能です。ヘルスチェックとフェイルオーバーレコードの関連付けの詳細については、「プライベートホストゾーンのフェイルオーバーの設定」を参照してください。

プライベートホストゾーンのレコードでサポートされるルーティングポリシー

プライベートホストゾーンにレコードを作成すると、次のルーティンポリシーを使用できます。

- シンプルルーティング
- フェイルオーバールーティング
- 複数値回答ルーティング
- 加重ルーティング
- レイテンシーに基づくルーティング
- 位置情報ルーティング
- 地理的近接性ルーティング

その他のルーティングポリシーを使用してプライベートホストゾーンでレコードを作成することはサポートされていません。

スプリットビュー DNS

Route 53 を使用して、スプリットビュー DNS (別名、スプリットホライズン DNS) を設定できます。スプリットビュー DNS では、内部使用 (accounting.example.com) とパブリックウェブサイト (www.example.com) などの外部使用で同じドメイン名 (example.com) を使用します。内部および外部で同じサブドメイン名を使用したいが、内部ユーザーと外部ユーザーに対して、異なるコンテンツを供給したり、異なる認証を要求したりする場合もあります。

スプリットビュー DNS を設定するには、以下の手順を実行します。

1. 同じ名前を持つパブリックホストゾーンおよびプライベートホストゾーンを作成します。(スプリットビュー DNS は、パブリックホストゾーンに別の DNS サービスを使用している場合でも機能します)。
2. 1 つ以上の Amazon VPC をプライベートホストゾーンに関連付けます。Route 53 VPC Resolver は、プライベートホストゾーンを使用して、指定された VPCs。
3. 各ホストゾーンにレコードを作成します。パブリックホストゾーンのレコードはインターネットトラフィックのルーティング方法を制御し、プライベートホストゾーンのレコードは Amazon VPC でのトラフィックのルーティング方法を制御します。

VPC とオンプレミスの両方のワークロードの名前解決を実行する必要がある場合は、Route 53 VPC Resolver を使用できます。詳細については、「Route 53 VPC Resolver とは」を参照してください。

名前空間が重複するパブリックホストゾーンとプライベートホストゾーン

や example.com など、名前空間が重複するプライベートホストゾーンとパブリックホストゾーンがある場合 accounting.example.com 、VPC Resolver は最も具体的な一致に基づいてトラフィックをルーティングします。ユーザーがプライベートホストゾーンに関連付けられた Amazon VPC の EC2 インスタンスにログインすると、Route 53 VPC Resolver が DNS クエリを処理する方法は次のとおりです。

1. VPC Resolver は、プライベートホストゾーンの名前が accounting.example.com などのリクエストのドメイン名と一致するかどうかを評価します。次のいずれかに該当すると、一致したとみなされます。
   - 完全な一致
   - プライベートホストゾーンの名前がリクエスト内のドメイン名の親である。例えば、リクエスト内のドメイン名が次のような名前であるとします。

     seattle.accounting.example.com

次のホストゾーンは seattle.accounting.example.com の親であるため、これらが一致します。

- accounting.example.com
- example.com

一致するプライベートホストゾーンがない場合、VPC Resolver はリクエストをパブリック DNS リゾルバーに転送し、リクエストは通常の DNS クエリとして解決されます。

2. プライベートホストゾーン名がリクエストのドメイン名と一致する場合、VPC Resolver は、accounting.example.com の A レコードなど、ドメイン名と DNS タイプに一致するレコードをホストゾーンで検索します。

> **Note**
>
> 一致するプライベートホストゾーンがあるが、リクエストのドメイン名とタイプに一致するレコードがない場合、VPC リゾルバーはリクエストをパブリック DNS リゾルバーに転送しません。代わりに、NXDOMAIN (存在しないドメイン) をクライアントに返します。

名前空間が重複する複数のプライベートホストゾーン

や example.com など、名前空間が重複するプライベートホストゾーンが 2 つ以上ある場合 accounting.example.com 、VPC Resolver は最も具体的な一致に基づいてトラフィックをルーティングします。

> **Note**
>
> プライベートホストゾーン (example.com) と、同じドメイン名のネットワークにトラフィックをルーティングする Route 53 VPC Resolver ルールがある場合、VPC Resolver ルールが優先されます。「Private hosted zones and Route 53 VPC Resolver rules」を参照してください。

ユーザーがすべてのプライベートホストゾーンに関連付けられている Amazon VPC の EC2 インスタンスにログインすると、VPC Resolver が DNS クエリを処理する方法は次のとおりです。

1. VPC Resolver は、accounting.example.com などのリクエスト内のドメイン名がプライベートホストゾーンのいずれかの名前と一致するかどうかを評価します。

2. リクエスト内のドメイン名と正確に一致するホストゾーンがない場合、VPC Resolver はリクエスト内のドメイン名の親である名前を持つホストゾーンをチェックします。例えば、リクエスト内のドメイン名が次のような名前であるとします。

   `seattle.accounting.example.com`

   次のホストゾーンは `seattle.accounting.example.com` の親であるため、一致します。

   - `accounting.example.com`
   - `example.com`

   VPC Resolver は よりも具体的`accounting.example.com`であるため、 を選択します`example.com`。

3. VPC Resolver は、 の A レコードなど、リクエスト内のドメイン名と DNS タイプに一致するレコードを`accounting.example.com`ホストゾーンで検索します`seattle.accounting.example.com`。

   リクエストのドメイン名とタイプに一致するレコードがない場合、VPC Resolver は NXDOMAIN (存在しないドメイン) をクライアントに返します。

プライベートホストゾーンと Route 53 VPC Resolver ルール

プライベートホストゾーン (example.com) と、同じドメイン名のネットワークにトラフィックをルーティングする VPC Resolver ルールがある場合、VPC Resolver ルールが優先されます。

例えば、次の設定があるとします。

- example.com というプライベートホストゾーンがあり、それを VPC に関連付けます。
- example.com のトラフィックをネットワークに転送する Route 53 VPC Resolver ルールを作成し、そのルールを同じ VPC に関連付けます。

この設定では、VPC Resolver ルールがプライベートホストゾーンよりも優先されます。DNS クエリは、プライベートホストゾーンのレコードに基づいて解決されるのではなく、ネットワークに転送されます。

サブドメインの責任の委任

サブドメインの責任を委任する NS レコードをプライベートホストゾーンに作成できるようになりました。詳細については、「リゾルバーの委任ルールのチュートリアル」を参照してください。

カスタム DNS サーバー

VPC 内の Amazon EC2 インスタンスでカスタム DNS サーバーを設定した場合、プライベート DNS クエリを VPC 用に Amazon が提供する DNS サーバーの IP アドレスにルーティングするようにそれらの DNS サーバーを設定する必要があります。この IP アドレスは、VPC ネットワーク範囲のベースに「プラス 2」した IP アドレスです。例えば、VPC の CIDR 範囲が 10.0.0.0/16 である場合、DNS サーバーの IP アドレスは 10.0.0.2 です。

VPCs とネットワーク間で DNS クエリをルーティングする場合は、VPC Resolver を使用できます。詳細については、「Route 53 VPC Resolver とは」を参照してください。

必要な IAM アクセス許可

プライベートホストゾーンを作成するには、Route 53 アクションのアクセス許可に加えて、Amazon EC2 アクションのアクセス許可を IAM に付与する必要があります。詳細については、「サービス承認リファレンス」の「Actions, resources, and condition keys for Route 53」を参照してください。

プライベートホストゾーンの作成

プライベートホストゾーンは、1 つ以上の Amazon Virtual Private Cloud (VPC) でホストするドメインを対象としたレコードのコンテナです。ドメイン (例えば、example.com) のホストゾーンを作成した後、VPC 内および VPC 間でそのドメインへのトラフィックをルーティングする方法を Amazon Route 53 に伝えるレコードを作成します。

> **Important**
>
> プライベートホストゾーンを作成する際、VPC とホストゾーンを関連付ける必要があります。VPC は、必ずホストゾーン作成時と同一のアカウントを使用して作成します。ホストゾーンを作成したら、別の AWS アカウントを使用して作成した VPCs など、追加の VPCs をホストゾーンに関連付けることができます。
> あるアカウントを使用して作成した VPC と、別のアカウントを使用して作成したプライベートホストゾーンを関連付けるには、関連付けを許可してから、その関連付けをプログラム的にする必要があります。詳細については、「Amazon VPC と、作成したプライベートホストゾーンを異なる AWS アカウントに関連付ける」を参照してください。

Route 53 API を使用してのプライベートホストゾーンの作成については、 [Amazon Route 53 API リファレンス] を参照してください。

Route 53 コンソールを使用してプライベートホストゾーンを作成するには

1. Route 53 ホストゾーンに関連付ける各 VPC について、次の VPC 設定を `true` に変更します。

   - `enableDnsHostnames`
   - `enableDnsSupport`

   詳細については、Amazon VPC ユーザーガイドの「VPC の DNS サポートを更新する」を参照してください。
2. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
3. Route 53 を初めて使用する場合は、[今すぐ始める] を選択します。

   既に Route 53 を利用している場合は、ナビゲーションペインの [Hosted zones (ホストゾーン)] を選択します。
4. [ホストゾーンの作成] を選択します。
5. [Create Private Hosted Zone] ペインで、ドメイン名を入力し、必要に応じてコメントも入力します。

   a ~ z、0 ~ 9、- (ハイフン) 以外の文字を指定する方法、および国際化されたドメイン名を指定する方法については、「DNS ドメイン名の形式」を参照してください。
6. [Type (タイプ)] リストから、[Private Hosted Zone (プライベートホストゾーン)] を選択します。
7. [VPC ID] リストで、このプライベートホストゾーンに関連付ける VPC を選択します。

   > **Note**
   >
   > コンソールに次のメッセージが表示されている場合、ホストゾーンを、同じ VPC 内にあり同じ名前空間を持つ別のホストゾーンと関連付けようとしています。
   > 「競合中のドメインは、特定の VPC または委託セットと既に関連付けられています」
   > 例えば、ホストゾーン A とホストゾーン B の両方で、`example.com`のように同じドメインネームとなっている場合は、両方のホストゾーンを共通の VPC に関連付けることはできません。
8. [ホストゾーンの作成] を選択します。

プライベートホストゾーンの一覧表示

Amazon Route 53 コンソールを使用して、現在の AWS アカウントで作成したすべてのホストゾーンを一覧表示できます。Route 53 API を使用してホストゾーンを一覧表示する方法については、Amazon Route 53 API リファレンスの「ListHostedZones」を参照してください。

AWS アカウントに関連付けられたホストゾーンを一覧表示するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [Hosted zones] を選択します。

   ホストゾーンページには、現在の AWS アカウントを使用して作成されたすべてのホストゾーンのリストが自動的に表示されます。[Type] 列は、ホストゾーンがプライベートかパブリックかを示しています。列見出しを選択すると、プライベートホストゾーンとパブリックホストゾーンがグループ分けされます。

プライベートホストゾーンにさらに VPC を関連付ける

同じ AWS アカウントを使用してホストゾーンと VPCs を作成した場合は、Amazon Route 53 コンソールを使用して、より多くの VPCs をプライベートホストゾーンに関連付けることができます。

> **Important**
>
> あるアカウントを使用して作成した VPC と、別のアカウントを使用して作成したプライベートホストゾーンを関連付ける場合は、まず関連付けを許可する必要があります。また、関連付けを許可する場合や VPC をホストゾーンに関連付ける場合はいずれも、 AWS コンソールを使用することはできません。詳細については、「Amazon VPC と、作成したプライベートホストゾーンを異なる AWS アカウントに関連付ける」を参照してください

Route 53 API を使用して、より多くの VPC をプライベートホストゾーンに関連付ける方法については、Amazon Route 53 API リファレンスの「AssociateVPCWithHostedZone」を参照してください。

Route 53 コンソールを使用してプライベートホストゾーンに VPC をさらに関連付けるには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [Hosted zones] を選択します。

3. さらに VPC を関連付けるプライベートホストゾーンのラジオボタンを選択します。
4. [編集] を選択します。
5. [Add VPC (VPC を追加)] を選択します。
6. このホストゾーンに関連付けるリージョンと VPC の ID を選択します。
7. さらに VPC をこのホストゾーンに関連付けるには、ステップ 5 と 6 を繰り返します。
8. [Save changes] (変更の保存) をクリックします。

Amazon VPC と、作成したプライベートホストゾーンを異なる AWS アカウントに関連付ける

1 つの AWS アカウントで作成した VPC を、別のアカウントで作成したプライベートホストゾーンに関連付ける場合は、次の手順を実行します。

Amazon VPC と、作成したプライベートホストゾーンを異なる AWS アカウントに関連付けるには

1. ホストゾーンを作成したアカウントを使用して、次のいずれかの方法で VPC とプライベートホストゾーンの関連付けを許可します。

   - AWS CLI – AWS CLI コマンドリファレンスの create-vpc-association-authorization を参照してください。
   - AWS SDK または AWS Tools for Windows PowerShell – ドキュメントページの該当するAWS ドキュメントを参照してください。
   - Amazon Route 53 API – [Amazon Route 53 API リファレンス] の「CreateVPCAssociationAuthorization」を参照してください。

   次の点に注意してください。

   - あるアカウントで作成した複数の VPC と別のアカウントで作成したホストゾーンを関連付ける場合は、VPC ごとに認可リクエストを送信する必要があります。
   - 関連付けを許可する際、ホストゾーン ID を指定する必要があるため、プライベートホストゾーンが存在している必要があります。
   - VPC とプライベートホストゾーンの関連付けを許可する場合や、関連付けを作成する場合はいずれも、Route 53 コンソールを使用することはできません。
2. VPC を作成したアカウントを使用して、VPC をこのホストゾーンと関連付けます。関連付けの承認と同様に、 AWS SDK、Tools for Windows PowerShell、、 AWS CLIまたは Route 53 API

を使用できます。この API を使用している場合は、「AssociateVPCWithHostedZone」アクションを使用します。

3. 推奨 – VPC をホストゾーンと関連付けるために、ここでの許可を削除します。許可を削除しても関連付けには影響しませんが、今後 この VPC とホストゾーンを再度関連付けることはできません。ホストゾーンと VPC を再関連付けしたい場合は、この手順のステップ 1 および 2 を繰り返します。

> **Important**
>
> `ListHostedZonesByVPC` は VPC を指定したホストゾーンを返し、`GetHostedZone` API はホストゾーンに関連付けられた VPC を返します。これらの API は、`AssociateVPCWithHostedZone` API によって作成されるホストゾーンと VPC の関連付け、またはプライベートホストゾーンの作成時のみを考慮します。VPC へのホストゾーンの関連付けの完全なリストが必要な場合は、ListProfileResourceAssociations も呼び出してください。

> **Note**
>
> 作成できる許可の最大数については、「エンティティのクォータ」を参照してください。

プライベートホストゾーンから VPC の関連付けを解除する

Amazon Route 53 コンソールを使用して、プライベートホストゾーンから VPC の関連付けを解除できます。これにより Route 53 は、VPC から DNS クエリが送られたホストゾーン内のレコードを使用する、トラフィックのルーティングを停止します。例えば、example.com ホストゾーンと VPC を関連付けた後に、その VPC とホストゾーンの関連付けを解除すると、Route 53 は、example.com または example.com ホストゾーン内の他のレコードの DNS クエリの解決を停止します。

> **Note**
>
> 最後の VPC とプライベートホストゾーンの関連付けを解除することはできません。その VPC の関連付けを解除するには、まず別の VPC をホストゾーンに関連付ける必要があります。

プライベートホストゾーンから VPC の関連付けを解除するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [Hosted zones] を選択します。
3. 1 つ以上のVPC の関連付けを解除する、プライベートホストゾーンに対応しているラジオボタンをオンにします。
4. [Edit] を選択します。
5. [Remove VPC (VPC を削除)] を選択します。このホストゾーンから関連付けを解除する VPC の横にあります。
6. [Save changes] (変更の保存) をクリックします。

プライベートホストゾーンの削除

このセクションでは、Amazon Route 53 コンソールを使用してプライベートホストゾーンを削除する方法を説明します。

デフォルトの SOA レコードと NS レコード以外のレコードがない場合にのみ、プライベートホストゾーンを削除できます。ホストゾーンに他のレコードが含まれる場合、ホストゾーンを削除する前にそれらを削除する必要があります。これによって、レコードが含まれているホストゾーンを誤って削除するのを防ぎます。

トピック

- 別のサービスによって作成されたプライベートホストゾーンを削除する
- Route 53 コンソールを使用してプライベートホストゾーンを削除する

別のサービスによって作成されたプライベートホストゾーンを削除する

プライベートホストゾーンが別のサービスで作成されている場合、Route 53 コンソールを使用して削除することはできません。代わりに、他のサービスに該当するプロセスを使用する必要があります。

- AWS Cloud Map – プライベート DNS 名前空間の作成 AWS Cloud Map 時に が作成したホストゾーンを削除するには、namespace を削除します。 はホストゾーンを自動的に AWS Cloud Map 削除します。詳細については、AWS Cloud Map デベロッパーガイドの名前空間の削除を参照してください。

- Amazon Elastic Container Service (Amazon ECS) Service Discovery – Service Discovery を使用してサービスを作成した際に、Amazon ECS が作成したプライベートホストゾーンを削除するには、名前空間を使用する Amazon ECS サービスを削除した上で、その名前空間を削除します。詳細については、Amazon Elastic Container Service デベロッパーガイドの「サービスの削除」を参照してください。

Route 53 コンソールを使用してプライベートホストゾーンを削除する

Route 53 コンソールを使用してプライベートホストゾーンを削除するには、以下の手順を実行します。

Route 53 コンソールを使用してプライベートホストゾーンを削除するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. 削除するホストゾーンに NS と SOA のレコードのみが含まれていることを確認します。追加レコードが含まれている場合、それを削除します。

   a. 削除するホストゾーンの名前を選択します。

   b. [Record (レコード)] ページで、レコードのリストに [Type (タイプ)] 列の値が [NS] または [SOA] 以外に設定されたレコードが含まれている場合、その行を選択して、[Delete (削除)] を選択します。

      複数の連続するレコードを選択するには、最初の行を選択し、[Shift] (シフト) キーを押したまま最後の行を選択します。複数の連続していないレコードを選択するには、最初の行を選択し、Ctrl キーを押したまま、残りの行を選択します。
3. [Hosted Zones (ホストゾーン)] ページで、削除するホストゾーンの行を選択します。
4. [削除] を選択します。
5. 確認キーを入力し、[Delete (削除)] を選択します。

VPC アクセス許可

VPC アクセス許可は Identity and Access management (IAM) ポリシー条件を使用して、AssociateVPCWithHostedZone、DisassociateVPCFromHostedZone、CreateVPCAssociationAuthorizat の API を使用する際に VPC の細かいアクセス許可を設定できます。

IAM ポリシー条件 を使用するとroute53:VPCs、他のユーザーにきめ細かな管理権限を付与できます AWS 。これにより、ホストゾーンに関連付ける、ホストゾーンの関連付けを解除する、VPC 関連付け認可を作成する、VPC 関連付け認可を削除する、ホストゾーンを作成する、または次のホストゾーンを一覧表示するアクセス許可をユーザーに付与できます。

- 単一の VPC。
- 同じリージョン内のすべての VPC。
- 複数の VPC。

VPC アクセス許可の詳細については、「詳細に設定されたアクセスコントロールのための IAM ポリシー条件の使用」を参照してください。

AWS ユーザーを認証する方法については、アイデンティティを使用した認証「」および「」を参照してください。Route 53 リソースへのアクセスを制御する方法については、「」を参照してくださいアクセスコントロール。

ホストゾーンを別の AWS アカウントに移行する

ホストゾーンを別のホストゾーンに移行する場合は AWS アカウント、以下の推奨ステップに従います。

これらのステップは、レコードの変更頻度が低いホストゾーンに最適です。頻繁にレコードが更新されるホストゾーンの場合は、次の点を考慮してください。

- 移行中にリソースレコードを更新しないでください。
- 委任が移管された後、古いホストゾーンと新しいホストゾーンの両方でリソースレコードの変更を公開します。

前提条件

AWS CLI をインストールまたはアップグレードする:

のダウンロード、インストール、設定の詳細については AWS CLI、 AWS Command Line Interface ユーザーガイドを参照してください。

> **Note**
>
> CLI を設定し、ホストゾーンを作成したアカウントと、ホストゾーンの移行先アカウントの両方を使用中に CLI を使用できるようにします。詳細については、AWS Command Line Interface ユーザーガイドの設定を参照してください。

を既に使用している場合は AWS CLI、CLI コマンドが最新の Route 53 機能をサポートするように、最新バージョンの CLI にアップグレードすることをお勧めします。

トピック

- ステップ 1: 移行の準備をする
- ステップ 2: 新しいホストゾーンを作成する
- ステップ 3: (オプション) ヘルスチェックを移行する
- ステップ 4: 古いホストゾーンから新しいホストゾーンにレコードを移行する
- ステップ 5: 古いホストゾーンと新しいホストゾーンのレコードを比較する
- ステップ 6: ドメイン登録を更新して新しいホストゾーンのネームサーバーを使用する
- ステップ 7: NS レコードの TTL をより高い値に戻す
- ステップ 8: DNSSEC 署名を再度有効にし、信頼チェーンを確立する (必要な場合)
- ステップ 9: (オプション) 古いホストゾーンを削除する

ステップ 1: 移行の準備をする

準備ステップは、ホストゾーンの移行に関連するリスクを最小限に抑える上で役立ちます。

1. ゾーンの可用性を監視する

ドメイン名の可用性をゾーンで監視できます。これにより、移行のロールバックにつながる可能性のある問題に対処できます。CloudWatch またはクエリログを使用してトラフィックが最も多いドメイン名を監視できます。クエリログのセットアップの詳細については、「Amazon Route 53 のモニタリング」を参照してください。

監視はシェルスクリプトまたはサードパーティサービスを通じて実行できます。ただし、ドメインが利用できないために顧客からフィードバックを得る可能性もあるため、ロールバックが必要かどうかを判断する唯一のシグナルではありません。

2. TTL 設定を下げる

レコードの TTL (有効期限) 設定は、DNS リゾルバーがレコードをキャッシュし、キャッシュされた情報を使用する期間を指定します。TTL が期限切れになると、リゾルバーはドメインの DNS サービスプロバイダに別のクエリを送信し、最新の情報を取得します。

NS レコードの一般的な TTL 設定は 172800 秒、つまり 2 日です。NS レコードには、ドメインネームシステム (DNS) がドメインのトラフィックをルーティングする方法に関する情報を得るために使用できるネームサーバーがリストされています。現在の DNS サービスプロバイダーと Route 53 の両方で NS レコードの TTL を下げることで、DNS を Route 53 に移行している際に問題が検出された場合のドメインのダウンタイムを短縮できます。TTL を下げないと、何か問題が発生した場合、ドメインはインターネット上で最大 2 日間使用できなくなる可能性があります。

TTL を下げるには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [Hosted Zones] (ホストゾーン) を選択します。
3. ホストゾーンの名前を選択します。
4. NS レコードを選択し、[Record details] (レコードの詳細) ペインで [Edit record] (レコードの編集) を選択します。
5. [TTL (Seconds)] の値を変更します。60 秒から 900 秒 (15 分) の間の値を指定することをお勧めします。
6. [保存] を選択します。

3. (DNSSEC を構成している場合) 親ゾーンから DS レコードを削除する

ドメインで DNSSEC を設定している場合は、ドメインを Route 53 に移行する前に、親ゾーンから Delegation Signer (DS) レコードを削除します。

親ゾーンが Route 53 を介してホストされている場合、詳細については「ドメインのパブリックキーの削除」を参照してください。別のレジストラが親ゾーンをホストしている場合は、それらのホストに対し DS レコードの削除を依頼します。

Route 53 は現在、DNSSEC 設定の移行をサポートしていません。そのため、親ゾーンから DS レコードを削除して、移行前にドメインに対して実行された DNSSEC 検証を無効にする必要があります。移行後、新しいホストゾーンで DNSSEC を設定し、それぞれの DS レコードを親ゾーンに追加することで、DNSSEC 検証を再度有効化できます。

4. 移行ホストゾーンに依存する他の進行中のオペレーションがないことを確認します。

一部のオペレーションは、移行ホストゾーンの DNS 解決に依存します。例えば、TLS/SSL 証明書の更新プロセスでは DNS レコードの変更が必要になる場合があり、プロバイダーは検証方法として DNS レコードの解決を試みます。移行前に、ホストゾーンの移行による予期しない影響を避けるために、他のオペレーションが行われていないことを確認する必要があります。

ステップ 2: 新しいホストゾーンを作成する

ホストゾーンを移行するアカウントに新しいホストゾーンを作成します。

AWS CLI または コンソールの手順のタブを選択します。

- CLI
- コンソール

CLI

次のコマンドを入力します。

```
aws route53 create-hosted-zone \
            --name $hosted_zone_name \
            --caller-reference $unique_string
```

詳細については、「create-hosted-zone」を参照してください。

Console

別のアカウントを使用して新しいホストゾーンを作成するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。

   ホストゾーンの移行先となるアカウントのアカウント認証情報を使用してサインインします。
2. ホストゾーンの作成。詳細については、「パブリックホストゾーンの作成」を参照してください。
3. ホストゾーン ID を書き留めます。この情報は、プロセス中に後で必要になる場合があります。
4. Route 53 コンソールからログアウトします。

「準備ステップ 1 の TTL 設定を下げる」の「TTL 設定を下げる」と同様、新しいゾーンの NS TTL も下げます。

ステップ 3: (オプション) ヘルスチェックを移行する

新しいアカウントの DNS レコードを、移行元のアカウントの Route 53 ヘルスチェックに関連付けることができます。Route 53 ヘルスチェックを移行するには、既存のヘルスチェックと同じ設定で新しいアカウントに新しいヘルスチェックを作成する必要があります。詳細については、「Amazon Route 53 ヘルスチェックの作成」を参照してください。

ステップ 4: 古いホストゾーンから新しいホストゾーンにレコードを移行する

コンソールまたは を使用して、 から別の AWS アカウント にレコードを移行できます AWS CLI。

Console

ゾーンに少数のレコードしか含まれていない場合は、Route 53 コンソールを使用して古いゾーンのレコードを一覧表示し、メモして、新しいゾーンに作成することを検討できます。ステップ 3: (オプション) ヘルスチェックを移行する でヘルスチェックを移行した場合は、新しいホストゾーンにレコードを作成するときに、新しいヘルスチェック ID を指定する必要があります。詳細については、以下の各トピックを参照してください。

- レコードの一覧表示
- Amazon Route 53 コンソールを使用したレコードの作成
- DNS フェイルオーバーの設定

「ステップ 1 の TTL を下げる設定」と同様に、新しいゾーンでも NS TTL を下げる必要があります。

CLI

ゾーンに多数のレコードが含まれている場合は、移行するレコードをエクスポートしてファイルにし、そのファイルを編集し、編集したファイルを使用して新しいホストゾーンにレコードを作成します。以下の手順では AWS CLI コマンドを使用しますが、この目的ではサードパーティー製ツールも使用できます。

1. 次のコマンドを実行します。

```
aws route53 list-resource-record-sets --hosted-zone-id hosted-zone-id > path-to-output-file
```

次の点に注意してください。

- *hosted-zone-id* には、移行するレコードを含む古いホストゾーンの ID を指定します。
- *path-to-output-file* に、出力を保存するディレクトリのパスとファイル名を指定します。
- > 文字を指定すると、指定されたファイルに出力が送信されます。
- は、100 を超えるレコードを含むホストゾーンのページ分割 AWS CLI を自動的に処理します。詳細については、「 AWS Command Line Interface ユーザーガイド」の AWS 「コマンドラインインターフェイスのページ分割オプションの使用」を参照してください。

  別のプログラムメソッドを使用して AWS SDKs の 1 つなどのレコードを一覧表示する場合、結果のページあたり最大 100 個のレコードを取得できます。100 個を超えるレコードがホストゾーンに含まれている場合は、すべてのレコードをリストするために複数のリクエストを送信する必要があります。

この出力のコピーを作成します。新しいホストゾーンでレコードを作成したら、新しいホストゾーンで コマンドを実行し AWS CLI `list-resource-record-sets`、2 つの出力を比較して、すべてのレコードが作成されていることを確認することをお勧めします。

2. 移行するレコードを編集する

`change-resource-record-sets` コマンドで使用する前に、エクスポートしたファイルを編集します。テキストエディターの検索と置き換え機能を使用して、これらの変更を行うことができます。

> **Note**
>
> 次の手順では、テキストエディターを使用した手動編集について説明します。上級ユーザーは、jq、Python、またはその他のスクリプト言語などのプログラムツールを使用して、これらの変換を自動化できます。

移行するレコードを含むこの手順のステップ 1 で作成したファイルのコピーを開き、次の変更を行います。

- ファイルの上部にある ResourceRecordSets 要素を Changes 要素に置き換えます。
- オプション – Comment 要素を追加します。
- ホストゾーン名の NS レコードと SOA レコードに関連する行を削除します。新しいホストゾーンには既にそれらのレコードがあります。
- レコードごとに、Action と ResourceRecordSets 要素を追加し、必要に応じて括弧 ({ }) を追加して JSON コードを有効にします。

> **Note**
>
> JSON 検証ツールを使用して、すべての中括弧と角括弧が正しい場所に配置されていることを確認します。オンライン JSON 検証ツールを検索するには、ブラウザで「JSON 検証ツール」を検索します。

- ホストゾーンに、同じホストゾーンで他のレコードを参照するエイリアスが含まれている場合は、以下の変更を行います。
  - ホストゾーン ID を、新しいホストゾーンの ID に変更します。

> **Important**
>
> エイリアスレコードが他のリソース (ロードバランサーなど) を指している場合は、ホストゾーン ID を、ドメインのホストゾーン ID に変更しないでください。ホストゾーン ID を誤って変更した場合は、ホストゾーン ID をドメインのホストゾーン ID ではなく、リソース自体のホストゾーン ID にロールバックしてください。リソースホストゾーン ID は、リソースが作成された AWS コンソールにあります。

  - エイリアスレコードをファイルの末尾に移動します。Route 53 は、エイリアスレコードを作成する前に、エイリアスレコードが参照するレコードを作成する必要があります。

> **Important**
>
> 1 つ以上のエイリアスレコードが他のエイリアスレコードを参照している場合、エイリアスターゲットであるレコードは、エイリアスレコードを参照する前にファイルに表示される必要があります。たとえば、alias.example.com が alias.alias.example.com のエイリアスターゲットである場合、alias.example.com がファイルの先頭に表示される必要があります。

- トラフィックをトラフィックポリシーインスタンスにルーティングするエイリアスレコードを削除します。レコードをメモし、後で再作成できるようにします。
- ステップ 3: (オプション) ヘルスチェックを移行する でヘルスチェックを移行した場合は、新しく作成されたヘルスチェック ID に関連付けるようにレコードを変更します。

次の例に示すのは、example.com のホストゾーンのレコードの編集されたバージョンです。赤の斜体で示されているテキストが新しい部分です。

```
{
    "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."
            }
```

```
        }
    ]
}
```

3. 大きなファイルを小さなファイルに分割する

   レコードが多数ある場合や、多くの値 (多数の IP アドレスなど) を含むレコードがある場合は、ファイルをより小さなファイルに分割しなければならないことがあります。最大値は以下のとおりです。

   - 各ファイルには、最大 1,000 件のレコードを含めることができます。
   - すべての Value 要素での結合された値の最大の長さは 32,000 バイトです。

4. 新しいホストゾーンにレコードを作成する

   次の CLI を入力します。

   ```
   aws route53 change-resource-record-sets \
               --hosted-zone-id new-hosted-zone-id \
               --change-batch file://path-to-file-that-contains-records
   ```

   次の値を指定します。

   - *new-hosted-zone-id* で、新しいホストゾーンの ID を指定します。
   - *path-to-file-that-contains-records* で、前のステップで編集したディレクトリのパスとファイル名を指定します。

   トラフィックポリシーインスタンスにトラフィックをルーティングするエイリアスレコードを削除している場合は、Route 53 コンソールを使用して、それらを再作成します。詳細については、「Amazon Route 53 コンソールを使用したレコードの作成」を参照してください。

ステップ 5: 古いホストゾーンと新しいホストゾーンのレコードを比較する

新しいホストゾーンですべてのレコードを正常に作成したことを確認するには、以下の CLI コマンドを入力して新しいホストゾーンのレコードをリストし、その出力を、古いホストゾーンからのレコードのリストと比較することをお勧めします。

```
aws route53 list-resource-record-sets \
            --hosted-zone-id new-hosted-zone-id \
```

```
            --output json > path-to-output-file
```

次の値を指定します。

- *new-hosted-zone-id* で、新しいホストゾーンの ID を指定します。
- *path-to-output-file* で、出力を保存するディレクトリのパスとファイル名を指定します。ステップ 4 で使用したファイル名とは異なるファイル名を使用します。

  > 文字を指定すると、指定されたファイルに出力が送信されます。

出力をステップ 4 の出力と比較します。NS レコードと SOA レコードの値、およびステップ 4 で行った変更 (異なるホストゾーン ID やドメイン名など) を除いて、2 つの出力は同じになるはずです。

新しいホストゾーンのレコードが古いホストゾーンのレコードに一致しない場合は、次のいずれかの操作を実行します。

- Route 53 コンソールを使用してマイナーな修正を行います。詳細については、「レコードの編集」を参照してください。
- 新しいホストゾーンで NS レコードと SOA レコードを除くすべてのレコードを削除し、ステップ 4 の手順を繰り返します。

ステップ 6: ドメイン登録を更新して新しいホストゾーンのネームサーバーを使用する

新しいホストゾーンでレコードの移行が終了したら、ドメイン登録のネームサーバーを変更し、新しいホストゾーンのネームサーバーを使用します。詳細については、「Amazon Route 53 を既存ドメインの DNS サービスにする」を参照してください。

ホストゾーンが使用中の場合、例えばユーザーがドメイン名を使用してウェブサイトを参照したり、ウェブアプリケーションにアクセスしたりしている場合、ウェブサイトやアプリケーションのトラフィック、E メールなど、ホストゾーンのトラフィックと可用性を引き続きモニタリングする必要があります。

- トラフィックが遅くなったり停止したりした場合 — ドメイン登録のネームサービスを古いホストゾーンの以前のネームサーバーに戻します。その後、何が悪かったのかを見極めます。
- トラフィックに影響がない場合 – 次のステップに進みます。

ステップ 7: NS レコードの TTL をより高い値に戻す

新しいホストゾーンで、NS レコードの TTL をより一般的な値、例えば 172800 秒 (2 日) に変更します。これにより、DNS リゾルバーがドメインのネームサーバーのクエリを送信するのを頻繁に待つ必要がないため、ユーザーのレイテンシーが改善されます。

TTL を変更するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [Hosted Zones] (ホストゾーン) を選択します。
3. ホストゾーンの名前を選択します。
4. NS レコードを選択し、[Record details] (レコードの詳細) ペインで [Edit record] (レコードの編集) を選択します。
5. [TTL (Seconds)] の値を、DNS リゾルバーがドメインのネームサーバーの名前をキャッシュする秒数に変更します。172800 秒の値を推奨します。
6. [保存] を選択します。

ステップ 8: DNSSEC 署名を再度有効にし、信頼チェーンを確立する (必要な場合)

2 つのステップで DNSSEC 署名を再度有効にできます。

1. Route 53 の DNSSEC 署名を有効にし、 AWS Key Management Serviceのカスタマー管理キーに基づいたキー署名キー (KSK) を Route 53 が作成するようにリクエストします。
2. Delegation Signer (DS) レコードを親ゾーンに追加して、ホストゾーンの信頼チェーンを作成します。これにより、信頼された暗号化署名を使用して DNS 応答を認証できます。

手順については、「DNSSEC 署名を有効にし、信頼チェーンを確立します。」を参照してください。

ステップ 9: (オプション) 古いホストゾーンを削除する

古いホストゾーンが不要であることが明らかな場合は、オプションで削除できます。手順については、「パブリックホストゾーンの削除」を参照してください。

> **Important**
>
> 新しいホストゾーンのネームサーバーを使用するようにドメイン登録を更新してから少なくとも 48 時間は、古いホストゾーンもこのホストゾーン内のレコードも削除しないでください。DNS リゾルバーがそのホストゾーンのレコードの使用を停止する前に古いホストゾーンを削除した場合、リゾルバーで新しいホストゾーンの使用を開始するまでドメインはインターネットで利用できないおそれがあります。

レコードを使用する

ドメイン (例えば、example.com) のホストゾーンを作成した後、そのドメインへのトラフィックをルーティングする方法をドメインネームシステム (DNS) に指定するレコードを作成します。

例えば、DNS が以下のように動作するレコードを作成することができます。

- example.com のインターネットトラフィックをデータセンター内のホストの IP アドレスにルーティングします。
- そのドメイン宛のメール (ichiro@example.com) をメールサーバー (mail.example.com) にルーティングします。
- operations.tokyo.example.com というサブドメインのトラフィックを異なるホストの IP アドレスにルーティングします。

各レコードには、ドメインまたはサブドメインの名前、レコードタイプ (MX が E メールをルーティングするタイプのレコードなど) 、そのレコードタイプのその他の情報 (MX レコードの場合、1 つ以上のメールサーバーのホスト名、各サーバーの優先度) が含まれます。各種レコードについては、「サポートされる DNS レコードタイプ」を参照してください。

ホストゾーン内の各レコードの名前は、ホストゾーンの名前で終わる要があります。例えば、example.com ホストゾーンには、サブドメイン www.example.com と accounting.tokyo.example.com のレコードを含めることができますが、サブドメイン www.example.ca のレコードを含めることはできません。

> **Note**
>
> 複雑なルーティング設定のレコードを作成するには、トラフィックフロービジュアルエディタを使用して設定をトラフィックポリシーとして保存することもできます。その後、トラ

フィックポリシーを同じホストゾーンまたは複数のホストゾーンの 1 つ以上のドメイン名 (example.com など) またはサブドメイン名 (www.example.com など) にリンクできます。新しいセットアップが期待どおりに機能しない場合は、更新をロールバックすることもできます。詳細については、「DNS トラフィックのルーティングにトラフィックフローを使用する」を参照してください。

Amazon Route 53 では、ホストゾーンに追加したレコードには課金されません。ホストゾーンで作成できるレコードの最大数については、「クォータ」を参照してください。

トピック

- ルーティングポリシーの選択
- エイリアスレコードと非エイリアスレコードの選択
- サポートされる DNS レコードタイプ
- Amazon Route 53 コンソールを使用したレコードの作成
- リソースレコードセットのアクセス許可
- Amazon Route 53 レコードの作成時または編集時に指定する値
- ゾーンファイルをインポートしてレコードを作成する
- レコードの編集
- レコードの削除
- レコードの一覧表示

ルーティングポリシーの選択

レコードを作成するときは、Amazon Route 53 がクエリに応答する方法を決定するルーティングポリシーを選択します。

- シンプルルーティングポリシー – ドメインで特定の機能を実行する単一のリソースがある場合に使用します。例えば、example.com ウェブサイトにコンテンツを提供する 1 つのウェブサーバーなどです。シンプルルーティングは、プライベートホストゾーンにレコードを作成するために使用できます。
- フェイルオーバールーティングポリシー – アクティブ/パッシブフェイルオーバーを構成する場合に使用します。フェイルオーバールーティングは、プライベートホストゾーンにレコードを作成するために使用できます。

- 位置情報ルーティングポリシー – ユーザーの位置に基づいてトラフィックをルーティングする場合に使用します。位置情報ルーティングは、プライベートホストゾーンにレコードを作成するために使用できます。
- 地理的近接性ルーティングポリシー – リソースの場所に基づいてトラフィックをルーティングし、必要に応じてトラフィックをある場所のリソースから別の場所のリソースに移動する場合に使用します。地理的近接性ルーティングは、プライベートホストゾーンにレコードを作成するために使用できます。
- レイテンシールーティングポリシー – 複数の にリソースがあり AWS リージョン 、レイテンシーが最も高いリージョンにトラフィックをルーティングする場合に使用します。レイテンシールーティングは、プライベートホストゾーンにレコードを作成するために使用できます。
- IP ベースのルーティングポリシー – トラフィックの送信元の IP アドレスがわかっており、ユーザーの位置に基づいてトラフィックをルーティングする際に使用します。
- 複数値回答ルーティングポリシー – ランダムに選ばれた最大 8 つの正常なレコードを使用して Route 53 が DNS クエリに応答する場合に使用します。複数値回答ルーティングは、プライベートホストゾーンにレコードを作成するために使用できます。
- 加重ルーティングポリシー– 指定した比率で複数のリソースにトラフィックをルーティングする場合に使用します。加重ルーティングポリシーは、プライベートホストゾーンにレコードを作成するために使用できます。

トピック

- シンプルルーティング
- フェイルオーバールーティング
- 位置情報ルーティング
- 地理的近接性ルーティング
- レイテンシーに基づくルーティング
- IP ベースルーティング
- 複数値回答ルーティング
- 加重ルーティング
- Amazon Route 53 が EDNS0 を使用してユーザーの場所を推定する方法

シンプルルーティング

シンプルなルーティングでは、加重やレイテンシーなどの特別な Route 53 ルーティングなしで、標準 DNS レコードを設定できます。通常、トラフィックを 1 つのリソースにルーティングします。たとえば、ウェブサイトのウェブサーバーにルーティングします。

プライベートホストゾーンのレコードに、シンプルルーティングポリシーを使用できます。

Route 53 コンソールでシンプルなルーティングポリシーを選択した場合、同じ名前とタイプを持つ複数のレコードを作成することはできませんが、複数の IP アドレスなど、同じレコードに複数の値を指定できます。(エイリアスレコードのシンプルなルーティングポリシーを選択した場合は、現在のホストゾーンで 1 つの AWS リソースまたは 1 つのレコードのみを指定できます) 。レコードに複数の値を指定すると、Route 53 はすべての値をランダムな順序で再帰リゾルバーに返し、リゾルバーは DNS クエリを送信したクライアント (ウェブブラウザなど) に値を返します。次に、クライアントは値を選択し、クエリを再送信します。シンプルなルーティングでは、複数の IP アドレスを指定できますが、ヘルスチェックは行われません。

シンプルルーティングポリシーを使用してレコードを作成するときに指定する値の詳細については、以下のトピックを参照してください。

- シンプルなレコードに固有の値
- シンプルなエイリアスレコードに固有の値
- すべてのルーティングポリシーに共通する値
- すべてのルーティングポリシーのエイリアスレコードに共通する値

フェイルオーバールーティング

フェイルオーバールーティングを使用すると、トラフィックが正常であればリソースに、最初のリソースが異常であれば別のリソースにルーティングできます。プライマリレコードとセカンダリレコードは、ウェブサイトとしてセットアップされた Amazon S3 バケットから複雑なレコードツリーにトラフィックをルーティングできます。詳細については、「アクティブ/パッシブ (フェイルオーバー)。」を参照してください。

フェイルオーバールーティングポリシーは、プライベートホストゾーンのレコードに使用できます。

フェイルオーバールーティングポリシーを使用してレコードを作成するときに指定する値の詳細については、以下のトピックを参照してください。

- フェイルオーバーレコードに固有の値

- フェイルオーバーエイリアスレコードに固有の値
- すべてのルーティングポリシーに共通する値
- すべてのルーティングポリシーのエイリアスレコードに共通する値

位置情報ルーティング

位置情報ルーティングでは、ユーザーの所在地、つまり DNS クエリの送信元の場所に基づいて、トラフィックを処理するリソースを選択できます。例えば、ヨーロッパからのすべてのクエリをフランクフルトリージョンの Elastic Load Balancing ロードバランサーにルーティングしなければならない場合があります。

位置情報ルーティングを使用すると、ユーザーの言語でコンテンツを表示できます。位置情報ルーティングを使用して、ディストリビューション権限を持つロケーションのみにコンテンツを制限することもできます。もう 1 つの用途は、予測および管理しやすい方法でエンドポイント間で負荷を分散し、各ユーザーロケーションが常に同じエンドポイントに移動するようにすることです。

地理的場所は、大陸別、国別、米国の州別に指定できます。重なり合う地理的リージョンについて別々のレコードを作成した場合は (例えば、北米用のレコードが 1 つ、カナダ用のレコードが 1 つ)、最も小さい地理的リージョンが優先されます。これにより、大陸のクエリを 1 つのリソースにルーティングし、その大陸の一部の国のクエリを異なるリソースにルーティングすることができます (各大陸の国の一覧については、「ロケーション」を参照してください)。

位置情報は、IP アドレスを場所にマッピングすることで動作します。ただし、一部の IP アドレスは場所にマッピングされないため、7 つの大陸すべてをカバーする位置情報レコードを作成しても、Amazon Route 53 は識別できない場所からいくつかの DNS クエリを取得します。マッピングされていない IP アドレスからのクエリと、位置情報レコードを作成していない場所からのクエリの両方を処理するデフォルトのレコードを作成できます。デフォルトレコードを作成しない場合、Route 53 はそのような場所からのクエリに対して "応答なし" という応答を返します。

位置情報ルーティングは、パブリックホストゾーンとプライベートホストゾーンの両方のレコードに使用できます。

詳細については、「Amazon Route 53 が EDNS0 を使用してユーザーの場所を推定する方法」を参照してください。

位置情報ルーティングポリシーを使用してレコードを作成するときに指定する値の詳細については、以下のトピックを参照してください。

- 位置情報レコードに固有の値

- 位置情報エイリアスレコードに固有の値
- すべてのルーティングポリシーに共通する値
- すべてのルーティングポリシーのエイリアスレコードに共通する値

プライベートホストゾーンのジオロケーションルーティング

プライベートホストゾーンの場合、Route 53 はクエリの送信元の VPC AWS リージョン の に基づいて DNS クエリに応答します。のリストについては AWS リージョン、Amazon EC2 ユーザーガイド」の「リージョンとゾーン」を参照してください。

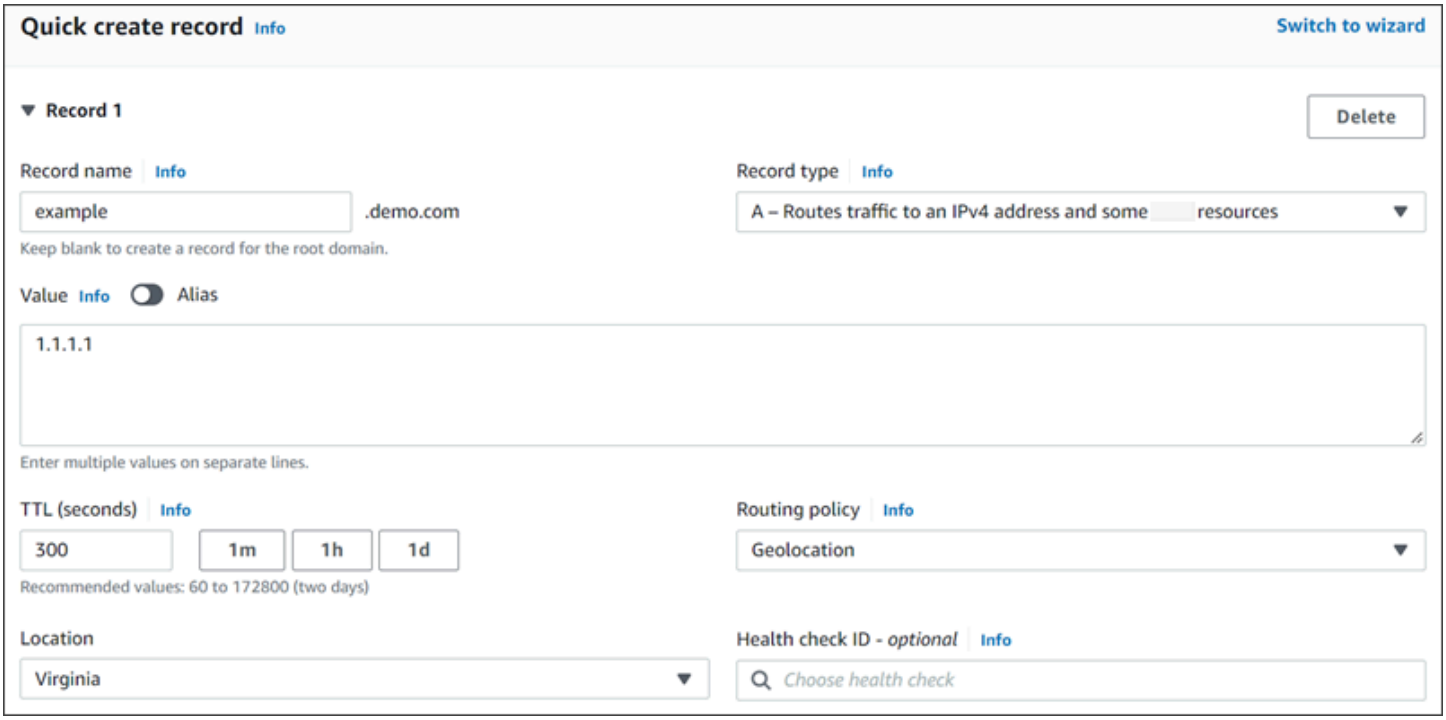
DNS クエリがハイブリッドネットワークのオンプレミス部分から発信された場合は、VPC が配置されている AWS リージョン から発信されたと見なされます。

ヘルスチェックを含めると、次のデフォルトレコードを作成できます。

- 地理的な場所にマップされていない IP アドレス。
- 位置情報レコードを作成していない場所からの DNS クエリ。

DNS クエリのリージョンの位置情報レコードが正常でない場合、デフォルトのレコードが返されます (正常である場合)。

次の図の設定例では、us-east-1 AWS リージョン (バージニア) からの DNS クエリは 1.1.1.1 エンドポイントにルーティングされます。



地理的近接性ルーティング

地理的近接性ルーティングでは、Amazon Route 53 はユーザーとリソースの場所に基づいてトラフィックをリソースにルーティングします。利用可能な最も近いリソースにトラフィックを送信します。バイアスと呼ばれる値を設定することで、特定のリソースへのトラフィックを増減することもできます。バイアスは、トラフィックがリソースに移動する地理的リージョンを拡大または縮小します。

リソースで地理的近接性ルールを作成し、各ルールに次の値のいずれかを指定します。

- AWS リソースを使用している場合は、リソースを作成した AWS リージョン または ローカルゾーングループを指定します。
- AWS リソース以外の を使用している場合は、リソースの緯度と経度を指定します。

AWS ローカルゾーンを使用するには、まずローカルゾーンを有効にする必要があります。詳細については、「AWS Local Zones ユーザーガイド」の「Getting started with Local Zones」を参照してください。

AWS リージョン とローカルゾーンの違いについては、Amazon EC2 ユーザーガイド」の「リージョンとゾーン」を参照してください。

Route 53 がリソースにルーティングするトラフィックの発信元の地理的リージョンのサイズを必要に応じて変更するには、バイアスに適切な値を指定します。

- Route 53 がリソースにルーティングするトラフィックの発信元の地理的リージョンのサイズを拡大するには、バイアスに 1 から 99 までの正の整数を指定します。Route 53 は隣接するリージョンのサイズを縮小します。
- Route 53 がリソースにルーティングするトラフィックの発信元の地理的リージョンのサイズを縮小するには、-1 から -99 までの負のバイアスを指定します。Route 53 は隣接するリージョンのサイズを拡大します。

> **Note**
>
> Route 53 はトラフィックフローコンソールを更新しています。旧コンソールは移行期間中も引き続きご使用いただけます。

お使いのコンソールのタブを選択します。

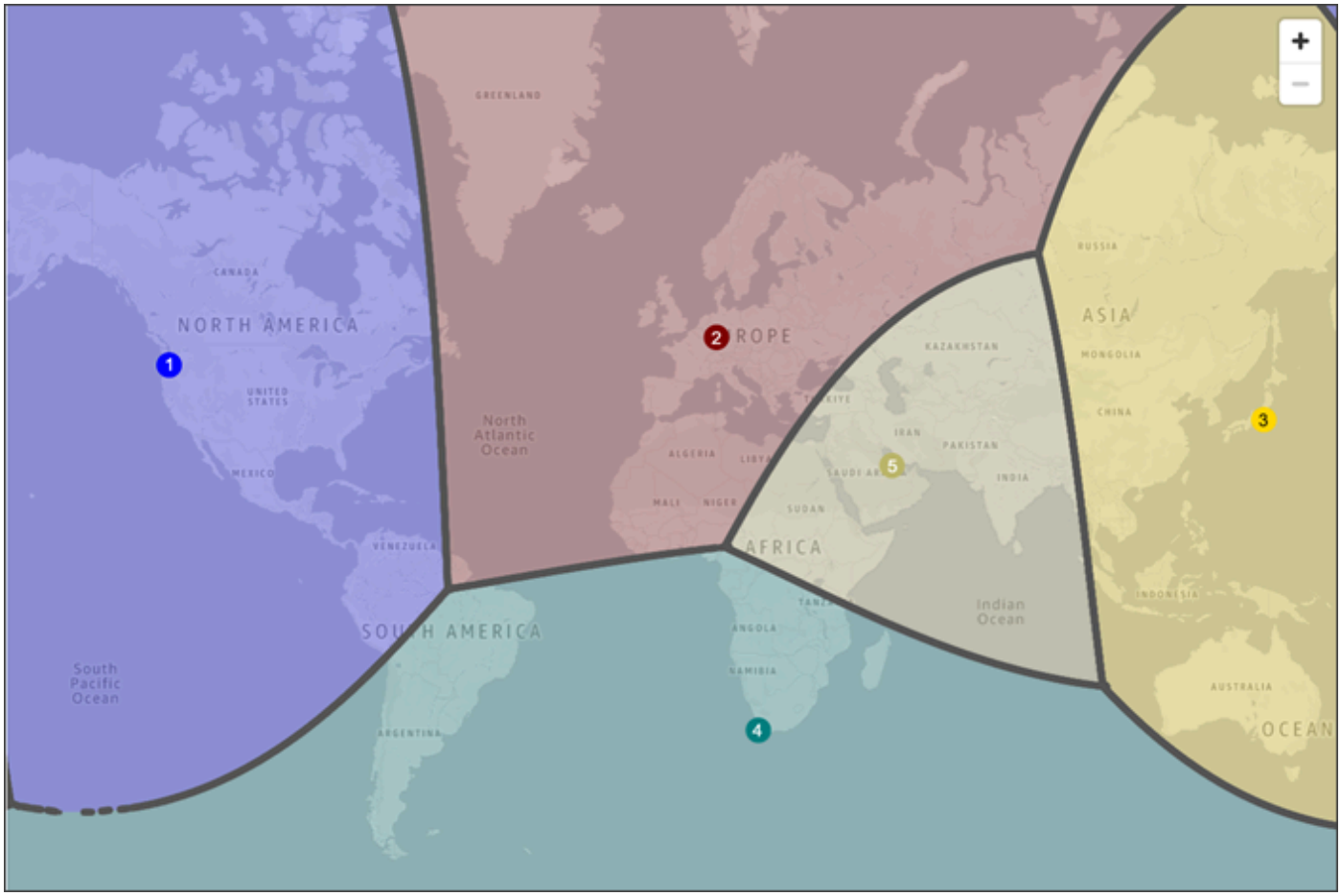
- 新しいコンソール
- 旧コンソール

New console

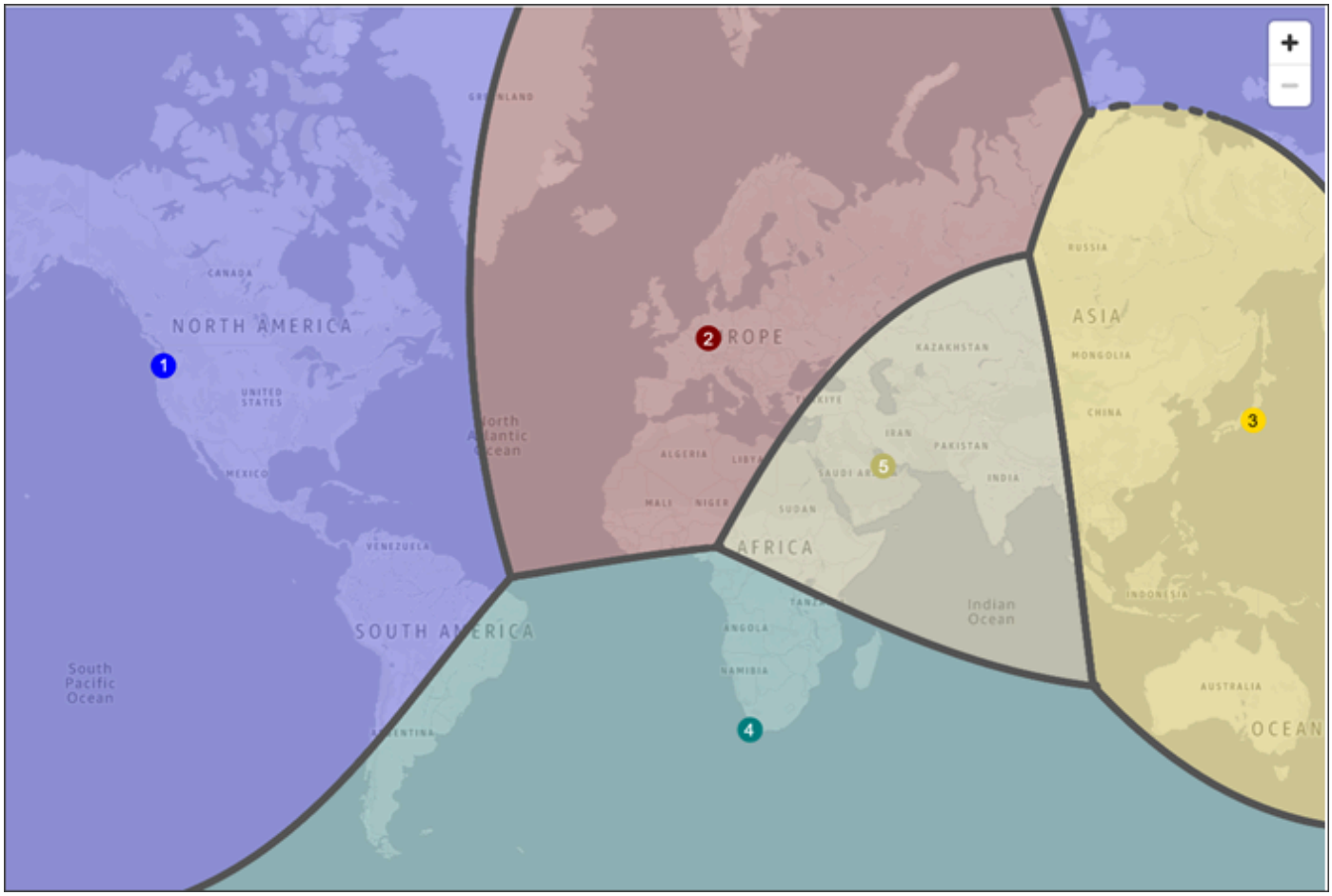
次のマップは、4 AWS リージョン (1 ~ 5 の番号) を示しています。

1. 米国西部 (オレゴン)
2. 欧州 (フランクフルト)
3. アジアパシフィック (東京)
4. アフリカ (ケープタウン)
5. 中東 (バーレーン)

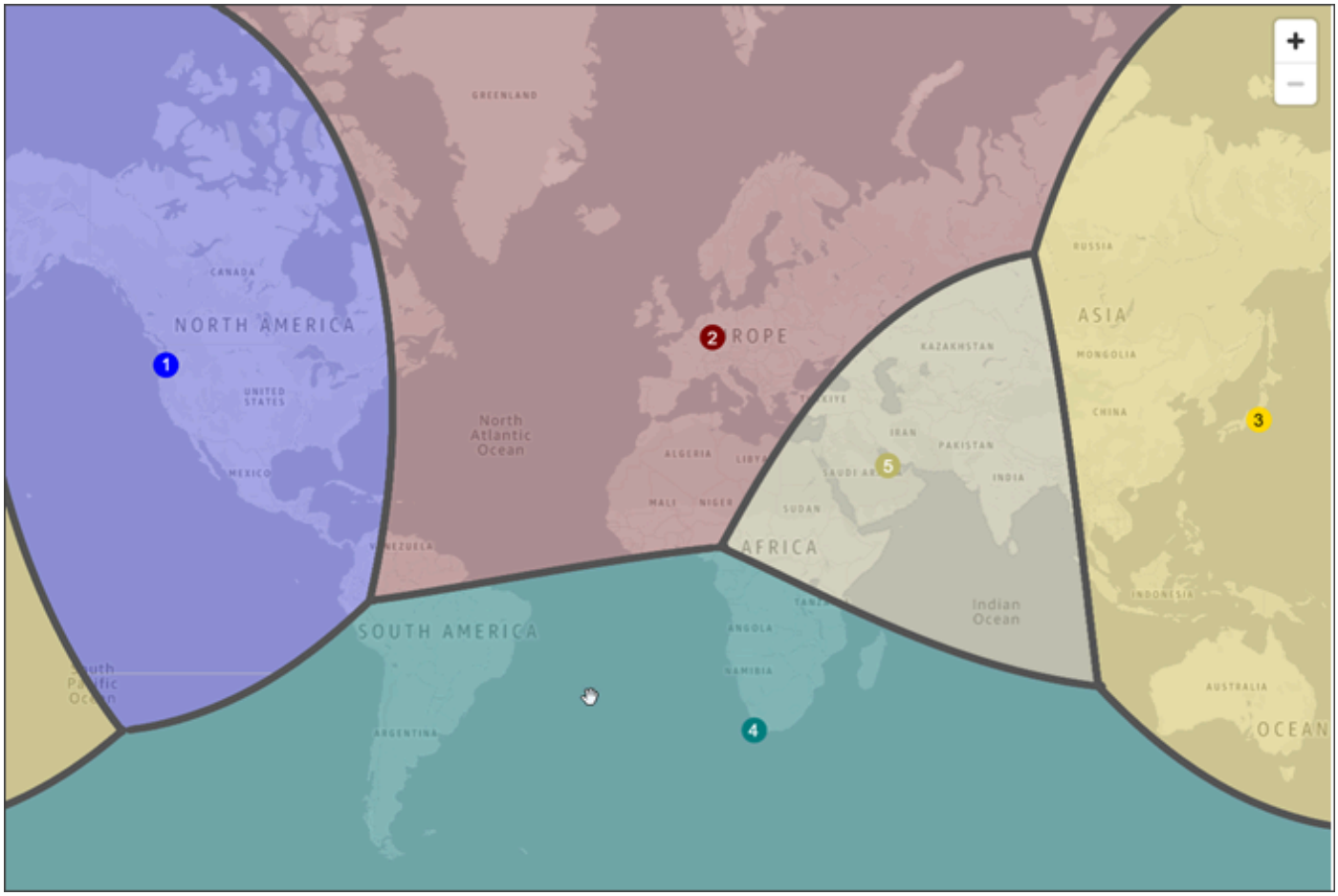
> **Note**
>
> マップは Traffic Flow でのみ使用できます。



次のマップでは、米国西部 (オレゴン) リージョン (マップ上の 1) に +25 のバイアスが追加されています。北米ではそれまでより広範囲から、さらに南米全域からもトラフィックがそのリージョンにルーティングされるようになっています。



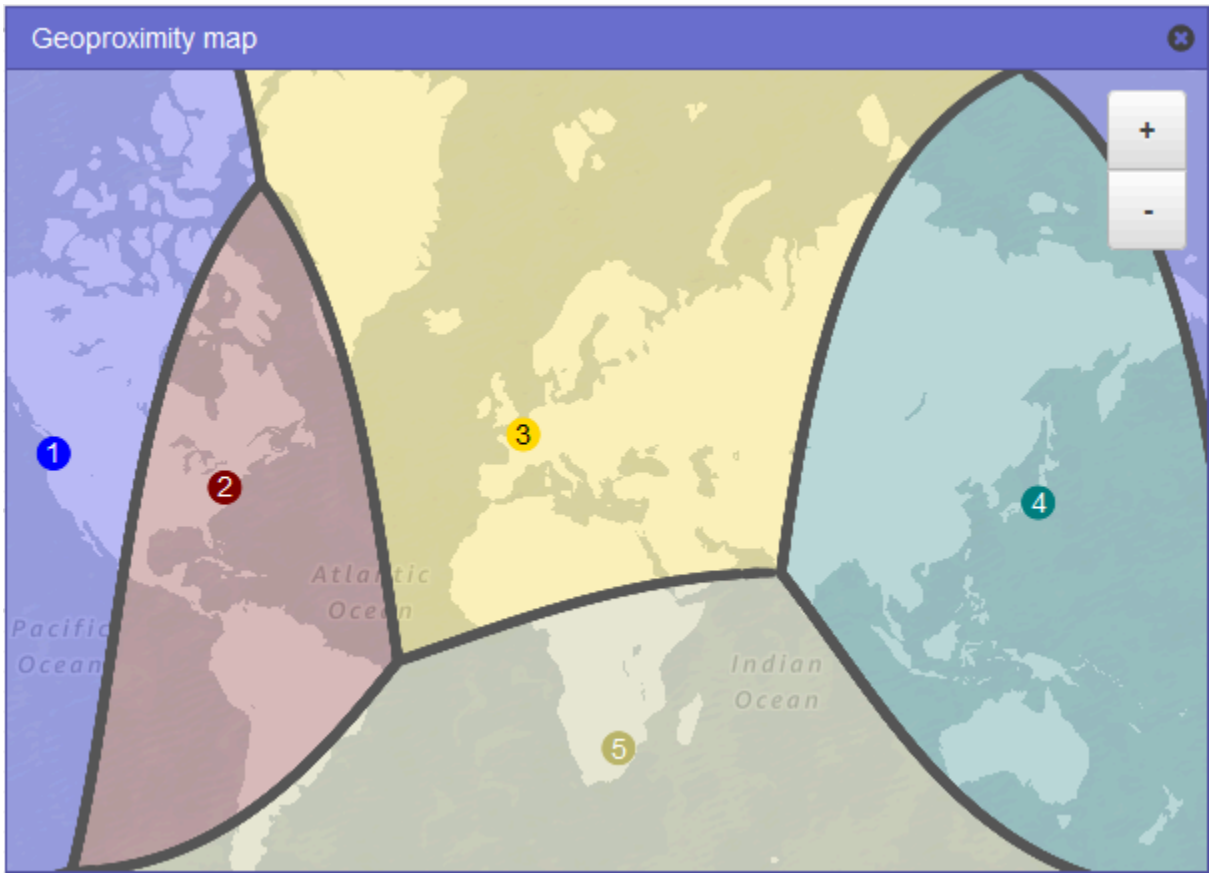
次のマップでは、米国西部 (オレゴン) リージョンのバイアスが -25 に変更されています。トラフィックは、以前よりも北米と南米の小さな部分からそのリージョンのリソースにルーティングされ、隣接するリージョン 2、3、および 4 のリソースにルーティングされるトラフィックが増えます。



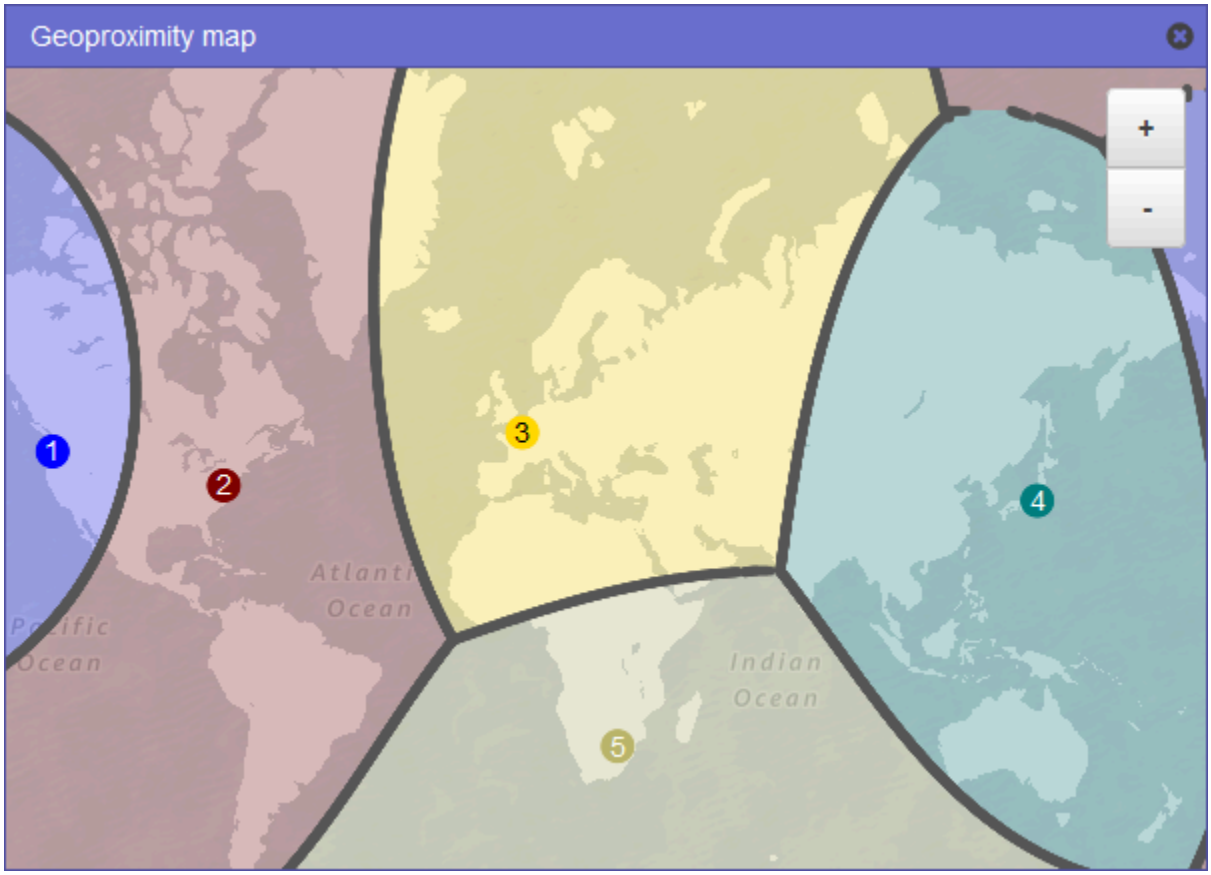
Old console

次のマップは、緯度と経度 AWS リージョン (5) で指定された 4 つの (1 ~ 4 の番号) と、南アフリカのヨハネスブルグの場所を示しています。

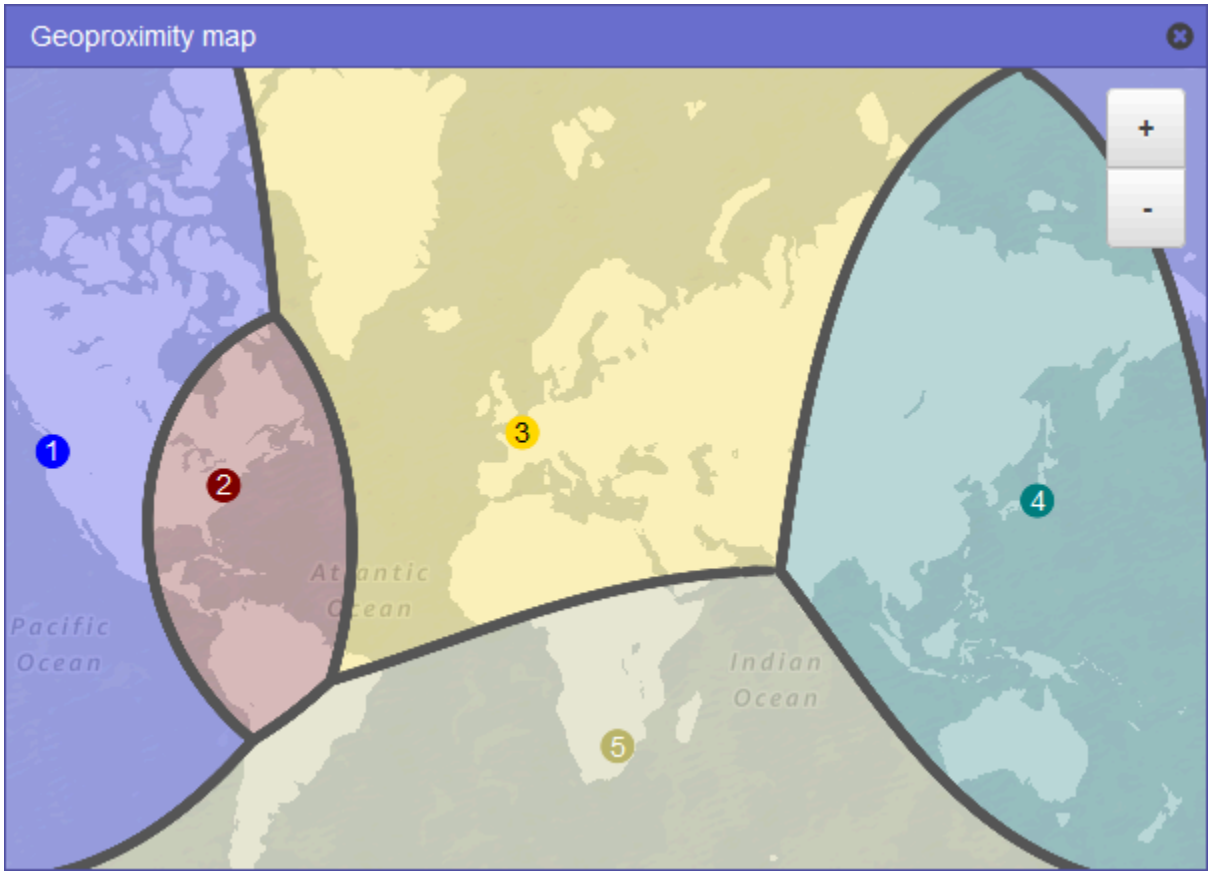
> **Note**
>
> マップは Traffic Flow でのみ使用できます。



次のマップでは、米国東部 (バージニア北部) リージョン (マップ上の 2) に +25 のバイアスが追加されています。北米ではそれまでより広範囲から、さらに南米全域からもトラフィックがそのリージョンにルーティングされるようになっています。



次のマップでは、米国東部 (バージニア北部) リージョンのバイアスが -25 に変更されています。北米および南米では、より狭い範囲からのトラフィックがそのリージョンのリソースにルーティングされ、隣接するリージョン (1、3、5) のリソースにルーティングされるトラフィックが増えています。



リソースのバイアスを変更する効果は、次のようないくつかの要因によって異なります。

- 所有するリソース数。
- リソースが互いにどの程度近いか。
- 地理的リージョン間の境界に近いユーザーの数。たとえば、 AWS リージョン 米国東部 (バージニア北部) と米国西部 (オレゴン) にリソースがあり、米国テキサス州ダラス、オースティン、サンアントニオに多くのユーザーがいるとします。これらの都市は両方のリソースからほぼ同じ距離にあるため、バイアスの小さな変化により、トラフィックが多くなる可能性があります AWS リージョン 。

トラフィックの突然のシフトによるリソースの負担を避けるため、バイアスを小さなステップで変更することをお勧めします。

詳細については、「Amazon Route 53 が EDNS0 を使用してユーザーの場所を推定する方法」を参照してください。

Amazon Route 53 がバイアスを使用してトラフィックをルーティングする方法

以下は、Amazon Route 53 がトラフィックをルーティングする方法を決定するのに使用する式です。

Bias (バイアス)

```
Biased distance = actual distance * [1 - (bias/100)]
```

バイアスの値が正の場合、Route 53 は DNS クエリのソースと地理的近接性レコードのリソース (の EC2 インスタンスなど AWS リージョン) を、実際よりも近くにあるものとして扱います。たとえば、次の地理的近接性レコードがあるとします。

- ウェブサーバー A のレコード、正のバイアスは 50
- ウェブサーバー B のレコード、バイアスなし

地理的近接性のレコードで正のバイアスが 50 ある場合、Route 53 はクエリのソースとそのレコードのリソース間の距離を半分にします。次に、Route 53 はクエリのソースに近いリソースを特定します。ウェブサーバー A がクエリのソースから 150 km で、ウェブサーバー B がクエリのソースから 100 km であるとします。どちらのレコードにもバイアスがない場合、Route 53 はクエリをより近くにあるウェブサーバー B にルーティングします。ただし、ウェブサーバー A のレコードの正のバイアスは 50 であるため、Route 53 はウェブサーバー A をクエリのソースから 75 km 離れているかのように扱います。その結果、Route 53 はクエリをウェブサーバー A にルーティングします。

以下に、正のバイアス 50 の計算を示します。

```
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
```

レイテンシーに基づくルーティング

アプリケーションが複数の でホストされている場合 AWS リージョン、レイテンシーを最小限に抑えて からのリクエストを処理することで AWS リージョン 、ユーザーのパフォーマンスを向上させることができます。

> **Note**
>
> ユーザーとリソース間のレイテンシーに関するデータは、ユーザーと AWS データセンター間のトラフィックに完全に基づいています。でリソースを使用していない場合 AWS リージョン、ユーザーとリソース間の実際のレイテンシーはレイテンシ AWS ーデータと大きく異なる場合があります。これは、リソースが AWS リージョンと同じ都市にある場合でも当てはまります。

レイテンシーベースルーティングを使用するには、複数の AWS リージョンのリソース用にレイテンシーレコードを作成します。Route 53 がドメインまたはサブドメイン (example.com または acme.example.com) の DNS クエリを取得すると、作成した AWS リージョン レイテンシーレコードをチェックし、ユーザーにレイテンシーが最も低いリージョンを見つけ、そのリージョンのレイテンシーレコードを選択します。Route 53 は、ウェブサーバーの IP アドレスなど、選択したレコードの値で応答します。

例えば、米国西部 (オレゴン) リージョンとアジアパシフィック (シンガポール) リージョンに Elastic Load Balancing ロードバランサーがあるとします。各ロードバランサーのレイテンシーレコードを作成します。ロンドンのユーザーがブラウザにあなたのドメイン名を入力した場合は次のようになります。

1. DNS がクエリを Route 53 ネームサーバーにルーティングします。
2. Route 53 は、ロンドンとシンガポールリージョン間のレイテンシーおよびロンドンとオレゴンリージョン間のレイテンシーに基づいて、そのリクエストのデータを参照します。
3. ロンドンとオレゴンリージョン間のレイテンシーのほうが低い場合、Route 53 はオレゴンのロードバランサーの IP アドレスをクエリに対して返します。ロンドンとシンガポールリージョン間のレイテンシーの方が低い場合、Route 53 はシンガポールのロードバランサーの IP アドレスをクエリに対して返します。

インターネット上のホスト間のレイテンシーは、ネットワーク接続やルーティングの変化に伴って時間の経過とともに変化する可能性があります。レイテンシーベースのルーティングでは、一定期間に取得されたレイテンシーデータが使用され、データはこれらの変更を反映します。今週オレゴンリージョンにルーティングされたリクエストは、来週シンガポールリージョンに送られる可能性があります。

> **Note**
>
> ブラウザまたは他のビューアが EDNS0 の edns-client-subnet 拡張をサポートする DNS リゾルバーを使用している場合、DNS リゾルバーはユーザーの IP アドレスを切り捨てたアドレスを Route 53 に送信します。レイテンシーベースルーティングを設定した場合、Route 53 はトラフィックをリソースにルーティングする際にこの値を考慮します。詳細については、「Amazon Route 53 が EDNS0 を使用してユーザーの場所を推定する方法」を参照してください。

レイテンシールーティングポリシーは、プライベートホストゾーンのレコードに使用できます。

レイテンシールーティングポリシーを使用してレコードを作成するときに指定する値の詳細については、以下のトピックを参照してください。

- レイテンシーレコードに固有の値
- レイテンシーエイリアスレコードに固有の値
- すべてのルーティングポリシーに共通する値
- すべてのルーティングポリシーのエイリアスレコードに共通する値

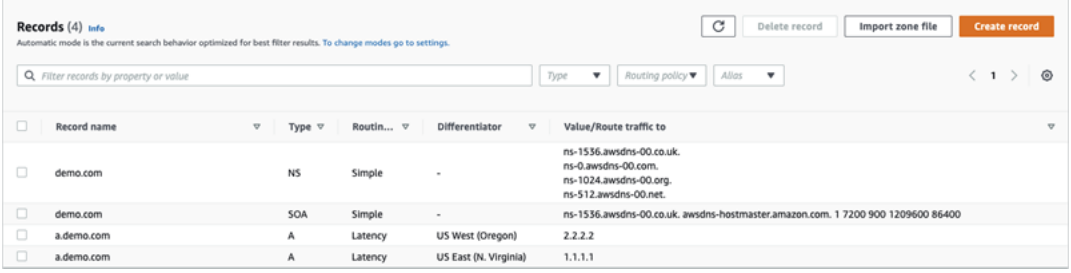
プライベートホストゾーンのレイテンシーに基づくルーティング

プライベートホストゾーンの場合、Route 53 は、同じ にある AWS リージョンエンドポイント、またはクエリの送信元の VPC AWS リージョン の に最も近いエンドポイントを使用して DNS クエリに応答します。

> **Note**
>
> アウトバウンドエンドポイントがインバウンドエンドポイントに転送されている場合、レコードはアウトバウンドエンドポイントではなく、インバウンドエンドポイントの位置に基づいて解決されます。

ヘルスチェックを含め、クエリのオリジンに対するレイテンシーが最も低いレコードが異常である場合、レイテンシーが次に低い正常なエンドポイントが返されます。

次の図の設定例では、us-east-1 AWS リージョンまたはそれに最も近い DNS クエリが 1.1.1.1 エンドポイントにルーティングされます。us-west-2 からの DNS クエリ、またはそれに最も近いクエリは、2.2.2.2 エンドポイントにルーティングされます。



IP ベースルーティング

Amazon Route 53 の IP ベースのルーティングを使用すると、ネットワーク、アプリケーション、クライアントに関する知識に基づいて DNS ルーティングを微調整できます。これにより、エンドユーザーに最適な DNS ルーティングを選択できます。IP ベースのルーティングでは、user-IP-to-endpointへのマッピングとして Route 53 にデータをアップロードすることで、パフォーマンスの向上やネットワークコストの削減をきめ細かく制御できます。

位置情報とレイテンシーベースのルーティングは、Route 53 が収集して最新の状態に保つデータを使用します。このアプローチは、ほとんどのお客様に適しています。IP ベースのルーティングを使用すると、顧客ベースについて知っている情報に基づいてルーティングを調整する機能を追加できます。例えば、グローバルビデオプロバイダーは、特定のインターネットサービスプロバイダー (ISP) からエンドユーザーをルーティングする場合があります。

以下に、IP ベースルーティングでの一般的なユースケースを示します。

- ネットワーク伝送コストやパフォーマンスを最適化するために、特定の ISP から特定のエンドポイントにエンドユーザーをルーティングしたい場合。
- クライアントの物理的な場所に関する情報に基づいて、位置情報ルーティングなど、既存の Route 53 ルーティングタイプにオーバーライドを追加したい場合。

IP 範囲の管理とリソースレコードセット (RRSet) への関連付け

IPv4 では長さ 1 ~ 24 ビットの CIDR ブロックを使用できますが、IPv6 では 1 ~ 48 ビットの長さの CIDR ブロックを使用できます。ゼロビット CIDR ブロック (0.0.0.0/0 または ::/0) を定義するには、デフォルト (「*」) の場所を使用します。

CIDR コレクションで指定されたものよりも長い CIDR を持つ DNS クエリの場合、Route 53 はそれを短い CIDR と一致させます。例えば、CIDR コレクションの CIDR ブロックとして 2001:0DB8::/32

を指定し、クエリが 2001:0DB8:0000:1234::/48 から発信された場合、そのクエリは一致します。一方、CIDR コレクションで 2001:0DB8:0000:1234::/48 を指定し、クエリが 2001:0DB8::/32 から発信された場合、これは一致せず、Route 53 はデフォルト (「*」) ロケーションのレコードで応答します。

CIDR ブロック (または IP 範囲) のセットは、CIDR ロケーション内にグループ化することができ、このグループは以下のように、CIDR コレクションと呼ばれる再利用可能なエンティティにグループ化されます。

CIDR ブロック

CIDR 表記での IP 範囲。例:192.0.2.0/24 または 2001:DB8::/32。

CIDR ロケーション

CIDR ブロックの名前付きリスト。これは例えば、example-isp-seattle = [192.0.2.0/24, 203.0.113.0/22, 198.51.100.0/24, 2001:DB8::/32]、のようになります。CIDR ロケーションリスト内のブロックは、隣接している必要や、同じ範囲である必要はありません。

IPv4 ブロックと IPv6 ブロックの両方を単一のロケーションに含めることが可能で、このロケーションはそれぞれ A レコードセットと AAAA レコードセットの両方に関連付けることができます。

慣例では、このロケーション名は土地の名前であることが多いですが、任意の文字列でも問題ありません (Company-A など)。

CIDR コレクション

名前付きロケーションのコレクション。これは例えば、mycollection = [example-isp-seattle, example-isp-tokyo] のようになります。

IP ベースのルーティングリソースレコードセットはコレクション内のロケーションを参照します。同じ名前とタイプのレコードセットでは、すべてのリソースレコードセットが同じコレクションを参照する必要があります。例えば、2 つのリージョンに Web サイトを作成し、これら 2 つの異なる CIDR ロケーションから、発信元 IP アドレスに基づいて特定の Web サイトに DNS クエリを送信する場合は、それらの両方のロケーションを同じ CIDR コレクションにリストする必要があります。

IP ベースルーティングポリシーは、プライベートホストゾーンのレコードに使用できません。

シンプルルーティングポリシーを使用してレコードを作成する際に指定する値については、以下のトピックを参照してください。

- IP ベースレコード特有の値
- IP ベースエイリアスレコードに特有の値
- すべてのルーティングポリシーに共通する値
- すべてのルーティングポリシーのエイリアスレコードに共通する値

トピック

- Creating a CIDR collection with CIDR locations and blocks (CIDR ロケーションとブロックを使用した CIDR コレクションの作成)
- CIDR ロケーションと CIDR ブロックの操作
- CIDR コレクションの削除
- 位置情報ルーティングを IP ベースのルーティングに移動する

Creating a CIDR collection with CIDR locations and blocks (CIDR ロケーションとブロックを使用した CIDR コレクションの作成)

使用を開始するには、CIDR コレクションを作成し、そのコレクションに CIDR ブロックとロケーションを追加します。

Route 53 コンソールを使用して CIDR コレクションを作成するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで、[IP-based routing] (IP ベースルーティング)、[CIDR collections] (CIDR コレクション) の順に選択します。
3. [Create CIDR collection] (CIDR コレクションを作成) を選択します。
4. [Create CIDR collection] (CIDR コレクションの作成) ペインで、[Details] (詳細) の下にコレクションの名前を入力します。
5. [Create collection] (コレクションを作成) を選択し、空のコレクションを作成します。

   - または -

   [CIDR ロケーションの作成] セクションの[CIDR ロケーション]ボックスに CIDR ロケーションの名前を入力します。ロケーション名には、識別できる任意の文字列を使用できます。例えば **`company 1`**、または **`Seattle`** などです。これらは、実際の地理的な名前でなくても問題ありません。

> **Important**
>
> CIDR ロケーション名の最大長は 16 文字です。

[CIDR ブロック] ボックスに CIDR ブロックを 1 行に 1 つずつ入力します。これらの指定には、IPv4 アドレス (/0 から /24 の範囲) または IPv6 アドレス (/0 から /48 の範囲) を使用します。

6. さらにロケーションと CIDR ブロックの入力を続ける場合は、CIDR ブロックを入力した後、[Create CIDR collection] (CIDR コレクションを作成) または [Add another location] (別のロケーションを追加) を選択します。コレクションごとに複数の CIDR ロケーションを入力できます。
7. CIDR ロケーションを入力し終えたら、[Create CIDR collection] (CIDR コレクションを作成) を選択します。

CIDR ロケーションと CIDR ブロックの操作

Route 53 コンソールから CIDR ロケーションを操作するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで、IP ベースのルーティング、CIDR コレクションを選択し、CIDR コレクションセクションで、コレクション名リストの CIDR コレクションへのリンクを選択します。

   [CIDR locations] (CIDR ロケーション) ページでは、CIDR ロケーションの作成や削除、ロケーションとそのブロックの編集を行うことができます。

   - [Create CIDR location] (CIDR ロケーションを作成) を選択し、ロケーションを作成します。
   - [Create CIDR location] (CIDR ロケーションの作成) ペインで、ロケーションとロケーションに関連付けられた CIDR ブロックの名前をそれぞれ入力し、[Create] (作成) を選択します。
   - CIDR ロケーションと内部のブロックを表示するには、ロケーションペインで、名前と CIDR ブロックを表示する対象のロケーションの横にあるラジオボタンをオンにします。

     このペインにある [編集] をクリックすると、ロケーションと CIDR ブロックの名前を更新することもできます。編集が完了したら、[Save] (保存) を選択します。

- CIDR ロケーションとその中のブロックを削除するには、削除する対象のロケーションの横でラジオボタンをオンにし、次に [Delete] (削除) を選択します。削除されたことを確認するには、テキスト入力フィールドにロケーション名を入力した上で、もう一度、[Delete] (削除) を選択します。

> **Important**
>
> 削除された CIDR ロケーションは元に戻せません。削除ロケーションに DNS レコードを関連付けている場合、使用しているドメインに到達できなくなる可能性があります。

CIDR コレクションの削除

Route 53 コンソールを使用して、CIDR コレクション、そのロケーション、およびブロックを削除するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで、[IP-based routing] (IP ベースルーティング)、[CIDR collections] (CIDR コレクション) の順に選択します。
3. CIDR コレクションセクションで、削除するコレクションのリンク名を選択します。
4. [CIDR locations] (CIDR ロケーション) ページで、1 つずつ各ロケーションを 選択した上で [Delete] (削除) を選択し、ダイアログボックスに対象の名前を入力した後、[Delete] (削除) を選択します。CIDR コレクションに関連付けられている個々のロケーションを削除した後、そのコレクションを削除できるようになります。
5. 各 CIDR ロケーションの削除が完了したら、[CIDR locations] (CIDR ロケーション) ページで、削除するコレクションの横にあるラジオボタンをオンにした上で、[Delete] (削除) を選択します。

位置情報ルーティングを IP ベースのルーティングに移動する

位置情報または地理的近接性ルーティングを使用し、特定のクライアントが物理的な場所またはネットワークトポロジに基づいて最適でないエンドポイントに一貫してルーティングされる場合、代わりに IP ベースのルーティングでそれらのクライアントのパブリック IP 範囲をターゲットにできます。

位置情報ルーティングを IP ベースのルーティングに移動するには

1. 上書きする位置情報レコードを特定します。次の例は、カリフォルニアの IP 範囲に合わせて微調整する位置情報設定を示しています。

   位置情報設定の例

レコードセット名	ルーティングポリシーと送信元	アプリケーションエンドポイントの IP アドレス
example.com	位置情報ルーティング (米国)	198.51.100.1
example.com	位置情報ルーティング (欧州)	198.51.100.2

2. カリフォルニアから新しいアプリケーションエンドポイントに IP 範囲を上書きするには、新しいレコードセット名 (geo.example.comではなく など) で位置情報ルーティングレコードを再作成しますexample.com。

   再作成された位置情報レコード

レコードセット名	ルーティングポリシーと送信元	アプリケーションエンドポイントの IP アドレス
geo.example.com	位置情報ルーティング (米国)	198.51.100.1
geo.example.com	位置情報ルーティング (欧州)	198.51.100.2

3. 再作成された位置情報ルーティングレコードセットを指す IP ベースのルーティングレコードとデフォルトレコードを作成します。

   IP ベースのルーティングレコード

レコードセット名	ルーティングポリシーと送信元	アプリケーションエンドポイントの IP アドレス
example.com	IP ベースルーティング (デフォルト)	geo.example.com へのエイリアスレコード。例えば、198.51.100.1 。
example.com	IP ベースルーティング (カリフォルニア IP 範囲)	198.51.100.3

複数値回答ルーティング

複数値回答ルーティングを使用すると、DNS クエリに応答してウェブサーバーの IP アドレスなど、複数の値を返すように Amazon Route 53 を設定できます。ほぼすべてのレコードに複数の値を指定できますが、複数値の回答ルーティングでは、各リソースの状態を確認することもできます。その後、Route 53 は正常なリソースの値のみを返します。これはロードバランサーに代わるものではありませんが、複数のヘルスチェックされた IP アドレスを返すことは、DNS を使用して稼働時間とロード共有を向上させる方法です。

トラフィックをウェブサーバーなどの複数のリソースにランダムにルーティングするには、リソースごとに 1 つの複数値回答レコードを作成し、オプションで Route 53 ヘルスチェックを各レコードにリンクします。Route 53 は最大 8 つの正常なレコードを持つ DNS クエリに応答し、DNS リゾルバーごとに異なる回答を返します。リゾルバーが応答をキャッシュした後にウェブサーバーが使用できなくなる場合、クライアントソフトウェアは応答内の別の IP アドレスを試すことができます。

次の点に注意してください。

- ヘルスチェックを複数値回答のレコードと関連付けている場合、Route 53 はヘルスチェックの結果が正常である場合にのみ、対応する IP アドレスを DNS クエリに返します。
- ヘルスチェックを複数値回答レコードと関連付けない場合、Route 53 は常にレコードを正常であると見なします。
- 8 つ以下の正常なレコードがある場合、Route 53 はすべての DNS クエリに正常なすべてのレコードを返します。
- すべてのレコードが異常である場合、Route 53 は DNS クエリに最大 8 つの異常なレコードを返します。

複数値回答ルーティングポリシーは、プライベートホストゾーンのレコードに使用できます。

複数値回答ルーティングポリシーを使用してレコードを作成するときに指定する値の詳細については、複数値回答レコードに固有の値 および すべてのルーティングポリシーに共通する値 を参照してください。

加重ルーティング

加重ルーティングを使用すると、複数のリソースを単一のドメイン名 (example.com) またはサブドメイン名 (acme.example.com) にリンクし、各リソースへのトラフィック量を選択できます。これは、ソフトウェアの新しいバージョンのロードバランシングとテストに役立ちます。

加重ルーティングを設定するには、リソースごとに同じ名前とタイプでレコードを作成します。各レコードに、各リソースに送信するトラフィックの量と一致する相対的な重みを付けます。Amazon Route 53 は、グループ内のすべてのレコードの合計重みに対する割合としてレコードに割り当てた重みに基づいて、リソースにトラフィックを送信します。

$$\frac{\text{Weight for a specified record}}{\text{Sum of the weights for all records}}$$

たとえば、トラフィックのごく一部を 1 つのリソースに送信し、残りを別のリソースに送信する場合は、重みを 1 と 255 に設定できます。重みが 1 のリソースは、トラフィックの 1/256 (1/(1+255)) を、他のリソースは 255/256 (255/(1+255)) を取得します。重みを変更することで、バランスを徐々に変更できます。リソースへのトラフィックの送信を停止する場合は、そのレコードの重みを 0 に変更します。

加重ルーティングポリシーを使用してレコードを作成するときに指定する値の詳細については、以下のトピックを参照してください。

- 加重レコードに固有の値
- 加重エイリアスレコードに固有の値
- すべてのルーティングポリシーに共通する値
- すべてのルーティングポリシーのエイリアスレコードに共通する値

加重ルーティングポリシーは、プライベートホストゾーンのレコードに使用できます。

ヘルスチェックと加重ルーティング

加重レコードのグループ内のすべてのレコードにヘルスチェックを追加する一方で、一部のレコードにゼロ以外の重みを付け、他のレコードの重みをゼロにした場合、ヘルスチェックは、次の例外を除いて、すべてのレコードの重みがゼロ以外の場合と同様に動作します。

- 最初に Route 53 は、ゼロ以外の加重レコード (存在する場合) のみを対象とします。
- 重みが 0 より大きいレコードがいずれも異常であった場合、Route 53 は、重みがゼロである加重レコードを対象にします。

次の表は、重みが 0 のレコードにヘルスチェックが含まれる場合の動作の詳細を示しています。

ヘルスチェックによるゼロウェイトレコード

	レコード 1	レコード 2	レコード 3
重み	1	1	0
ヘルスチェックが含まれていますか?	はい	はい	はい
ヘルスチェックステータス	異常	異常	Healthy
DNSクエリに回答しましたか?	いいえ	なし	はい
ヘルスチェックステータス	異常	異常	異常
DNS query answered?	はい	はい	いいえ
ヘルスチェックステータス	異常	Healthy	異常
DNSクエリに回答しましたか?	いいえ	はい	いいえ
ヘルスチェックステータス	Healthy	Healthy	異常
DNSクエリに回答しましたか?	はい	はい	いいえ

	レコード 1	レコード 2	レコード 3
ヘルスチェックステータス	Healthy	Healthy	Healthy
DNSクエリに回答しましたか?	はい	はい	いいえ

次の表は、重みが 0 のレコードにヘルスチェックが含まれない場合の動作の詳細を示しています。

ヘルスチェックなしのゼロウェイトレコード

	レコード 1	レコード 2	レコード 3
重み	1	1	0
ヘルスチェックが含まれていますか?	はい	はい	いいえ
ヘルスチェックステータス	Healthy	Healthy	N/A
DNS query answered?	Yes	はい	No
ヘルスチェックステータス	異常	異常	該当なし
DNSクエリに回答しましたか?	いいえ	なし	はい

	レコード 1	レコード 2	レコード 3
ヘルスチェックステータス	異常	Healthy	該当なし
DNS query answered?	いいえ	はい	いいえ

Amazon Route 53 が EDNS0 を使用してユーザーの場所を推定する方法

位置情報、地理的近接性、IP ベース、およびレイテンシーに関するルーティングの精度を高めるために、Amazon Route 53 は EDNS0 の edns-client-subnet 拡張をサポートしています (EDNS0 は DNS プロトコルにオプションの拡張機能を追加します) 。Route 53 では、DNS リゾルバーが edns-subnet をサポートしている場合のみ、edns-subnet を使用できます。

- ブラウザまたは他のビューワーが edns-client-subnet をサポートしていない DNS リゾルバーを使用する場合、Route 53 は DNS リゾルバーのソース IP アドレスを使用してユーザーがどこにいるかを推測し、リゾルバーの場所の DNS レコードを使用して位置情報クエリに応答します。
- ブラウザまたは他のビューワーが edns-client-subnet をサポートする DNS リゾルバーを使用する場合、DNS リゾルバーは Route 53 にユーザーの IP アドレスの短縮バージョンを送信します。Route 53 は、リゾルバーの送信元 IP アドレスではなく短縮された IP アドレスからユーザーの場所を見つけます。これにより、通常、より正確な場所が得られます。Route 53 は、ユーザーの場所の DNS レコードを位置情報クエリに返します。
- EDNS0 は、プライベートホストゾーンには適用されません。プライベートホストゾーンの場合、Route 53 は、プライベートホストゾーン AWS リージョン がある の VPC リゾルバーからのデータを使用して、位置情報とレイテンシーのルーティングを決定します。

edns-client-subnet の詳細については、EDNS Client Subnet RFC の「DNS リクエストのクライアントサブネット」を参照してください。

エイリアスレコードと非エイリアスレコードの選択

Amazon Route 53 エイリアスレコードは、DNS への Route 53 固有の拡張機能を提供します。エイリアスレコードを使用すると、CloudFront ディストリビューションや Amazon S3 バケットなどの選択した AWS リソースにトラフィックをルーティングできます。また、エイリアスレコードにより、ホストゾーン内のあるレコードから別のレコードにトラフィックをルーティングできます。

CNAME レコードとは異なり、DNS 名前空間の最上位ノード (Zone Apex とも呼ばれる) にエイリアスレコードを作成できます。例えば、example.com という DNS 名を登録する場合、Zone Apex は example.com になります。example.com の CNAME レコードを作成することはできませんが、トラフィックを example.com にルーティングする www.example.com のエイリアスレコードを作成できます (www.example.com のレコードタイプが CNAME でない限り) 。

Route 53 がエイリアスレコードに対する DNS クエリを受信すると、Route 53 はそのリソースに適用可能な値を返します。

- Amazon API Gateway リージョン固有のカスタム API またはエッジ最適化 API – Route 53 はお客様の API の 1 つ以上の IP アドレスで応答します。
- Amazon VPC インターフェイスエンドポイント – Route 53 はインターフェイスエンドポイントの 1 つ以上の IP アドレスで応答します。
- CloudFront ディストリビューション – Route 53 は、お客様のコンテンツを提供できる CloudFront エッジサーバーの 1 つまたは複数の IP アドレスで応答します。
- App Runner サービス – Route 53 は 1 つ以上の IP アドレスで応答します。
- Elastic Beanstalk 環境 – Route 53 はその環境の 1 つまたは複数の IP アドレスで応答します。
- Elastic Load Balancing ロードバランサー – Route 53 は、ロードバランサーの 1 つまたは複数の IP アドレスで応答します。これには、Application Load Balancer、Classic Load Balancer、Network Load Balancer が含まれます。
- AWS Global Accelerator アクセラレーター – Route 53 はアクセラレーターの IP アドレスで応答します。
- OpenSearch Service – Route 53 は OpenSearch Service カスタムドメインの 1 つ以上の IP アドレスで応答します。
- 静的ウェブサイトとして設定されている Amazon S3 バケット – Route 53 は Amazon S3 バケットの 1 つの IP アドレスで応答します。
- 同じホストゾーン内の同じタイプの別の Route 53 レコード – Route 53 は、エイリアスレコードで参照されたレコードに関するクエリを受け取ったのかのように応答します (「エイリアスレコードと CNAME レコードの比較」を参照してください)。
- AWS AppSync ドメイン名 – Route 53 は、インターフェイスエンドポイントの 1 つ以上の IP アドレスで応答します。

詳細については、「AWS リソースへのインターネットトラフィックのルーティング」を参照してください。

エイリアスレコードを使用して AWS リソースにトラフィックをルーティングすると、Route 53 はリソースの変更を単独で検出します。例えば、エイリアスレコード example.com が lb1-1234.us-east-2.elb.amazonaws.com の Elastic Load Balancing ロードバランサーを指し示しているとします。ロードバランサーの IP アドレスが変更されると、Route 53 は新しい IP アドレスを使用して DNS クエリへの応答を開始します。

エイリアスレコードが AWS リソースを指す場合、有効期限 (TTL) を設定することはできません。Route 53 はリソースのデフォルトの TTL を使用します。エイリアスレコードが同じホストゾーン内の別のレコードを指す場合、Route 53 はターゲットレコードの TTL を使用します。Elastic Load Balancing の現在の TTL 値の詳細については、Elastic Load Balancing ユーザーガイドの「リクエストルーティング」で「ttl」を検索してください。

Route 53 コンソールを使用したレコード作成の詳細については、「Amazon Route 53 コンソールを使用したレコードの作成」を参照してください。エイリアスレコードに指定する値の詳細については、「Amazon Route 53 レコードの作成時または編集時に指定する値」の該当するトピックを参照してください。

- シンプルなエイリアスレコードに固有の値
- 加重エイリアスレコードに固有の値
- レイテンシーエイリアスレコードに固有の値
- フェイルオーバーエイリアスレコードに固有の値
- 位置情報エイリアスレコードに固有の値
- 地理的近接性エイリアスレコードに固有の値
- すべてのルーティングポリシーのエイリアスレコードに共通する値

エイリアスレコードと CNAME レコードの比較

エイリアスレコードは CNAME レコードに似ていますが、次のようないくつかの大きな違いがあります。次のリストでは、エイリアスレコードと CNAME レコードを比較します。

クエリのリダイレクト先とすることができるリソース

エイリアスレコード

エイリアスレコードは、以下を含むがこれらに限定されない、選択した AWS リソースにのみクエリをリダイレクトできます。

- Amazon S3 バケット

- CloudFront ディストリビューション
- 同じ Route 53 ホストゾーンの他のレコード

例えば、acme.example.com という名前の Amazon S3 バケットにクエリをリダイレクトする acme.example.com という名前のエイリアスレコードを作成できます。example.com ホストゾーン内の zenith.example.com という名前のレコードにクエリをリダイレクトする acme.example.com エイリアスレコードを作成することもできます。

CNAME レコード

CNAME レコードは、DNS クエリを任意の DNS レコードにリダイレクトできます。例えば、acme.example.com からzenith.example.com または acme.example.org にクエリをリダイレクトする CNAME レコードを作成できます。クエリのリダイレクト先ドメインの DNS サービスとして　Route 53 を使用する必要はありません。

ドメインと同じ名前のレコードの作成 (Zone Apex にあるレコード)

エイリアスレコード

ほとんどの設定では、ホストゾーン (Zone Apex) と同じ名前のエイリアスレコードを作成できます。1 つの例外は、Zone Apex (example.com など) から CNAME のタイプを持つ同じホストゾーン (zenith.example.com など) のレコードにクエリをリダイレクトする場合です。これは、トラフィックがルーティングされているレコードとエイリアスレコードのタイプが同じでなければならず、Zone Apex の CNAME レコードの作成はエイリアスレコードであってもサポートされていないためです。

CNAME レコード

ホストゾーン (Zone Apex) と同じ名前の CNAME レコードを作成することはできません。これは、ドメイン名のホストゾーン (example.com) とサブドメインのホストゾーン (zenith.example.com) の両方に当てはまります。

DNS クエリの料金設定

エイリアスレコード

Route 53 では、 AWS リソースへのエイリアスクエリには課金されません。詳細については、「Amazon Route 53 料金表」を参照してください。

CNAME レコード

Route 53 では、CNAME クエリに対して課金されます。

> **Note**
>
> Route 53 ホストゾーン (同じホストゾーンまたは別のホストゾーン) の別のレコードの名前にリダイレクトする CNAME レコードを作成した場合、各 DNS クエリは 2 つのクエリとして課金されます。
>
> - Route 53 は、リダイレクト先のレコードの名前で最初の DNS クエリに応答します。
> - 次に、DNS リゾルバーは、最初のレスポンスでレコードの別のクエリを送信して、トラフィックを誘導する場所 (ウェブサーバーの IP アドレスなど) に関する情報を取得する必要があります。
>
> CNAME レコードが別の DNS サービスでホストされているレコードの名前にリダイレクトされる場合、Route 53 では、 1 つのクエリに対して課金されます。別の DNS サービスでは、2 番目のクエリに対して課金される場合があります。

DNS クエリで指定されたレコードタイプ

エイリアスレコード

Route 53 は、エイリアスレコードの名前 (acme.example.com など) とエイリアスレコードのタイプ (A や AAAA など) が DNS クエリの名前およびタイプと一致した場合にだけ DNS クエリに応答します。

CNAME レコード

CNAME レコードは、A や AAAA など、DNS クエリで指定されたレコードタイプに関係なく、レコード名の DNS クエリをリダイレクトします。

dig クエリまたは nslookup クエリでレコードがリストされる方法

エイリアスレコード

dig クエリまたは nslookup クエリへのレスポンスでは、エイリアスレコードは、レコードを作成したときに指定したレコードタイプとして表示されます (A や AAAA など)。(エイリアスレコードに指定するレコードタイプは、トラフィックをルーティングするリソースによって異なります。例えば、S3 バケットにトラフィックをルーティングするには、タイプに A を指定します)。エイリアスプロパティは、Route 53 コンソールまたは AWS CLI `list-resource-record-sets` コマンドなどのプログラムによるリクエストへのレスポンスでのみ表示されます。

CNAME レコード

CNAME レコードは、dig または nslookup クエリへの応答で CNAME レコードとして表示されます。

サポートされる DNS レコードタイプ

Amazon Route 53 は、このセクションに一覧表示されている DNS レコードタイプをサポートしています。それぞれのレコードタイプの説明には、API を使用して Route 53 にアクセスするときに `Value` 要素を書式化する例も含まれています。

> **Note**
>
> ドメイン名を含むレコードタイプの場合は、完全修飾ドメイン名 (例えば、www.example.com) を入力します。末尾のドットはオプションです。Route 53 では、ドメイン名が完全修飾ドメイン名であると見なされます。つまり、Route 53 では、(末尾にドットのない) www.example.com と (末尾にドットのある) www.example.com. が同一と見なされます。

Route 53 は、エイリアスレコードと呼ばれる DNS 機能の拡張を提供します。CNAME レコードと同様に、エイリアスレコードを使用すると、選択した AWS リソース (CloudFront ディストリビューションや Amazon S3 バケットなど) にトラフィックをルーティングできます。エイリアスレコードと CNAME レコードの比較など、詳細については、「エイリアスレコードと非エイリアスレコードの選択」を参照してください。

トピック

- A レコードタイプ
- AAAA レコードタイプ
- CAA レコードタイプ
- CNAME レコードタイプ
- DS レコードタイプ
- HTTPS レコードタイプ
- MX レコードタイプ
- NAPTR レコードタイプ

- NS レコードタイプ
- PTR レコードタイプ
- SOA レコードタイプ
- SPF レコードタイプ
- SRV レコードタイプ
- SSHFP レコードタイプ
- SVCB レコードタイプ
- TLSA レコードタイプ
- TXT レコードタイプ

A レコードタイプ

A レコードと、ドット形式 10 進表記の IPv4 アドレスを使用して、ウェブサーバーなどのリソースにトラフィックをルーティングします。

Amazon Route 53 コンソールの例

```
192.0.2.1
```

Route 53 API の例

```
<Value>192.0.2.1</Value>
```

AAAA レコードタイプ

AAAA レコードと、コロン区切り 10 進表記の IPv6 アドレスを使用して、ウェブサーバーなどのリソースにトラフィックをルーティングします。

Amazon Route 53 コンソールの例

```
2001:0db8:85a3:0:0:8a2e:0370:7334
```

Route 53 API の例

```
<Value>2001:0db8:85a3:0:0:8a2e:0370:7334</Value>
```

CAA レコードタイプ

CAA レコードでは、ドメインまたはサブドメインの証明書の発行を許可する認証機関 (CA) を指定します。CAA レコードを作成すると、間違った CA がドメインの証明書を発行することを防止できます。CAA レコードは、ドメインの所有者であることを検証する要件など、認証機関によって指定されたセキュリティ要件に代わるものではありません。

CAA レコードを使用して以下を指定できます。

- SSL/TLS 証明書を発行できる認証機関 (CA)
- CA がドメインまたはサブドメインの証明書を発行するときに連絡する電子メールアドレスまたは URL

CAA レコードをホストゾーンに追加する際、スペースで区切られた 3 つの設定を指定します。

```
flags tag "value"
```

CAA レコードのフォーマットについて、以下の点に注意してください。

- `tag` の値として使用できる文字は A〜Z、a〜z、0〜9 のみです。
- `value` は常に引用符「""」で囲んでください。
- 一部の CA には `value` の追加の値が許可されるか、要求されます。名前と値のペアとして追加の値を指定し、セミコロン (;) で区切ります。次に例を示します。

  ```
  0 issue "ca.example.net; account=123456"
  ```
- CA がサブドメイン (例えば、www.example.com) の証明書のリクエストを受け取り、サブドメインの CAA レコードが存在しない場合、CA は CAA レコードの親ドメイン (例えば、example.com) に対して DNS クエリを送信します。親ドメインのレコードが存在し、証明書リクエストが有効な場合、CA はサブドメインの証明書を発行します。
- CAA レコードに指定する値を判断するには、CA に相談することをお勧めします。
- 同じ名前の CAA レコードと CNAME レコードを作成することはできません。DNS では CNAME レコードと他のタイプのレコードの両方で同じ名前を使用できないためです。

トピック

- CA にドメインまたはサブドメインの証明書の発行を許可する
- CA にドメインまたはサブドメインのワイルドカード証明書の発行を許可する

- CA にドメインまたはサブドメインの証明書を発行させない
- CA が無効な証明書リクエストを受信した場合に CA がお客様に通知するよう要求する
- CA でサポートされている別の設定を使用する
- 例

CA にドメインまたはサブドメインの証明書の発行を許可する

CA にドメインまたはサブドメインの証明書の発行を許可するには、ドメインまたはサブドメインと同じ名前でレコードを作成し、次の設定を指定します。

- flags – `0`
- tag – `issue`
- value – ドメインまたはサブドメインの証明書の発行を許可する CA のコード

例えば、ca.example.net が example.com に証明書を発行するよう許可するとします。以下の設定を使用して example.com の CAA レコードを作成します。

```
0 issue "ca.example.net"
```

AWS Certificate Manager に証明書の発行を許可する方法については、AWS Certificate Manager ユーザーガイド の CAA レコードの設定を参照してください。

CA にドメインまたはサブドメインのワイルドカード証明書の発行を許可する

CA にドメインまたはサブドメインのワイルドカード証明書の発行を許可するには、ドメインまたはサブドメインと同じ名前でレコードを作成し、次の設定を指定します。ワイルドカード証明書はドメインまたはサブドメイン、およびそのすべてのサブドメインに適用されます。

- flags – `0`
- tag – `issuewild`
- value – ドメインまたはサブドメイン、およびそのサブドメインの証明書の発行を許可する CA のコード

例えば、ca.example.net が example.com にワイルドカード証明書を発行するよう許可する場合、その許可は example.com とそのすべてのサブドメインに適用されます。以下の設定を使用して example.com の CAA レコードを作成します。

```
0 issuewild "ca.example.net"
```

CA にドメインまたはサブドメインのワイルドカード証明書を発行するよう許可するには、ドメインまたはサブドメインと同じ名前でレコードを作成し、次の設定を指定します。ワイルドカード証明書はドメインまたはサブドメイン、およびそのすべてのサブドメインに適用されます。

CA にドメインまたはサブドメインの証明書を発行させない

CA にドメインまたはサブドメインの証明書を発行させないためには、ドメインまたはサブドメインと同じ名前でレコードを作成し、次の設定を指定します。

- flags – `0`
- tag – `issue`
- value – `";"`

例えば、CA が example.com に証明書を発行しないようにしたいとします。以下の設定を使用して example.com の CAA レコードを作成します。

```
0 issue ";"
```

CA に example.com またはそのサブドメインに証明書を発行させないためには、以下の設定で example.com の CAA レコードを作成します。

```
0 issuewild ";"
```

> **Note**
>
> example.com の CAA レコードを作成し、次の両方の値を指定すると、ca.example.net の値を使用している CA は example.com の証明書を発行できます。
>
> ```
> 0 issue ";"
> 0 issue "ca.example.net"
> ```

CA が無効な証明書リクエストを受信した場合に CA がお客様に通知するよう要求する

無効な証明書リクエストを受信した CA がお客様に連絡するよう設定するには、以下の設定を指定します。

- flags – `0`
- tag – `iodef`
- value – CA が無効な証明書のリクエストを受信した場合に、CA からの通知を希望する URL または E メールアドレス。該当する形式を使用します。

  `"mailto:`*`email-address`*`"`

  `"http://`*`URL`*`"`

  `"https://`*`URL`*`"`

例えば、証明書に対する無効なリクエストを受信した CA が admin@example.com に E メールを送信するには、以下の設定を使用して CAA レコードを作成します。

```
0 iodef "mailto:admin@example.com"
```

CA でサポートされている別の設定を使用する

CA が CAA レコード用に RFC で定義されていない機能をサポートしている場合、以下の設定を指定します。

- flags – 128 (この値に設定すると、CA で指定された機能がサポートされていない場合に、CA による証明書の発行を防ぐことができます)
- tag – CA に使用を許可するタグ
- value – タグの値に対応する値

例えば、CA が無効な証明書リクエストを受け取った場合に、テキストメッセージを送信する機能を CA がサポートしているとします。(当社では、このオプションをサポートする CA は認識されていません。) レコードの設定は次のようになります。

```
128 exampletag "15555551212"
```

例

Route 53 コンソールの例

```
0 issue "ca.example.net"
```

```
0 iodef "mailto:admin@example.com"
```

Route 53 API の例

```
<ResourceRecord>
   <Value>0 issue "ca.example.net"</Value>
   <Value>0 iodef "mailto:admin@example.com"</Value>
</ResourceRecord>
```

CNAME レコードタイプ

CNAME レコードは、acme.example.com などの現在のレコードの名前に対する DNS クエリを、別のドメイン (example.com、example.net など) またはサブドメイン (acme.example.com、zenith.example.org など) にマッピングします。

> **Important**
>
> DNS プロトコルでは、Zone Apex とも呼ばれる、DNS 名前空間の最上位ノードに対して CNAME レコードを作成することができません。例えば、example.com という DNS 名を登録する場合、Zone Apex は example.com になります。example.com に対して CNAME レコードを作成することはできませんが、www.example.com、newproduct.example.com などに対しては CNAME レコードを作成できます。
>
> さらに、サブドメインに対して CNAME レコードを作成する場合、そのサブドメインの他のレコードを作成できません。例えば、www.example.com の CNAME を作成する場合、Name フィールドの値が www.example.com の他のレコードは作成できません。

Amazon Route 53 では、エイリアスレコードもサポートされています。これにより、CloudFront ディストリビューションや Amazon S3 バケットなどの選択された AWS リソースにクエリをルーティングできます。エイリアスはいろいろな意味で CNAME レコードタイプと似ていますが、エイリアスは Zone Apex に対して作成することができます。詳細については、「エイリアスレコードと非エイリアスレコードの選択」を参照してください。

Route 53 コンソールの例

```
hostname.example.com
```

Route 53 API の例

```
<Value>hostname.example.com</Value>
```

DS レコードタイプ

Delegation Signer (DS) レコードは、委任されたサブドメインゾーンのゾーンキーを参照します。DNSSEC 署名を設定するときに、信頼のチェーンを確立するときに DS レコードを作成することがあります。Route 53 の DNSSEC の設定の詳細については、「Amazon Route 53 での DNSSEC 署名の設定」を参照してください。

最初の 3 つの値は、キータグ、アルゴリズム、ダイジェストタイプを表す 10 進値です。4 番目の値は、ゾーンキーのダイジェストです。DS レコードの形式については、「RFC 4034」を参照してください。

Route 53 コンソールの例

```
123 4 5 1234567890abcdef1234567890absdef
```

Route 53 API の例

```
<Value>123 4 5 1234567890abcdef1234567890absdef</Value>
```

HTTPS レコードタイプ

HTTPS リソースレコードは、拡張設定情報を提供するサービスバインディング (SVCB) DNS レコードの形式であり、クライアントは HTTP プロトコルを使用してサービスに簡単かつ安全に接続できます。設定情報は、複数の DNS クエリを必要とするのではなく、1 つの DNS クエリで接続を許可するパラメータで提供されます。

HTTPS リソースレコードの形式は次のとおりです。

```
SvcPriority TargetName SvcParams(optional)
```

以下のパラメータについては、RFC 9460 セクション 9.1 で説明されています。

SvcPriority

優先度を表す整数。優先度 0 はエイリアスモードを意味し、通常は Zone Apex でのエイリアスを目的としています。この値は Route 53 の整数 0 ~ 32767 で、そのうち 1 ~ 32767 はサービスモードレコードです。優先度を下げ、選好度を上げます。

targetName

エイリアスターゲット (エイリアスモードの場合) または代替エンドポイント (ServiceMode の場合) のドメイン名。

SvcParams (オプション)

空白で区切られたリスト。各パラメータは Key=Value ペアまたはスタンドアロンキーで構成されます。複数の値がある場合は、カンマ区切りのリストとして表示されます。定義された SvcParams を次に示します。

- `1:alpn` – Application Layer Protocol Negotiation Protocol ID。デフォルトは HTTP/1.1、h2 は HTTP/2 over TLS、h3 は HTTP/3 (HTTP over QUIC protocol) です。
- `2:no-default-alpn` – デフォルトはサポートされていないため、`alpn` パラメータを指定する必要があります。
- `3:port` – 代替エンドポイント、またはサービスに到達できるポート。
- `4:ipv4hint` – IPv4 アドレスのヒント。
- `5:ech` – 暗号化されたクライアント Hello。
- `6:ipv6hint` – IPv6 アドレスのヒント。
- `7:dohpath` – DNS over HTTPS テンプレート
- `8:ohttp` - サービスは、不明瞭な HTTP ターゲットを操作します。

エイリアスモードの Amazon Route 53 コンソールの例

```
0 example.com
```

サービスモードの Amazon Route 53 コンソールの例

```
16 example.com alpn="h2,h3" port=808
```

エイリアスモードの Amazon Route 53 API の例

```
<Value>0 example.com</Value>
```

サービスモードの Amazon Route 53 API の例

```
<Value>16 example.com alpn="h2,h3" port=808</Value>
```

詳細については、「RFC 9460, Service Binding and Parameter Specification via the DNS (SVCB and HTTPS Resource Records)」を参照してください。

> **Note**
>
> Route 53 は任意の unknown-key プレゼンテーション形式 `keyNNNNN` をサポートしていません

MX レコードタイプ

MX レコードは、メールサーバーの名前を指定します。複数のメールサーバーがある場合は、優先順位を指定します。MX レコードの各値には、優先順位とドメイン名という 2 つの値が含まれます。

優先度

E メールサーバーの優先度を表す整数。サーバーを 1 つのみ指定する場合、優先順位は 0 ~ 65535 の任意の整数を指定できます。複数のサーバーを指定する場合、指定した優先度の値は、E メールをルーティングする順序の E メールサーバーを示します。優先順位の値が最も小さいサーバーが優先されます。例えば、E メールサーバーを 2 台所有しており、優先度に 10 および 20 と指定した場合は、利用できない場合を除き、E メールは常に優先度 10 でサーバーに送られます。10 および 10 を指定すると、メールは 2 つのサーバーにほぼ均等的にルーティングされます。

ドメイン名

E メールサーバーのドメイン名。A レコードまたは AAAA レコードの名前 (mail.example.com など) を指定します。RFC 2181, Clarifications to the DNS Specification のセクション 10.3 では、ドメイン名の値に CNAME レコードの名前を指定することを禁止しています。(RFC における「エイリアス」は CNAME レコードを意味します。Route 53 のエイリアスレコードではありません)。

Amazon Route 53 コンソールの例

```
10 mail.example.com
```

Route 53 API の例

```
<Value>10 mail.example.com</Value>
```

NAPTR レコードタイプ

名前付け権限ポインタ (NAPTR) は、動的委任発見システム (DDDS) アプリケーションで、1 つの値を別の値に変換または置き換えるために使用されるレコードのタイプです。例えば、1 つの一般的な用途は、電話番号を SIP URI に変換する場合です。

NAPTR レコードの `Value` 要素は、6 つのスペース区切りの値で構成されます。

Order

複数のレコードを指定した場合、DDDS アプリケーションがレコードを評価する順序。有効な値は 0 ~ 65535 です。

Preference

[Order] が同じ複数のレコードを指定した場合、それらのレコードが評価される順序の基本設定。例えば、[Order] が 1 のレコードが 2 つある場合、DDDS アプリケーションはまず [Preference] が小さいレコードを評価します。有効な値は 0 ~ 65535 です。

Flags

DDDS アプリケーションに固有の設定。RFC 3404 で現在定義されている値は、大文字および小文字の "A"、"P"、"S"、"U" と空の文字列 "" です。[Flags] は引用符で囲んでください。

サービス

DDDS アプリケーションに固有の設定。[Service] は引用符で囲んでください。

詳細については、該当する RFC を参照してください。

- URI DDDS アプリケーション – https://tools.ietf.org/html/rfc3404#section-4.4
- S-NAPTR DDDS アプリケーション – https://tools.ietf.org/html/rfc3958#section-6.5
- U-NAPTR DDDS アプリケーション – https://tools.ietf.org/html/rfc4848#section-4.5

Regexp

DDDS アプリケーションが入力値を出力値に変換するために使用する正規表現。例えば、IP 電話システムが正規表現を使用して、ユーザーが入力した電話番号を SIP URI に変換することができます。[Regexp] は引用符で囲んでください。[Regexp] の値と [Replacement] のいずれかを指定します。両方は指定しないでください。

正規表現には、次のいずれかの出力可能な ASCII 文字を含めることができます。

- a ~ z

- 0-9
- - (ハイフン)
- (スペース)
- ! # $ % & ' ( ) * + , - / : ; < = > ? @ [ ] ^ _ ` { | } ~ .
- " (引用符)。文字列にリテラル引用符を含めるには、文字列の前に \ 文字を置きます (\")。
- \ (バックスラッシュ)。文字列にバックスラッシュを含めるには、文字列の前に \ を置きます (\\)。

他のすべての値 (国際化ドメインなど) を 8 進数形式で指定します。

[Regexp] の構文については、「RFC 3402, section 3.2, Substitution Expression Syntax」を参照してください。

置換

DDDS アプリケーションが DNS クエリを送信する次のドメイン名の完全修飾ドメイン名 (FQDN)。DDDS アプリケーションは、入力値を [Replacement] に指定した値 (ある場合) に置き換えます。[Regexp] の値と [Replacement] のいずれかを指定します。両方は指定しないでください。[Regexp] の値を指定する場合は、[代替] にドット (.) を指定します。

ドメイン名には、a ~ z、0 ~ 9、- (ハイフン) を含めることができます。

DDDS アプリケーションと NAPTR レコードについては、次の RFC を参照してください。

- RFC 3401
- RFC 3402
- RFC 3403
- RFC 3404

Amazon Route 53 コンソールの例

```
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 の例

```
<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 レコードタイプ

NS レコードはホストゾーンのネームサーバーを識別します。次の点に注意してください。

- NS レコードの最も一般的な使用方法は、インターネットトラフィックがドメインにルーティングされる方法を制御することです。ホストゾーンのレコードを使用してドメインのトラフィックをルーティングするには、デフォルトの NS レコードの 4 つのネームサーバーを使用するようにドメイン登録設定を更新します (これは、ホストゾーンと同じ名前を持つ NS レコードです)。
- サブドメイン (acme.example.com) 用に別のホストゾーンを作成し、そのホストゾーンを使用して、サブドメインとそのサブドメイン (subdomain.acme.example.com) のインターネットトラフィックをルーティングできます。この設定は、ホストゾーンでルートドメイン (example.com) 用の別の NS レコードを作成することにより指定します (「ホストゾーンへのサブドメインの責任の委任」と呼ばれます)。詳細については、「サブドメインのトラフィックのルーティング」を参照してください。
- また、NS レコードを使用して、ホワイトラベルネームサーバーを設定することもできます。詳細については、「ホワイトラベルネームサーバーの設定」を参照してください。
- NS レコードのもう 1 つの用途は、サブドメインの権限をオンプレミスリゾルバーに委任する委任ルールを作成するときのプライベートホストゾーン用です。委任ルールを作成する前に、この NS レコードを作成する必要があります。詳細については、「Resolver エンドポイントが VPCs からネットワークに DNS クエリを転送する方法」を参照してください。

NS レコードの詳細については、「Amazon Route 53 がパブリックホストゾーンに作成する NS レコードと SOA レコード」を参照してください。

Amazon Route 53 コンソールの例

```
ns-1.example.com
```

Route 53 API の例

```
<Value>ns-1.example.com</Value>
```

PTR レコードタイプ

PTR レコードは、IP アドレスを対応するドメイン名にマッピングします。

Amazon Route 53 コンソールの例

```
hostname.example.com
```

Route 53 API の例

```
<Value>hostname.example.com</Value>
```

SOA レコードタイプ

Start of Authority (SOA) のレコードは、ドメインおよび対応する Amazon Route 53 のホストゾーンに関する情報を提供します。SOA レコードのフィールドについては、「Amazon Route 53 がパブリックホストゾーンに作成する NS レコードと SOA レコード」を参照してください。

Route 53 コンソールの例

```
ns-2048.awsdns-64.net hostmaster.awsdns.com 1 1 1 1 60
```

Route 53 API の例

```
<Value>ns-2048.awsdns-64.net hostmaster.awsdns.com 1 1 1 1 60</Value>
```

SPF レコードタイプ

以前は、メールの送信者の身元を確認するために SPF レコードが使用されていました。しかし、レコードタイプが SPF のレコードを作成することはもうお勧めできません。RFC 7208「Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1」が更新され、「... [RFC4408] で定義されたその存在と仕組みが相互運用性の問題を起こしています。したがって、その使用は SPF バージョン 1 ではもはや適切ではない。実装では使用してはならない」とされています。RFC 7208 のセクション 14.1「The SPF DNS Record Type」を参照してください。

SPF レコードの代わりに、該当する値を含む TXT レコードを作成することをお勧めします。有効な値については、Wikipedia の記事「センダーポリシーフレームワーク」を参照してください。

Amazon Route 53 コンソールの例

```
"v=spf1 ip4:192.168.0.1/16 -all"
```

Route 53 API の例

```
<Value>"v=spf1 ip4:192.168.0.1/16 -all"</Value>
```

SRV レコードタイプ

SRV レコードの Value 要素は 4 つのスペース区切りの値で構成されます。最初の 3 つの値は、優先順位、重み、およびポートをそれぞれ表す 10 進値です。4 番目の値は、ドメイン名です。SRV レコードは、メールや通信用のサービスなどのサービスにアクセスするために使用されます。SRV レコードの形式については、接続先のサービスのマニュアルを参照してください。

Amazon Route 53 コンソールの例

```
10 5 80 hostname.example.com
```

Route 53 API の例

```
<Value>10 5 80 hostname.example.com</Value>
```

SSHFP レコードタイプ

Secure Shell フィンガープリントレコード (SSHFP) は、ドメイン名に関連付けられた SSH キーを識別します。SSHFP レコードは、信頼チェーンを確立するために DNSSEC で保護する必要があります。DNSSEC の詳細については、「Amazon Route 53 での DNSSEC 署名の設定」を参照してください。

SSHFP リソースレコードの形式は次のとおりです。

```
[Key Algorithm] [Hash Type] Fingerprint
```

以下のパラメータは RFC 4255 で定義されています。

キーアルゴリズム

アルゴリズムタイプ:

- 0 – 予約済みで、使用されていません。

- 1: RSA – Rivest–Shamir–Adleman アルゴリズムは、最初のパブリックキー暗号システムの 1 つであり、安全なデータ転送に引き続き使用されています。
- 2: DSA – デジタル署名アルゴリズムは、デジタル署名の連邦情報処理標準です。DSA は、モジュール式指数と離散対数の数学モデルに基づいています。
- 3: ECDSA – 楕円曲線デジタル署名アルゴリズムは、楕円曲線暗号を使用する DSA のバリアントです。
- 4: Ed25519 – Ed25519 アルゴリズムは、SHA-512 (SHA-2) と Curve25519 を使用する EdDSA 署名スキームです。
- 6: Ed448 – Ed448 は、SHAKE256 と Curve448 を使用する EdDSA 署名スキームです。

ハッシュタイプ

パブリックキーハッシュの作成に使用されるアルゴリズム:

- 0 – 予約済みで、使用されていません。
- 1: SHA-1
- 2: SHA-256

Fingerprint

ハッシュの 16 進数表現。

Amazon Route 53 コンソールの例

```
1 1 09F6A01D2175742B257C6B98B7C72C44C4040683
```

Route 53 API の例

```
<Value>1 1 09F6A01D2175742B257C6B98B7C72C44C4040683</Value>
```

詳細については、「RFC 4255: Using DNS to Securely Publish Secure Shell (SSH) Key Fingerprints」を参照してください。

SVCB レコードタイプ

SVCB レコードを使用して、サービスエンドポイントにアクセスするための設定情報を配信します。SVCB は汎用 DNS レコードであり、さまざまなアプリケーションプロトコルのパラメータをネゴシエートするために使用できます。

SVCB リソースレコードの形式は次のとおりです。

```
SvcPriority TargetName SvcParams(optional)
```

以下のパラメータについては、RFC 9460 セクション 2.3 で説明されています。

SvcPriority

優先度を表す整数。優先度 0 はエイリアスモードを意味し、通常は Zone Apex でのエイリアスを目的としています。優先度を下げ、選好度を上げます。

targetName

エイリアスターゲット (エイリアスモードの場合) または代替エンドポイント (ServiceMode の場合) のドメイン名。

SvcParams (オプション)

空白で区切られたリスト。各パラメータは Key=Value ペアまたはスタンドアロンキーで構成されます。複数の値がある場合は、カンマ区切りのリストとして表示されます。この値は Route 53 の整数 0 ~ 32767 で、そのうち 1 ~ 32767 はサービスモードレコードです。定義された SvcParams を次に示します。

- `1:alpn` – Application Layer Protocol Negotiation Protocol ID。デフォルトは HTTP/1.1、h2 は HTTP/2 over TLS、h3 は HTTP/3 (HTTP over QUIC protocol) です。
- `2:no-default-alpn` – デフォルトはサポートされていないため、`alpn` パラメータを指定する必要があります。
- `3:port` – サービスに到達できる代替エンドポイントのポート。
- `4:ipv4hint` – IPv4 アドレスのヒント。
- `5:ech` – 暗号化されたクライアント Hello。
- `6:ipv6hint` – IPv6 アドレスのヒント。
- `7:dohpath` – DNS over HTTPS テンプレート
- `8:ohttp` - サービスは、不明瞭な HTTP ターゲットを操作します。

エイリアスモードの Amazon Route 53 コンソールの例

```
0 example.com
```

サービスモードの Amazon Route 53 コンソールの例

```
16 example.com alpn="h2,h3" port=808
```

エイリアスモードの Amazon Route 53 API の例

```
<Value>0 example.com</Value>
```

サービスモードの Amazon Route 53 API の例

```
<Value>16 example.com alpn="h2,h3" port=808</Value>
```

詳細については、「RFC 9460, Service Binding and Parameter Specification via the DNS (SVCB and HTTPS Resource Records)」を参照してください。

> **Note**
>
> Route 53 は任意の unknown-key プレゼンテーション形式 keyNNNNN をサポートしていません

TLSA レコードタイプ

TLSA レコードを使用して、名前付きエンティティの DNS ベースの認証 (DANE) を使用します。TLSA レコードは証明書/パブリックキーを Transport Layer Security (TLS) エンドポイントに関連付け、クライアントは DNSSEC で署名された TLSA レコードを使用して証明書/パブリックキーを検証できます。

TLSA レコードは、ドメインで DNSSEC が有効になっている場合にのみ信頼できます。DNSSEC の詳細については、「Amazon Route 53 での DNSSEC 署名の設定」を参照してください。

TLSA リソースレコードの形式は次のとおりです。

```
[Certificate usage] Selector [Matching type] [Certificate association data]
```

以下のパラメータは、RFC 6698 のセクション 3 で指定されています。

証明書の使用

TLS ハンドシェイクで提示された証明書と一致させるために使用される、提供された関連付けを指定します。

- 0: CA 制約 – 証明書またはパブリックキーは、TLS のサーバーによって提供されるエンドエンティティ証明書のパブリックキーインフラストラクチャ (PKIX) 証明書パスのいずれかにある必要があります。この制約により、指定されたサービスの証明書を発行するために使用できる CA が制限されます。
- 1: サービス証明書の制約 – TLS でサーバーから提供されたエンドエンティティ証明書と一致する必要があるエンドエンティティ証明書 (またはパブリックキー) を指定します。この証明書は、ホスト上の指定されたサービスで使用できるエンドエンティティ証明書を制限します。
- 2: 信頼アンカーアサーション – TLS でサーバーから提供されたエンドエンティティ証明書を検証するときに「トラストアンカー」として使用する必要がある証明書 (またはパブリックキー) を指定します。ドメイン管理者がトラストアンカーを指定できるようにします。
- 3: ドメイン発行の証明書 – TLS でサーバーから提供されたエンドエンティティ証明書と一致する必要がある証明書 (またはパブリックキー) を指定します。この証明書により、ドメイン管理者は、サードパーティー CA を関与させることなくドメインの証明書を発行できます。この証明書は PKIX 検証に合格する必要はありません。

Selector

ハンドシェイクでサーバーによって提示された証明書のどの部分が関連付け値と照合されるかを指定します。

- 0: 証明書全体が一致する必要があります。
- 1: サブジェクトパブリックキー、または DER エンコードされたバイナリ構造が一致している必要があります。

マッチングタイプ

証明書一致の表示 (セレクタフィールドによって決定) を指定します。

- 0: コンテンツの完全一致。
- 1: SHA-256 ハッシュ。
- 2: SHA-512 ハッシュ。

証明書の関連付けデータ

他のフィールドの設定に基づいて照合されるデータ。

Amazon Route 53 コンソールの例

```
0 0 1 d2abde240d7cd3ee6b4b28c54df034b97983a1d16e8a410e4561cb106618e971
```

Route 53 API の例

```
<Value>0 0 1 d2abde240d7cd3ee6b4b28c54df034b97983a1d16e8a410e4561cb106618e971</Value>
```

詳細については、「RFC 6698, The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA」を参照してください。

TXT レコードタイプ

TXT レコードには、二重引用符 (") で囲まれた 1 つ以上の文字列が含まれます。シンプルルーティングポリシーを使用する際には、同じ TXT レコードにあるドメインのすべての値 (example.com) またはサブドメイン (www.example.com) を含めます。

トピック

- TXT レコード値の入力
- TXT レコード値の特殊文字
- TXT レコード値の大文字と小文字
- 例

TXT レコード値の入力

1 つの文字列には、最大 255 文字を含めることができます。これには以下のものが含まれます。

- a ~ z
- A ~ Z
- 0-9
- スペース
- - (ハイフン)
- ! " # $ % & ' ( ) * + , - / : ; < = > ? @ [\ ] ^ _ ` { | } ~ .

255 文字を超える値を入力する必要がある場合、値を 255 文字以下の文字列に分割し、各文字列を二重引用符 (") で囲みます。コンソールで、同じ行にすべての文字列を一覧表示します。

```
"String 1" "String 2" "String 3"
```

API の場合、すべての文字列を同じ Value 要素に含めます。

```
<Value>"String 1" "String 2" "String 3"</Value>
```

TXT レコード内の値の最大長は 4,000 文字です。

複数の TXT 値を入力するには、値を 1 行に 1 つ入力します。

TXT レコード値の特殊文字

TXT レコードが以下の文字を含む場合は、エスケープコードを使って、*\3 ## 8 ####*という形式で文字を指定する必要があります。

- 8 進数で文字 000 ~ 040 (10 進数で 0 ~ 32、16 進数で 0x20 ~ 0x00)
- 8 進数で文字 177 ~ 377 (10 進数で 127 ~ 255、16 進数で 0xFF ~ 0x7F)

例えば、TXT レコードの値が "exämple.com" の場合、"ex\344mple.com" と指定します。

ASCII 文字および 8 進コードの間のマッピングについては、インターネットで「ASCII 8 進コード」を検索してください。ASCII Code - The extended ASCII table に役立つ情報があります。

文字列に引用符 (") を含めるには、引用符の前にバックスラッシュ (\) を配置します (\")。

TXT レコード値の大文字と小文字

ケースが保持され、"Ab" と "aB" は異なる値となります。

例

Amazon Route 53 コンソールの例

個別の行にそれぞれの値を入力します。

```
"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 の例

個別の Value 要素にそれぞれの値を入力します。

```
<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>
```

Amazon Route 53 コンソールを使用したレコードの作成

以下の手順では、Amazon Route 53 コンソールを使用してレコードを作成する方法について説明します。Route 53 API を使用してレコードを作成する方法については、「Amazon Route 53 API リファレンス」の「ChangeResourceRecordSets」を参照してください。

> **Note**
>
> 複雑なルーティング設定のレコードを作成するには、トラフィックフロービジュアルエディタを使用して設定をトラフィックポリシーとして保存することもできます。その後、トラフィックポリシーを同じホストゾーンまたは複数のホストゾーンの 1 つ以上のドメイン名 (example.com など) またはサブドメイン名 (www.example.com など) にリンクできます。新しいセットアップが期待どおりに機能しない場合は、更新をロールバックすることもできます。詳細については、「DNS トラフィックのルーティングにトラフィックフローを使用する」を参照してください。

Route 53 コンソールを使用してレコードを作成するには

1. エイリアスレコードを作成しない場合は、ステップ 2 に進みます。

   また、Elastic Load Balancing ロードバランサーまたは別の Route 53 レコード以外の AWS リソースに DNS トラフィックをルーティングするエイリアスレコードを作成する場合は、ステップ 2 に進みます。

   Elastic Load Balancing ロードバランサーにトラフィックをルーティングするエイリアスレコードを作成する場合、および、複数の異なるアカウントを使用してホストゾーンとロードバランサーを作成した場合は、手順「Elastic Load Balancing ロードバランサーの DNS 名を取得する」を実行してロードバランサーの DNS 名を取得します。
2. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
3. ナビゲーションペインで [Hosted zones] を選択します。
4. ドメインにすでにホストゾーンがある場合は、ステップ 5 に進みます。それ以外の場合は、該当する手順を実行してホストゾーンを作成します。

- インターネットトラフィックを Amazon S3 バケットや Amazon EC2 インスタンスなどのリソースにルーティングするには、「パブリックホストゾーンの作成」を参照してください。
- VPC でトラフィックをルーティングするには、「プライベートホストゾーンの作成」を参照してください。

5. [ホストゾーン] ページで、レコードを作成するホストゾーンの名前を選択します。
6. [Create record (レコードを作成)] を選択します。
7. 適切なルーティングポリシーと値を選択し、定義します。詳細については、作成するレコードの種類に関するトピックを参照してください。

   - すべてのルーティングポリシーに共通する値
   - すべてのルーティングポリシーのエイリアスレコードに共通する値
   - シンプルなレコードに固有の値
   - シンプルなエイリアスレコードに固有の値
   - フェイルオーバーレコードに固有の値
   - フェイルオーバーエイリアスレコードに固有の値
   - 位置情報レコードに固有の値
   - 位置情報エイリアスレコードに固有の値
   - 地理的近接性レコードに固有の値
   - 地理的近接性エイリアスレコードに固有の値
   - レイテンシーレコードに固有の値
   - レイテンシーエイリアスレコードに固有の値
   - IP ベースレコード特有の値
   - IP ベースエイリアスレコードに特有の値
   - 複数値回答レコードに固有の値
   - 加重レコードに固有の値
   - 加重エイリアスレコードに固有の値
8. [レコードを作成] を選択します。

> **Note**
>
> 新しいレコードが Route 53 DNS サーバーに伝達されるまでにしばらく時間がかかります。現在、変更が反映されたことを確認するには、GetChange API アクションを使用す

る方法しかありません。通常、変更は 60 秒以内にすべての Route 53 ネームサーバーに伝播します。

9. レコードを複数作成する場合は、ステップ 7 ~ 8 を繰り返します。

Elastic Load Balancing ロードバランサーの DNS 名を取得する

1. エイリアスレコードを作成する Classic、Application、または Network Load Balancer の作成に使用した AWS アカウント AWS マネジメントコンソール を使用して にサインインします。
2. Amazon EC2 コンソールの https://console.aws.amazon.com/ec2/ を開いてください。
3. ナビゲーションペインで、[Load Balancers] を選択します。
4. ロードバランサーのリストで、エイリアスレコードを作成するロードバランサーを選択します。
5. [Description] タブで、[DNS name] の値を取得します。
6. 他の Elastic Load Balancing ロードバランサーに対してもエイリアスレコードを作成する場合は、ステップ 4 と 5 を繰り返します。
7. からサインアウトします AWS マネジメントコンソール。
8. Route 53 ホストゾーンの作成に使用した AWS アカウントを使用して、 に AWS マネジメントコンソール 再度サインインします。
9. 手順「Amazon Route 53 コンソールを使用したレコードの作成」のステップ 3 に戻ります。

リソースレコードセットのアクセス許可

リソースレコードセットのアクセス許可は、Identity and Access Management (IAM) ポリシー条件を使用して、Route 53 コンソールまたは ChangeResourceRecordSets API を使用するときのアクションに対するきめ細かなアクセス許可を設定できます。

リソースレコードセットは、同じ名前とタイプ (およびクラス) の DNS レコードのグループですが、ほとんどの場合、クラスは常に IN またはインターネットです。ただし、異なるデータを保持します。例えば、位置情報ルーティングを選択した場合、同じドメインの異なるエンドポイントを指す複数の A レコードまたは AAAA レコードを設定できます。これらの A レコードまたは AAAA レコードはすべて、リソースレコードセットを形成します。DNS 用語の詳細については、「RFC 7719」を参照してください。

IAM ポリシー条件 、route53:ChangeResourceRecordSetsNormalizedRecordNames、route53:ChangeResource よび を使用するとroute53:ChangeResourceRecordSetsActions、他の AWS アカウントの

AWS 他のユーザーに詳細な管理権限を付与できます。これにより、あるユーザーに、次のアクセス許可を付与できます。

- 単一リソースレコードセット。
- 特定の DNS レコードタイプのすべてのリソースレコードセット。
- 名前に特定の文字列が含まれるリソースレコードセット。
- ChangeResourceRecordSets API、または Route 53 コンソール使用時の `CREATE | UPSERT | DELETE` アクションのいずれか、またはすべての実行。

Route 53 のポリシー条件のいずれかを組み合わせたアクセス許可を作成することもできます。例えば、あるユーザーに marketing-example.com の A レコードデータを変更するアクセス許可を付与するが、そのユーザーにはレコードの削除を許可しないことができます。

リソースレコードセットのアクセス許可の詳細と使用方法の例については、「詳細に設定されたアクセスコントロールのための IAM ポリシー条件の使用」を参照してください。

AWS ユーザーを認証する方法については、アイデンティティを使用した認証「」を参照してください。Route 53 リソースへのアクセスを制御する方法については、「」を参照してくださいアクセスコントロール。

Amazon Route 53 レコードの作成時または編集時に指定する値

Amazon Route 53 コンソールを使用してレコードを作成する場合、指定する値は、使用するルーティングポリシーと、トラフィックを AWS リソースにルーティングするエイリアスレコードを作成するかどうかによって異なります。

ターゲット AWS リソースを指定する特定のリソース (Elastic Load Balancing、CloudFront ディストリビューション、Amazon S3 バケットなど) にトラフィックをルーティングするエイリアスレコード。オプションで、ヘルスチェックを関連付けたり、ターゲットヘルス評価を設定したりすることもできます。以下のトピックは、各ルーティングポリシーとレコードタイプに必要な値に関する詳細情報を提供しており、Route 53 レコードを効果的に設定するのに役立ちます。

トピック

- すべてのルーティングポリシーに共通する値
- すべてのルーティングポリシーのエイリアスレコードに共通する値
- シンプルなレコードに固有の値
- シンプルなエイリアスレコードに固有の値

- フェイルオーバーレコードに固有の値
- フェイルオーバーエイリアスレコードに固有の値
- 位置情報レコードに固有の値
- 位置情報エイリアスレコードに固有の値
- 地理的近接性レコードに固有の値
- 地理的近接性エイリアスレコードに固有の値
- レイテンシーレコードに固有の値
- レイテンシーエイリアスレコードに固有の値
- IP ベースレコード特有の値
- IP ベースエイリアスレコードに特有の値
- 複数値回答レコードに固有の値
- 加重レコードに固有の値
- 加重エイリアスレコードに固有の値

すべてのルーティングポリシーに共通する値

これらは、Amazon Route 53 レコードを作成または編集するときに指定できる共通の値です。これらの値は、すべてのルーティングポリシーによって使用されます。

トピック

- レコード名
- 値/トラフィックのルーティング先
- TTL (秒)

レコード名

トラフィックをルーティングするドメインまたはサブドメインの名前を入力します。デフォルト値はホストゾーンの名前です。

> **Note**
>
> ホストゾーンと同じ名前のレコードを作成する場合は、[名前] フィールドに値 (@ 記号など) を入力しないでください。

CNAME レコード

[レコードタイプ] の値が [CNAME] のレコードを作成する場合、レコードの名前をホストゾーンの名前と同じにすることはできません。

特殊文字

a ~ z、0 ~ 9、- (ハイフン) 以外の文字を指定する方法、および国際化されたドメイン名を指定する方法については、「DNS ドメイン名の形式」を参照してください。

ワイルドカード文字

名前にはアスタリスク (*) を使用できます。DNSは、名前の中の位置に応じて、「*」をワイルドカードまたはアスタリスク (ASCII 42) として処理します。詳細については、「ホストゾーンおよびレコード名のアスタリスク (*) を使用する」を参照してください。

> **Important**
>
> 型が NS であるリソースレコードセットに対して * ワイルドカードを使用することはできません。

値/トラフィックのルーティング先

IP アドレス、またはレコードタイプに応じた別の値を選択します。[レコードタイプ] の値として適切な値を入力します。[CNAME] を除くすべてのタイプは、複数の値を入力できます。各値は個別の行に入力します。

A — IPv4 アドレス

IPv4 形式の IP アドレス。例えば、192.0.2.235。

AAAA — IPv6 アドレス

IPv6 の形式の IP アドレス。例えば、2001:0db8:85a3:0:0:8a2e:0370:7334。

CAA — 認証局の承認

[Record name] (レコード名) で指定されたドメインまたはサブドメインの証明書またはワイルドカード証明書を発行可能な認証機関を制御する、スペースで区切られた 3 つの値です。CAA レコードを使用して以下を指定できます。

- SSL/TLS 証明書を発行できる認証機関 (CA)

- CA がドメインまたはサブドメインの証明書を発行するときに連絡する電子メールアドレスまたは URL

CNAME — 正規名

Route 53 で、このレコードに対する DNS クエリに応答して返される完全修飾ドメイン名 (例えば、www.example.com)。末尾のドットはオプションです。Route 53 では、ドメイン名が完全修飾ドメイン名であると見なされます。つまり、Route 53 では、(末尾にドットのない) www.example.com と (末尾にドットのある) www.example.com. が同一と見なされます。

MX — メール交換

優先順位とメールサーバーを指定するドメイン名。例えば、10 mailserver.example.com。末尾のドットはオプションです。

NAPTR — 名前付け権限ポインタ

動的委任発見システム (DDDS) アプリケーションで、1 つの値を別の値に変換または置き換えるために使用される、スペースで区切られた 6 つの設定。詳細については、「NAPTR レコードタイプ」を参照してください。

PTR — ポインタ

Route 53 が返すように設定するドメイン名。

NS – ネームサーバー

ネームサーバーのドメイン名。例えば、ns1.example.com。

> **Note**
>
> 単純なルーティングポリシーのみで NS レコードを指定できます。

SPF — センダーポリシーフレームワーク

引用符で囲まれた SPF のレコード。例えば、"v=spf1 ip4:192.168.0.1/16-all"。SPF レコードは推奨されていません。詳細については、「サポートされる DNS レコードタイプ」を参照してください。

SRV — サービスロケーター

SRV レコード。SRV レコードは、メールや通信用のサービスなどのサービスにアクセスするために使用されます。SRV レコードの形式については、接続先のサービスのマニュアルを参照してください。末尾のドットはオプションとして扱われます。

SRV レコードの形式は次のとおりです。

[優先順位] [重み] [ポート] [サーバーのホスト名]

次に例を示します。

1 10 5269 xmpp-server.example.com。

TXT — テキスト

テキストレコード。テキストは引用符で囲みます。例えば、"Sample text entry"。

TTL (秒)

DNS 再帰リゾルバーがこのレコードに関する情報をキャッシュする秒単位の時間。より長い値 (172800 秒、2 日など) を指定した場合、DNS 再帰リゾルバーが Route 53 に対して行う必要がある呼び出しの数を減らします。これにより、レイテンシーが短縮され、Route 53 サービスの請求額が削減されます。詳細については、「Amazon Route 53 によりドメインのトラフィックをルーティングする方法」を参照してください。

ただし、TTL に長い値を指定すると、レコードの変更 (新しい IP アドレスなど) が有効になるまでに時間がかかります。再帰リゾルバーは、Route 53 に最新情報を要求する前に、キャッシュ内の値を長期間使用します。既に使用されているドメインまたはサブドメインの設定を変更する場合は、まず 300 秒などの短い値を指定し、新しい設定が正しいことを確認したら値を増やすことをお勧めします。

このレコードをヘルスチェックに関連付ける場合は、クライアントがヘルスステータスの変化に迅速に応答するように、TTL を 60 秒以下に指定することをお勧めします。

すべてのルーティングポリシーのエイリアスレコードに共通する値

これらは、Amazon Route 53 レコードを作成または編集するときに指定できる一般的なエイリアス値です。これらの値は、すべてのルーティングポリシーによって使用されます。

トピック

- レコード名
- への値/ルートトラフィック

レコード名

トラフィックをルーティングするドメインまたはサブドメインの名前を入力します。デフォルト値はホストゾーンの名前です。

> **Note**
>
> ホストゾーンと同じ名前のレコードを作成する場合は、[名前] フィールドに値 (@ 記号など) を入力しないでください。

CNAME レコード

[Type] (タイプ) の値が [CNAME] のレコードを作成する場合、レコードの名前をホストゾーンの名前と同じ名前にすることはできません。

CloudFront ディストリビューションと Amazon S3 バケットへのエイリアス

指定する値は、トラフィックをルーティングする AWS リソースによって異なります。

- CloudFront ディストリビューション – ディストリビューションには、レコードの名前と一致する代替ドメイン名が含まれる必要があります。例えば、レコード名が acme.example.com の場合、CloudFront ディストリビューションには代替ドメイン名の 1 つとして acme.example.com が含まれる必要があります。詳細については、Amazon CloudFront デベロッパーガイドの「代替ドメイン名 (CNAME) を使用する」を参照してください。
- Amazon S3 バケット – レコード名は、Amazon S3 バケット名と一致する必要があります。例えば、 バケット名が [acme.example.com] である場合、このレコード名も [acme.example.com] である必要があります。

また、ウェブサイトホスティング用にバケットを設定する必要があります。詳細については、Amazon Simple Storage Service ユーザーガイドのウェブサイトホスティング用にバケットを設定するを参照してください。

特殊文字

a～z、0～9、- (ハイフン) 以外の文字を指定する方法、および国際化されたドメイン名を指定する方法については、「DNS ドメイン名の形式」を参照してください。

ワイルドカード文字

名前にはアスタリスク (*) を使用できます。DNSは、名前の中の位置に応じて、「*」をワイルドカードまたはアスタリスク (ASCII 42) として処理します。詳細については、「ホストゾーンおよびレコード名のアスタリスク (*) を使用する」を参照してください。

への値/ルートトラフィック

リストから選択する値、または フィールドに入力する値は、トラフィックをルーティングする AWS リソースによって異なります。

特定の AWS リソースにトラフィックをルーティングするように Route 53 を設定する方法の詳細については、「」を参照してくださいAWS リソースへのインターネットトラフィックのルーティング。

Important

同じ AWS アカウントを使用してホストゾーンとトラフィックをルーティングするリソースを作成し、リソースがエンドポイントリストに表示されない場合は、以下を確認してください。

- [レコードタイプ] でサポートされている値を選択したことを確認します。サポートされている値は、トラフィックのルーティング先のリソースに固有です。例えば、S3 バケットにトラフィックをルーティングするには、[レコードタイプ] として [A — IPv4 アドレス] を選択する必要があります。
- アカウントに、該当するリソースを一覧表示するために必要な IAM アクセス許可があることを確認します。例えば、CloudFront ディストリビューションを [エンドポイント] リストに表示するためには、アカウントが次のアクションを実行するアクセス許可を持っている必要があります: `cloudfront:ListDistributions`。

IAM ポリシーの例については、「Amazon Route 53 コンソールを使用するために必要なアクセス許可」を参照してください。

異なる AWS アカウントを使用してホストゾーンとリソースを作成した場合、エンドポイントリストにはリソースは表示されません。[エンドポイント] に入力する値を決定するには、リソースタイプに関する次のドキュメントを参照してください。

API Gateway のカスタムリージョン API とエッジ最適化 API

API Gateway のカスタムリージョン API とエッジ最適化 API で、次のいずれかを行います。

- 同じアカウントを使用して、Route 53 ホストゾーンと API を作成した場合 – [エンドポイント] を選択し、リストから API を選択します。API が多数ある場合は、API エンドポイントの最初の数文字を入力してリストをフィルタリングすることができます。

  > **Note**
  >
  > このレコードの名前は、API のカスタムドメイン名 (例: api.example.com) と一致している必要があります。

- 別のアカウントを使用して、Route 53 ホストゾーンと API を作成した場合 – API の API エンドポイント (例: api.example.com) を入力します。

  1 つの AWS アカウントを使用して現在のホストゾーンを作成し、別のアカウントを使用して API を作成した場合、API は API Gateway APIs のエンドポイントリストに表示されません。

  1 つのアカウントを使用して現在のホストゾーンを作成し、すべての API を作成するのに 1 つ以上の別のアカウントを使用した場合、[エンドポイント] リストの [API Gateway API] に「No targets available」と表示されます。詳細については、「ドメイン名を使用してトラフィックを Amazon API Gateway の API にルーティングする」を参照してください。

CloudFront ディストリビューション

CloudFront ディストリビューションの場合は、次のいずれかの操作を実行します。

- Route 53 ホストゾーンと CloudFront ディストリビューションを作成する際に同じアカウントを使用している場合 – [エンドポイント] を選択し、リストからディストリビューションを選択します。ディストリビューションが多数ある場合は、ディストリビューションのドメイン名の最初の数文字を入力することでリストをフィルタ処理できます。

ディストリビューションがリストに表示されていない場合は、次の点を確認してください。

- このレコードの名前は、ディストリビューションの代替ドメイン名に一致する必要があります。
- ディストリビューションに代替ドメイン名を追加したばかりの場合、変更がすべての CloudFront エッジロケーションに反映されるまでに 15 分かかることがあります。変更が伝達されるまで、Route 53 は新しい代替ドメイン名を認識できません。

- Route 53 ホストゾーンとディストリビューションを作成する際に異なるアカウントを使用している場合 – ディストリビューションの CloudFront ドメイン名を入力します (例えば、d111111abcdef8.cloudfront.net)。

  1 つの AWS アカウントを使用して現在のホストゾーンを作成し、別のアカウントを使用してディストリビューションを作成した場合、ディストリビューションはエンドポイントリストに表示されません。

  1 つのアカウントを使用して現在のホストゾーンを作成し、1 つ以上の別のアカウントを使用してすべてのディストリビューションを作成した場合 、[エンドポイント] リストの [CloudFront ディストリビューション] に「No targets available」と表示されます。

> **Important**
>
> すべてのエッジロケーションに伝達されていない CloudFront ディストリビューションにクエリをルーティングしないでください。その場合、ユーザーは該当するコンテンツにアクセスできません。

CloudFront ディストリビューションには、レコードの名前と一致する代替ドメイン名が含まれる必要があります。例えば、レコード名が acme.example.com の場合、CloudFront ディストリビューションには代替ドメイン名の 1 つとして acme.example.com が含まれる必要があります。詳細については、Amazon CloudFront デベロッパーガイドの「代替ドメイン名 (CNAME) を使用する」を参照してください。

ディストリビューションに対して IPv6 が有効になっている場合は、2 つのレコードを作成します。1 つは [レコードタイプ] として [A — IPv4 アドレス]の値を持つもの、もう 1 つは [AAAA IPv6 — アドレス] の値を持つものとします。詳細については、「ドメイン名を使用したトラフィックの Amazon CloudFront ディストリビューションへのルーティング」を参照してください。

App Runner サービス

App Runner サービスで、次のいずれかの操作を行います。

- 同じアカウントを使用して Route 53 ホストゾーンと App Runner サービスを作成した場合は、を選択し AWS リージョン、リストからトラフィックをルーティングする環境のドメイン名を選択します。
- 異なるアカウントを使用して Route 53 ホストゾーンと App Runner を作成した場合 – カスタムドメイン名を入力します。詳細については、「Managing custom domain names for App Runner」(App Runner サービスでのカスタムドメイン名の管理) を参照してください。

  1 つの AWS アカウントを使用して現在のホストゾーンを作成し、別のアカウントを使用して App Runner を作成した場合、App Runner はエンドポイントリストに表示されません。

詳細については、「Amazon Route 53 での App Runner サービスに対するトラフィックのルーティングの設定」を参照してください。

ローカル化されたサブドメインがある Elastic Beanstalk 環境

Elastic Beanstalk 環境のドメイン名に環境をデプロイしたリージョンが含まれている場合、トラフィックを環境にルーティングするエイリアスレコードを作成できます。たとえば、ドメイン名 `my-environment.us-west-2.elasticbeanstalk.com` はローカル化されたドメイン名です。

> **Important**
>
> 2016 年の初めよりも前に作成された環境の場合、ドメイン名にはリージョンは含まれていません。これらの環境にトラフィックをルーティングするには、エイリアスレコードの代わりに CNAME レコードを作成する必要があります。ルートドメイン名に対して CNAME レコードを作成することはできないことに注意してください。例えば、ドメイン名が example.com の場合、acme.example.com のトラフィックを Elastic Beanstalk 環境にルーティングするレコードは作成できますが、example.com のトラフィックを Elastic Beanstalk 環境にルーティングするレコードは作成できません。

ローカル化されたサブドメインがある Elastic Beanstalk 環境の場合は、次のいずれかを実行します。

- Route 53 ホストゾーンと Elastic Beanstalk 環境を作成する際に同じアカウントを使用している場合 – [エンドポイント] を選択し、リストから環境を選択します。環境が多数ある場合は、環境の CNAME 属性の最初の数文字を入力することでリストをフィルタ処理できます。

- 別のアカウントを使用して、Route 53 ホストゾーンと Elastic Beanstalk 環境を作成した場合—Elastic Beanstalk 環境の CNAME 属性を入力します。

詳細については、「AWS Elastic Beanstalk 環境へのトラフィックのルーティング」を参照してください。

ELB ロードバランサー

ELB ロードバランサーの場合は、次のいずれかの操作を実行します。

- Route 53 ホストゾーンとロードバランサーを作成する際に同じアカウントを使用している場合 – [エンドポイント] を選択し、リストからロードバランサーを選択します。ロードバランサーが多数ある場合は、DNS 名の最初の数文字を入力することでリストをフィルタ処理できます。
- Route 53 ホストゾーンとロードバランサーを作成する際に異なるアカウントを使用している場合 – 「Elastic Load Balancing ロードバランサーの DNS 名を取得する」の手順で取得した値を入力します。

  1 つの AWS アカウントを使用して現在のホストゾーンを作成し、別のアカウントを使用してロードバランサーを作成した場合、ロードバランサーはエンドポイントリストに表示されません。

  1 つのアカウントを使用して現在のホストゾーンを作成し、すべてのロードバランサーを作成するのに 1 つ以上の別のアカウントを使用した場合、[エンドポイント] リストの [Elastic Load Balancers] に「No targets available」と表示されます。

コンソールは、別のアカウントのアプリケーションと Classic Load Balancer に dualstack. を付加します。ウェブブラウザなどのクライアントが、ドメイン名 (example.com) またはサブドメイン名 (www.example.com) の IP アドレスをリクエストする場合、クライアントは IPv4 アドレス (A レコード)、IPv6 アドレス (AAAA レコード)、または IPv4 アドレスと IPv6 アドレスの両方を (別のリクエストで) リクエストできます。[dualstack.] の指定により、Route 53 は、クライアントがリクエストした IP アドレス形式に基づいて、ロードバランサーに対する適切な IP アドレスで応答することができます。

詳細については、「ELB ロードバランサーへのトラフィックのルーティング」を参照してください。

AWS Global Accelerator アクセラレーター

AWS Global Accelerator アクセラレーターの場合は、アクセラレーターの DNS 名を入力します。現在のアカウントまたは別の AWS アカウントを使用して作成したアクセラレーターの DNS 名を入力できます AWS 。

Amazon S3 バケット

ウェブサイトエンドポイントとして設定された Amazon S3 バケットの場合、次のいずれかを実行します。

- Route 53 ホストゾーンと Amazon S3 バケットを作成する際に同じアカウントを使用している場合 – [エンドポイント] を選択し、リストからバケットを選択します。バケットが多数ある場合は、DNS 名の最初の数文字を入力することでリストをフィルタ処理できます。

  [エンドポイント] の値は、バケットの Amazon S3 ウェブサイトエンドポイントに変わります。
- 別のアカウントを使用して、Route 53 ホストゾーンと Amazon S3 bucket を作成した場合 – S3 バケットを作成したリージョンの名前を入力します。Amazon Web Services 全般のリファレンス の「Amazon S3 ウェブサイトのエンドポイント」にアクセスし、表にあるウェブサイトのエンドポイント列の値を使用します。

  現在の AWS アカウント以外のアカウントを使用して Amazon S3 バケットを作成した場合、バケットはエンドポイントリストに表示されません。

ウェブサイトホスティング用にバケットを設定する必要があります。詳細については、Amazon Simple Storage Service ユーザーガイドのウェブサイトホスティング用にバケットを設定するを参照してください。

レコード名は、Amazon S3 バケット名と一致する必要があります。例えば、Amazon S3 バケット名が [acme.example.com] である場合、このレコード名も [acme.example.com] である必要があります。

加重エイリアス、レイテンシーエイリアス、フェイルオーバーエイリアス、または位置情報エイリアスのレコードのグループの中には、Amazon S3 バケットにクエリをルーティングするレコードを 1 つだけ作成できます。これは、レコード名はバケット名と一致する必要があり、バケット名はグローバルに一意である必要があるためです。

Amazon OpenSearch Service

OpenSearch Service で、次のいずれかの操作を行います。

- OpenSearch Service カスタムドメイン: レコードの名前はカスタムドメインの名前と一致する必要があります。例えば、カスタムドメイン名が [test.example.com] である場合、このレコード名も [test.example.com] である必要があります。
- 同じアカウントを使用して Route 53 ホストゾーンと OpenSearch Service ドメインを作成した場合は、 を選択し AWS リージョン、ドメイン名を選択します。

- 異なるアカウントを使用して Route 53 ホストゾーンと OpenSearch Service を作成した場合 – カスタムドメイン名を入力します。詳細については、「カスタムエンドポイントを作成する」を参照してください。

  1 つの AWS アカウントを使用して現在のホストゾーンを作成し、別のアカウントを使用して OpenSearch Service ドメインを作成した場合、そのドメインはエンドポイントリストに表示されません。

  1 つのアカウントを使用して現在のホストゾーンを作成し、すべての OpenSearch Service ドメインを作成するのに 1 つ以上の別のアカウントを使用した場合、[エンドポイント] リストの [OpenSearch Service] に「No targets available」と表示されます。

詳細については、「Amazon Route 53 を Amazon OpenSearch Service ドメインエンドポイントにルーティングする Amazon Route 53 の設定」を参照してください。

Amazon VPC インターフェイスのエンドポイント

Amazon VPC インターフェイスエンドポイントで、以下のいずれかを行います。

- Route 53 ホストゾーンとインターフェイスエンドポイントを作成する際に同じアカウントを使用している場合 – [エンドポイント] を選択し、リストからインターフェイスエンドポイントを選択します。インターフェイスエンドポイントが多数ある場合は、DNS ホスト名の最初の数文字を入力することでリストをフィルタリングすることができます。
- 別のアカウントを使用して Route 53 ホストゾーンとインターフェイスエンドポイントを作成した場合 – インターフェイスエンドポイントの DNS ホスト名 (例: vpce-123456789abcdef01-example-us-east-1a.elasticloadbalancing.us-east-1.vpce.amazonaws.com) を入力します。

  1 つの AWS アカウントを使用して現在のホストゾーンを作成し、別のアカウントを使用してインターフェイスエンドポイントを作成した場合、インターフェイスエンドポイントは VPC エンドポイントのエンドポイントリストに表示されません。

  1 つのアカウントを使用して現在のホストゾーンを作成し、すべてのインターフェイスエンドポイントを作成するのに 1 つ以上の別のアカウントを使用した場合、[エンドポイント] リストの [VPC エンドポイント] に「No targets available」と表示されます。

  詳細については、「ドメイン名を使用してトラフィックを Amazon Virtual Private Cloud インターフェイスエンドポイントにルーティングする」を参照してください。

このホストゾーン内のレコード

このホストゾーン内のレコードの場合は、[エンドポイント] を選択し、該当するレコードを選択します。レコードが多数ある場合は、名前の最初の数文字を入力することでリストをフィルタ処理できます。

ホストゾーンにデフォルトの NS および SOA レコードのみが含まれる場合、[エンドポイント] リストには「No targets available」と表示されます。

> **Note**
>
> ホストゾーン ([zone apex] といいます) と同じ名前のエイリアスレコードを作成する場合、[レコードタイプ] の値が [CNAME] のレコードは選択できません。これは、トラフィックがルーティングされているレコードとエイリアスレコードのタイプが同じでなければならず、Zone Apex の CNAME レコードの作成はエイリアスレコードであってもサポートされていないためです。

シンプルなレコードに固有の値

シンプルなレコードを作成するときは、以下の値を指定します。

トピック

- ルーティングポリシー
- レコード名
- 値/トラフィックのルーティング先
- レコードタイプ
- TTL (秒)

ルーティングポリシー

[Simple routing] (シンプルルーティング) を選択します。

レコード名

トラフィックをルーティングするドメインまたはサブドメインの名前を入力します。デフォルト値はホストゾーンの名前です。

> **Note**
>
> ホストゾーンと同じ名前のレコードを作成する場合は、[名前] フィールドに値 (@ 記号など) を入力しないでください。

レコード名の詳細については、レコード名 を参照してください。

値/トラフィックのルーティング先

IP アドレス、またはレコードタイプに応じた別の値を選択します。[レコードタイプ] の値として適切な値を入力します。[CNAME] を除くすべてのタイプは、複数の値を入力できます。各値は個別の行に入力します。

次の値にトラフィックをルーティングするか、次の値を指定できます。

- A — IPv4 アドレス
- AAAA — IPv6 アドレス
- CAA —認証局の承認

- CNAME — 正規名
- MX — メール交換
- NAPTR — 名前付け権限ポインタ
- NS – ネームサーバー

  ネームサーバーのドメイン名。例えば、ns1.example.com。

  > **Note**
  >
  > 単純なルーティングポリシーのみで NS レコードを指定できます。

- PTR — ポインタ
- SPF — センダーポリシーフレームワーク
- SRV — サービスロケーター
- TXT — テキスト

上記の値の詳細については、「common values for Value/Route traffic to」(値/トラフィックのルーティング先) を参照してください。

レコードタイプ

DNS レコードタイプ。詳細については、「サポートされる DNS レコードタイプ」を参照してください。

Route 53 が DNS クエリに応答する方法に基づいて、レコードタイプの値を選択します。

TTL (秒)

DNS 再帰リゾルバーがこのレコードに関する情報をキャッシュする秒単位の時間。より長い値 (172800 秒、2 日など) を指定した場合、DNS 再帰リゾルバーが Route 53 に対して行う必要がある呼び出しの数を減らします。これにより、レイテンシーが短縮され、Route 53 サービスの請求額が削減されます。詳細については、「Amazon Route 53 によりドメインのトラフィックをルーティングする方法」を参照してください。

ただし、TTL に長い値を指定すると、レコードの変更 (新しい IP アドレスなど) が有効になるまでに時間がかかります。再帰リゾルバーは、Route 53 に最新情報を要求する前に、キャッシュ内の値を長期間使用します。既に使用されているドメインまたはサブドメインの設定を変更する場合は、まず 300 秒などの短い値を指定し、新しい設定が正しいことを確認したら値を増やします。

シンプルなエイリアスレコードに固有の値

エイリアスレコードを作成するときは、以下の値を指定します。詳細については、「エイリアスレコードと非エイリアスレコードの選択」を参照してください。

> **Note**
>
> で Route 53 を使用している場合 AWS GovCloud (US) Region、この機能にはいくつかの制限があります。詳細については、AWS GovCloud (US) ユーザーガイドの Amazon Route 53 のページを参照してください。

トピック

- ルーティングポリシー
- レコード名
- への値/ルートトラフィック
- レコードタイプ
- ターゲットの正常性の評価

ルーティングポリシー

[Simple routing] (シンプルルーティング) を選択します。

レコード名

トラフィックをルーティングするドメインまたはサブドメインの名前を入力します。デフォルト値はホストゾーンの名前です。

> **Note**
>
> ホストゾーンと同じ名前のレコードを作成する場合は、[名前] フィールドに値 (@ 記号など) を入力しないでください。

レコード名の詳細については、レコード名 を参照してください。

への値/ルートトラフィック

リストから選択する値、または フィールドに入力する値は、トラフィックをルーティングする AWS リソースによって異なります。

ターゲットにできる AWS リソースの詳細については、値/ルートトラフィックのエイリアスレコードの一般的な値を参照してください。

特定の AWS リソースにトラフィックをルーティングするように Route 53 を設定する方法の詳細については、「」を参照してくださいAWS リソースへのインターネットトラフィックのルーティング。

レコードタイプ

DNS レコードタイプ。詳細については、「サポートされる DNS レコードタイプ」を参照してください。

トラフィックをルーティングする AWS リソースに基づいて、該当する値を選択します。

API Gateway のカスタムリージョン API またはエッジ最適化 API

[A — IPv4 アドレス] を選択します。

Amazon VPC インターフェイスのエンドポイント

[A — IPv4 アドレス] を選択します。

CloudFront 配信

[A — IPv4 アドレス] を選択します。

ディストリビューションに対して IPv6 が有効になっている場合は、2 つのレコードを作成します。1 つは [タイプ] として [A — IPv4 アドレス] の値を持つもの、もう 1つは [AAAA — IPv6 アドレス] の値を持つものとします。

App Runner サービス

[A — IPv4 アドレス] を選択します。

ローカル化されたサブドメインがある Elastic Beanstalk 環境

[A — IPv4 アドレス] を選択します。

ELB ロードバランサー

[A — IPv4 アドレス] または [AAAA — IPv6 アドレス] を選択します。

Amazon S3 バケット

[A — IPv4 アドレス] を選択します。

OpenSearch Service

[A — IPv4 アドレス] または [AAAA — IPv6 アドレス] を選択します。

このホストゾーン内の別のレコード

エイリアスを作成するレコードのタイプを選択します。[NS] および [SOA] 以外のすべてのタイプがサポートされます。

> **Note**
>
> ホストゾーン (Zone Apex といいます) と同じ名前のエイリアスレコードを作成する場合、[タイプ] の値が [CNAME] のレコードにトラフィックをルーティングすることはできません。これは、トラフィックがルーティングされているレコードとエイリアスレコードのタイプが同じでなければならず、zone apex の CNAME レコードの作成はエイリアスレコードであってもサポートされていないためです。

ターゲットの正常性の評価

[Routing policy] (ルーティングポリシー) の値が [Simple] (シンプル) の場合、[No] (いいえ) またはデフォルトの [Yes] (はい) を選択できます。[Evaluate target health] (ターゲットヘルスを評価) は、[Simple] (シンプル) ルーティングに一切影響を及ぼさないためです。指定の名前とタイプのレコードが 1 つのみの場合、Route 53 は、ソースが正常かどうかに関係なく、そのレコードの値を使用して DNS クエリに応答します。

他のルーティングポリシーの場合、ターゲットヘルスの評価は、エイリアスレコードが参照するリソースのヘルスを Route 53 がチェックするかどうかを決定します。

- ターゲットヘルスの評価が運用上の利点を提供するサービス: ロードバランサー (ELB) とロードバランサーを使用する AWS Elastic Beanstalk 環境の場合、ターゲットヘルスの評価を「はい」に設定すると、Route 53 は異常なリソースからトラフィックをルーティングできます。
- 高可用性サービス: Amazon S3 バケット、VPC インターフェイスエンドポイント、Amazon API Gateway、Amazon OpenSearch Service AWS Global Accelerator、Amazon VPC Lattice などのサービスの場合、ターゲットヘルスの評価は高可用性のために設計されているため、運用上の利点はありません。これらのサービスのフェイルオーバーシナリオでは、代わりに Route 53 ヘルスチェックを使用します。

さまざまな AWS のサービスでターゲットヘルスを評価する方法の詳細については、 API リファレンスのEvaluateTargetHealth ドキュメント」を参照してください。

フェイルオーバーレコードに固有の値

フェイルオーバーレコードを作成するときは、以下の値を指定します。

> **Note**
>
> プライベートホストゾーンでのフェイルオーバーレコードの作成については、「プライベートホストゾーンのフェイルオーバーの設定」を参照してください。

トピック

- ルーティングポリシー
- レコード名
- レコードタイプ
- TTL (秒)
- 値/トラフィックのルーティング先
- フェイルオーバーレコードタイプ
- ヘルスチェック
- 記録 ID

ルーティングポリシー

[フェイルオーバー] を選択します。

レコード名

トラフィックをルーティングするドメインまたはサブドメインの名前を入力します。デフォルト値はホストゾーンの名前です。

> **Note**
>
> ホストゾーンと同じ名前のレコードを作成する場合は、[レコード名] フィールドに値 (@ 記号など) を入力しないでください。

フェイルオーバーレコードのグループで、両方のレコードに同じ名前を入力します。

レコード名の詳細については、レコード名 を参照してください。

レコードタイプ

DNS レコードタイプ。詳細については、「サポートされる DNS レコードタイプ」を参照してください。

プライマリフェイルオーバーレコードとセカンダリフェイルオーバーレコードの両方に同じ値を選択してください。

TTL (秒)

DNS 再帰リゾルバーがこのレコードに関する情報をキャッシュする秒単位の時間。より長い値 (172,800 秒、2 日など) を指定した場合、DNS 再帰リゾルバーが Route 53 に対して行う必要がある呼び出しの数を減らします。これにより、レイテンシーが短縮され、Route 53 サービスの請求額が削減されます。詳細については、「Amazon Route 53 によりドメインのトラフィックをルーティングする方法」を参照してください。

ただし、TTL に長い値を指定すると、レコードの変更 (新しい IP アドレスなど) が有効になるまでに時間がかかります。再帰リゾルバーは、Route 53 に最新情報を要求する前に、キャッシュ内の値を長期間使用します。既に使用されているドメインまたはサブドメインの設定を変更する場合は、まず 300 秒などの短い値を指定し、新しい設定が正しいことを確認したら値を増やします。

このレコードをヘルスチェックに関連付ける場合は、クライアントがヘルスステータスの変化に迅速に応答するように、TTL を 60 秒以下に指定します。

値/トラフィックのルーティング先

IP アドレス、またはレコードタイプに応じた別の値を選択します。[レコードタイプ] の値として適切な値を入力します。[CNAME] を除くすべてのタイプは、複数の値を入力できます。各値は個別の行に入力します。

次の値にトラフィックをルーティングするか、次の値を指定できます。

- A — IPv4 アドレス
- AAAA — IPv6 アドレス
- CAA —認証局の承認
- CNAME — 正規名
- MX — メール交換
- NAPTR — 名前付け権限ポインタ

- PTR — ポインタ
- SPF — センダーポリシーフレームワーク
- SRV — サービスロケーター
- TXT — テキスト

上記の値の詳細については、「common values for Value/Route traffic to」(値/トラフィックのルーティング先) を参照してください。

フェイルオーバーレコードタイプ

このレコードに該当する値を選択します。フェイルオーバーが正常に動作するためには、プライマリフェイルオーバーレコードを 1 つとセカンダリフェイルオーバーレコードを 1 つ作成する必要があります。

[レコード名] および [レコードタイプ] の値がフェイルオーバーレコードと同じである非フェイルオーバーレコードを作成することはできません。

ヘルスチェック

Route 53 で、指定されたエンドポイントの正常性をチェックし、エンドポイントが正常であるときにのみ、このレコードを使用して DNS クエリに応答する場合は、ヘルスチェックを選択します。

Route 53 は、レコード内で指定されたエンドポイント、例えば、[値] フィールドの IP アドレスで指定されたエンドポイントの正常性はチェックしません。Route 53 は、レコードのヘルスチェックを選択したとき、ヘルスチェックで指定されたエンドポイントの正常性をチェックします。エンドポイントが正常であるかどうかを、Route 53 がどのように判断するかについては、「Amazon Route 53 でヘルスチェックの正常性を判断する方法」を参照してください。

ヘルスチェックとレコードの関連付けは、Route 53 が DNS クエリに応答するレコードを 2 つ以上選択していて、Route 53 がヘルスチェックのステータスに部分的に基づいている場合にのみ便利です。以下の設定でのみ、ヘルスチェックを使用してください。

- 名前、種類、およびルーティングポリシー (フェイルオーバーレコードや加重レコードなど) が同じレコードのグループ内のすべてのレコードのヘルスをチェックし、すべてのレコードのヘルスチェック ID を指定します。レコードのヘルスチェックが正常ではないエンドポイントを特定した場合、Route 53 はそのレコードの値を使用してクエリへの応答を停止します。
- フェイルオーバーエイリアス、位置情報エイリアス、レイテンシーエイリアス、IP ベースエイリアス、または加重エイリアスレコードのグループ内にあるエイリアスレコードまたはレコード

の [Evaluate target health] (ターゲットのヘルスを評価) で、[Yes] (はい) を選択します。エイリアスレコードが同じホストゾーン内の非エイリアスレコードを参照する場合、参照先レコードのヘルスチェックも指定する必要があります。エイリアスレコードにヘルスチェックを関連付けた上で、[Evaluate Target Health] (ターゲットの正常性の評価) で [Yes] (はい) を選択した場合、これらの設定は両方とも有効になります。詳細については、「エイリアスレコードにヘルスチェックを関連付けるとどうなるか」を参照してください。

ヘルスチェックでエンドポイントをドメイン名でのみ指定する場合は、エンドポイントごとに個別のヘルスチェックを作成します。例えば、www.example.com のコンテンツを配信する各 HTTP サーバーについて、ヘルスチェックを作成します。[ドメイン名] の値には、レコードの名前 (example.com) ではなく、サーバーのドメイン名 (us-east-2-www.example.com など) を指定します。

> **Important**
>
> この構成で、[ドメイン名] の値がレコードの名前と一致するヘルスチェックを作成し、それらのレコードにヘルスチェックを関連付けた場合、ヘルスチェックで予想できない結果が生じます。

記録 ID

プライマリレコードとセカンダリレコードを一意に識別する値を入力します。

フェイルオーバーエイリアスレコードに固有の値

フェイルオーバーエイリアスレコードを作成するときは、以下の値を指定します。

詳細については、以下のトピックを参照してください。

- プライベートホストゾーンでのフェイルオーバーレコードの作成については、「プライベートホストゾーンのフェイルオーバーの設定」を参照してください。
- エイリアスレコードの詳細については、「エイリアスレコードと非エイリアスレコードの選択」を参照してください。

トピック

- ルーティングポリシー
- レコード名
- レコードタイプ
- 値/トラフィックのルーティング先
- フェイルオーバーレコードタイプ
- ヘルスチェック
- ターゲットの正常性の評価
- 記録 ID

ルーティングポリシー

[フェイルオーバー] を選択します。

レコード名

トラフィックをルーティングするドメインまたはサブドメインの名前を入力します。デフォルト値はホストゾーンの名前です。

> **Note**
>
> ホストゾーンと同じ名前のレコードを作成する場合は、[レコード名] フィールドに値 (@ 記号など) を入力しないでください。

フェイルオーバーレコードのグループで、両方のレコードに同じ名前を入力します。

レコード名の詳細については、レコード名 を参照してください。

レコードタイプ

DNS レコードタイプ。詳細については、「サポートされる DNS レコードタイプ」を参照してください。

トラフィックをルーティングする AWS リソースに基づいて、該当する値を選択します。プライマリフェイルオーバーレコードとセカンダリフェイルオーバーレコードの両方に同じ値を選択してください。

API Gateway のカスタムリージョン API またはエッジ最適化 API

[A — IPv4 アドレス] を選択します。

Amazon VPC インターフェイスのエンドポイント

[A — IPv4 アドレス] を選択します。

CloudFront 配信

[A — IPv4 アドレス] を選択します。

ディストリビューションに対して IPv6 が有効になっている場合は、2 つのレコードを作成します。1 つは [タイプ] として [A — IPv4 アドレス] の値を持つもの、もう 1つは [AAAA — IPv6 アドレス] の値を持つものとします。

App Runner サービス

[A — IPv4 アドレス] を選択します。

ローカル化されたサブドメインがある Elastic Beanstalk 環境

[A — IPv4 アドレス] を選択します。

ELB ロードバランサー

[A — IPv4 アドレス] または [AAAA — IPv6 アドレス] を選択します。

Amazon S3 バケット

[A — IPv4 アドレス] を選択します。

OpenSearch Service

[A — IPv4 アドレス] または [AAAA — IPv6 アドレス] を選択します。

このホストゾーン内の別のレコード

エイリアスを作成するレコードのタイプを選択します。[NS] および [SOA] 以外のすべてのタイプがサポートされます。

> **Note**
>
> ホストゾーン (Zone Apex といいます) と同じ名前のエイリアスレコードを作成する場合、[タイプ] の値が [CNAME] のレコードにトラフィックをルーティングすることはできません。これは、トラフィックがルーティングされているレコードとエイリアスレコードのタイプが同じでなければならず、Zone Apex の CNAME レコードの作成はエイリアスレコードであってもサポートされていないためです。

値/トラフィックのルーティング先

リストから選択する値、または フィールドに入力する値は、トラフィックをルーティングする AWS リソースによって異なります。

ターゲットにできる AWS リソースの詳細については、値/ルートトラフィックのエイリアスレコードの一般的な値を参照してください。

特定の AWS リソースにトラフィックをルーティングするように Route 53 を設定する方法の詳細については、「」を参照してくださいAWS リソースへのインターネットトラフィックのルーティング。

> **Note**
>
> プライマリフェイルオーバーレコードとセカンダリフェイルオーバーレコードを作成する場合、オプションで、 [名前] および [レコードタイプ] が同じ値のフェイルオーバーレコードを 1 つとフェイルオーバーエイリアスレコードを 1 つ作成できます。フェイルオーバーレコードとフェイルオーバーエイリアスレコードを混在させる場合、いずれかをプライマリレコードにすることができます。

フェイルオーバーレコードタイプ

このレコードに該当する値を選択します。フェイルオーバーが正常に動作するためには、プライマリフェイルオーバーレコードを 1 つとセカンダリフェイルオーバーレコードを 1 つ作成する必要があります。

[レコード名] および [レコードタイプ] の値がフェイルオーバーレコードと同じである非フェイルオーバーレコードを作成することはできません。

ヘルスチェック

Route 53 で、指定されたエンドポイントの正常性をチェックし、エンドポイントが正常であるときにのみ、このレコードを使用して DNS クエリに応答する場合は、ヘルスチェックを選択します。

Route 53 は、レコード内で指定されたエンドポイント、例えば、[値] フィールドの IP アドレスで指定されたエンドポイントの正常性はチェックしません。Route 53 は、レコードのヘルスチェックを選択したとき、ヘルスチェックで指定されたエンドポイントの正常性をチェックします。エンドポイントが正常であるかどうかを、Route 53 がどのように判断するかについては、「Amazon Route 53 でヘルスチェックの正常性を判断する方法」を参照してください。

ヘルスチェックをレコードに関連付けることに意味があるのは、Route 53 が複数のレコードの中から選択して DNS クエリに応答しており、その選択の一部をヘルスチェックのステータスに基づいて行うように Route 53 を設定する必要がある場合だけです。以下の設定でのみ、ヘルスチェックを使用してください。

- 名前、種類、およびルーティングポリシー (フェイルオーバーレコードや加重レコードなど) が同じレコードのグループ内のすべてのレコードのヘルスをチェックし、すべてのレコードのヘルスチェック ID を指定します。レコードのヘルスチェックが正常ではないエンドポイントを特定した場合、Route 53 はそのレコードの値を使用してクエリへの応答を停止します。
- フェイルオーバーエイリアス、位置情報エイリアス、レイテンシーエイリアス、IP ベースエイリアス、または加重エイリアスレコードのグループ内にあるエイリアスレコードまたはレコードの [Evaluate target health] (ターゲットのヘルスを評価) で、[Yes] (はい) を選択します。エイリアスレコードが同じホストゾーン内の非エイリアスレコードを参照する場合、参照先レコードのヘルスチェックも指定する必要があります。エイリアスレコードにヘルスチェックを関連付けた上で、[Evaluate Target Health] (ターゲットの正常性の評価) で [Yes] (はい) を選択した場合、これらの設定は両方とも有効になります。詳細については、「エイリアスレコードにヘルスチェックを関連付けるとどうなるか」を参照してください。

ヘルスチェックでドメイン名によってのみエンドポイントを指定する場合、エンドポイントごとにヘルスチェックを作成することをお勧めします。例えば、www.example.com のコンテンツを配信する各 HTTP サーバーについて、ヘルスチェックを作成します。[ドメイン名] の値には、レコードの名前 (example.com) ではなく、サーバーのドメイン名 (us-east-2-www.example.com など) を指定します。

> **Important**
>
> この構成で、[ドメイン名] の値がレコードの名前と一致するヘルスチェックを作成し、それらのレコードにヘルスチェックを関連付けた場合、ヘルスチェックで予想できない結果が生じます。

ターゲットの正常性の評価

Route 53 で、このレコードを使用して [エンドポイント] で指定されたリソースの正常性を確認することによって DNS クエリに応答するかどうかを判定する場合は、[Yes] を選択します。

次の点に注意してください。

API Gateway のカスタムリージョン API とエッジ最適化 API

エンドポイントが API Gateway カスタムリージョン API またはエッジ最適化 API である場合、[ターゲットの正常性の評価] を [Yes] に設定するための特別な要件はありません。

CloudFront ディストリビューション

エンドポイントが CloudFront ディストリビューションの場合、[ターゲットの正常性の評価] を [Yes] に設定することはできません。

ローカル化されたサブドメインがある Elastic Beanstalk 環境

[エンドポイント] で Elastic Beanstalk 環境を指定し、その環境に ELB ロードバランサーが含まれている場合、Elastic Load Balancing はクエリをロードバランサーに登録されている正常な Amazon EC2 インスタンスにのみルーティングします。(複数の Amazon EC2 インスタンスが含まれている場合、環境には自動的に ELB ロードバランサーが含まれます。) [ターゲットの正常性の評価] を [Yes] に設定したとき、正常な Amazon EC2 インスタンスがない場合やロードバランサー自体が正常でない場合、Route 53 は他に利用可能なリソースがあれば、そこにクエリをルーティングします。

環境に 1 つの Amazon EC2 インスタンスが含まれている場合、特別な要件はありません。

ELB ロードバランサー

ヘルスチェックの動作はロードバランサーのタイプによって異なります。

- [Classic Load Balancers] – [エンドポイント] で ELB Classic Load Balancer を指定した場合、Elastic Load Balancing は、ロードバランサーに登録されている正常な Amazon EC2 インスタンスにのみクエリをルーティングします。[ターゲットの正常性の評価] を [Yes] に設

定したとき、正常な EC2 インスタンスがない場合やロードバランサー自体が正常でない場合、Route 53 は他のリソースにクエリをルーティングします。

- アプリケーションと Network Load Balancer – ELB アプリケーションまたは Network Load Balancer を指定し、[Evaluate Target health (ターゲットの正常性の評価)] を Yes に設定すると、Route 53 は、ロードバランサーに関連付けられているターゲットグループの正常性に基づいて、クエリをロードバランサーにルーティングします。
  - アプリケーションまたは Network Load Balancer が正常とみなされるには、ターゲットを含むターゲットグループに、正常なターゲットが 1 つ以上含まれている必要があります。ターゲットグループに異常なターゲットのみが含まれている場合、ロードバランサーは異常であるとみなされ、Route 53 はクエリを他のリソースにルーティングします。
  - 登録されたターゲットを持たないターゲットグループは異常であるとみなされます。

> **Note**
>
> ロードバランサーを作成するときは、Elastic Load Balancing のヘルスチェックの設定を行います。これは Route 53 のヘルスチェックではありませんが、同様の機能を実行します。ELB ロードバランサーに登録する EC2 インスタンスに対しては Route 53 のヘルスチェックを作成しないでください。

S3 バケット

エンドポイントが S3 バケットである場合、[ターゲットの正常性の評価] を [Yes] に設定するための特別な要件はありません。

Amazon VPC インターフェイスのエンドポイント

エンドポイントが Amazon VPC インターフェイスエンドポイントである場合、[ターゲットの正常性の評価] を [Yes] に設定するための特別な要件はありません。

同じホストゾーンの他のレコード

Endpoint で指定した AWS リソースがレコードまたはレコードのグループ (加重レコードのグループなど) で、別のエイリアスレコードではない場合は、ヘルスチェックをエンドポイント内のすべてのレコードに関連付けることをお勧めします。詳細については、「ヘルスチェックを省略するとどうなるか」を参照してください。

記録 ID

プライマリレコードとセカンダリレコードを一意に識別する値を入力します。

位置情報レコードに固有の値

位置情報レコードを作成するときは、以下の値を指定します。

トピック

- ルーティングポリシー
- レコード名
- レコードタイプ
- TTL (秒)
- 値/トラフィックのルーティング先
- ロケーション
- 米国の州
- ヘルスチェック
- 記録 ID

ルーティングポリシー

[位置情報] を選択します。

レコード名

トラフィックをルーティングするドメインまたはサブドメインの名前を入力します。デフォルト値はホストゾーンの名前です。

> **Note**
>
> ホストゾーンと同じ名前のレコードを作成する場合は、[名前] フィールドに値 (@ 記号など) を入力しないでください。

位置情報レコードのグループで、すべてのレコードに同じ名前を入力します。

レコード名の詳細については、レコード名 を参照してください。

レコードタイプ

DNS レコードタイプ。詳細については、「サポートされる DNS レコードタイプ」を参照してください

位置情報レコードのグループ内のすべてのレコードに同じ値を選択します。

TTL (秒)

DNS 再帰リゾルバーがこのレコードに関する情報をキャッシュする秒単位の時間。より長い値 (172,800 秒、2 日など) を指定した場合、DNS 再帰リゾルバーが Route 53 に対して行う必要がある呼び出しの数を減らします。これにより、レイテンシーが短縮され、Route 53 サービスの請求額が削減されます。詳細については、「Amazon Route 53 によりドメインのトラフィックをルーティングする方法」を参照してください。

ただし、TTL に長い値を使用する場合、再帰的なリゾルバーは、Route 53 に最新の情報を問い合わせるまでに、長い間キャッシュ内の値を使用するため、レコードに対する変更 (例えば、新しい IP アドレス) が有効になるまでの時間が長くなります。既に使用されているドメインまたはサブドメインの設定を変更する場合、最初は 300 秒など短い値を指定し、新しい設定が正しいことを確認したら、値を増やすことをお勧めします。

このレコードをヘルスチェックに関連付ける場合、ヘルスステータスの変化にクライアントがすばやく対応できるよう、60 秒以下の TTL を指定することをお勧めします。

値/トラフィックのルーティング先

IP アドレス、またはレコードタイプに応じた別の値を選択します。[レコードタイプ] の値として適切な値を入力します。[CNAME] を除くすべてのタイプは、複数の値を入力できます。各値は個別の行に入力します。

次の値にトラフィックをルーティングするか、次の値を指定できます。

- A — IPv4 アドレス
- AAAA — IPv6 アドレス
- CAA —認証局の承認
- CNAME — 正規名
- MX — メール交換
- NAPTR — 名前付け権限ポインタ
- PTR — ポインタ
- SPF — センダーポリシーフレームワーク
- SRV — サービスロケーター
- TXT — テキスト

上記の値の詳細については、「common values for Value/Route traffic to」(値/トラフィックのルーティング先) を参照してください。

ロケーション

クエリの発信元の場所に基づいて DNS クエリに応答するように Route 53 を設定する場合は、Route 53 がこのレコードの設定を使用して応答する対象の大陸または国を選択します。Route 53 が米国の各州について DNS クエリに応答する場合は、[ロケーション] リストから [米国] を選択し、[サブロケーション] グループから州を選択します。

プライベートホストゾーンの場合は、リソース AWS リージョン がある に最も近い大陸、国、またはサブディビジョンを選択します。例えば、リソースが us-east-1 にある場合であれば、北米、米国、またはバージニアを指定します。

> **Important**
>
> [ロケーション] に関する [デフォルト] の値を持つ位置情報レコードを 1 つ作成することをお勧めします。これにより、レコードを作成していない地理的場所および Route 53 が位置を識別できない IP アドレスをカバーできます。

[レコード名] および [レコードタイプ] の値が位置情報コードと同じである非位置情報レコードを作成することはできません。

詳細については、「位置情報ルーティング」を参照してください

Amazon Route 53 が各大陸に関連付ける国を次に示します。国コードは、ISO 3166 のものです。詳細については、Wikipedia の記事、「ISO 3166-1 alpha-2」を参照してください。

アフリカ (AF)

AO、BF、BI、BJ、BW、CD、CF、CG、CI、CM、CV、DJ、DZ、EG、ER、ET、GA、GH、GM、GN

南極 (AN)

AQ、GS、TF

アジア (AS)

AE、AF、AM、AZ、BD、BH、BN、BT、CC、CN、GE、HK、ID、IL、IN、IO、IQ、IR、JO、JP、KG

欧州 (EU)

AD、AL、AT、AX、BA、BE、BG、BY、CH、CY、CZ、DE、DK、EE、ES、FI、FO、FR、GB、GG、

> **Note**
>
> 一部のプロバイダーは、TR がアジアにあると見なしており、IP アドレスにはそれが反映されます。

北米 (NA)

AG、AI、AW、BB、BL、BM、BQ、BS、BZ、CA、CR、CU、CW、DM、DO、GD、GL、GP、GT、H

オセアニア (OC)

AS、AU、CK、FJ、FM、GU、KI、MH、MP、NC、NF、NR、NU、NZ、PF、PG、PN、PW、SB、TK

南米 (SA)

AR、BO、BR、CL、CO、EC、FK、GF、GY、PE、PY、SR、UY、VE

> **Note**
>
> Route 53 では、以下の国の位置情報レコードの作成をサポートしていません。ブーベ島 (BV)、クリスマス島 (CX)、西サハラ (EH)、ハード島とマクドナルド諸島 (HM)。これらの国の IP アドレスに関するデータは利用できません。

米国の州

クエリの発信元である米国の州に基づいて DNS クエリに応答するように Route 53 を設定する場合は、[米国の州] リストから州を選択します。米国の海外領土 (プエルトリコなど) は [Location (ロケーション)] リストに国として表示されます。

> **Important**
>
> 一部の IP アドレスは、米国と関連付けられていますが、個々の州とは関連付けられていません。米国のすべての州に対するレコードを作成する場合は、これらの関連付けられていない IP アドレスのクエリをルーティングするために、米国のレコードも作成することをお勧めします。米国のレコードを作成しない場合、Route 53 は関連付けられていない米国の IP アドレスからの DNS クエリに対して、デフォルトの位置情報レコードの設定 (作成している場合) または "応答なし" の応答を使用して応答します。

ヘルスチェック

Route 53 で、指定されたエンドポイントの正常性をチェックし、エンドポイントが正常であるときにのみ、このレコードを使用して DNS クエリに応答する場合は、ヘルスチェックを選択します。

Route 53 は、レコード内で指定されたエンドポイント、例えば、[値] フィールドの IP アドレスで指定されたエンドポイントの正常性はチェックしません。Route 53 は、レコードのヘルスチェックを選択したとき、ヘルスチェックで指定されたエンドポイントの正常性をチェックします。エンドポイントが正常であるかどうかを、Route 53 がどのように判断するかについては、「Amazon Route 53 でヘルスチェックの正常性を判断する方法」を参照してください。

ヘルスチェックをレコードに関連付けることに意味があるのは、Route 53 が複数のレコードの中から選択して DNS クエリに応答しており、その選択の一部をヘルスチェックのステータスに基づいて行うように Route 53 を設定する必要がある場合だけです。以下の設定でのみ、ヘルスチェックを使用してください。

- 名前、種類、およびルーティングポリシー (フェイルオーバーレコードや加重レコードなど) が同じレコードのグループ内のすべてのレコードのヘルスをチェックし、すべてのレコードのヘルスチェック ID を指定します。レコードのヘルスチェックが正常ではないエンドポイントを特定した場合、Route 53 はそのレコードの値を使用してクエリへの応答を停止します。
- フェイルオーバーエイリアス、位置情報エイリアス、レイテンシーエイリアス、IP ベースエイリアス、または加重エイリアスレコードのグループ内にあるエイリアスレコードまたはレコードの [Evaluate target health] (ターゲットのヘルスを評価) で、[Yes] (はい) を選択します。エイリアスレコードが同じホストゾーン内の非エイリアスレコードを参照する場合、参照先レコードのヘルスチェックも指定する必要があります。エイリアスレコードにヘルスチェックを関連付けた上で、[Evaluate Target Health] (ターゲットの正常性の評価) で [Yes] (はい) を選択した場合、これらの設定は両方とも有効になります。詳細については、「エイリアスレコードにヘルスチェックを関連付けるとどうなるか」を参照してください。

ヘルスチェックでドメイン名によってのみエンドポイントを指定する場合、エンドポイントごとにヘルスチェックを作成することをお勧めします。例えば、www.example.com のコンテンツを配信する各 HTTP サーバーについて、ヘルスチェックを作成します。[ドメイン名] の値には、レコードの名前 (example.com) ではなく、サーバーのドメイン名 (us-east-2-www.example.com など) を指定します。

> **Important**
>
> この構成で、[ドメイン名] の値がレコードの名前と一致するヘルスチェックを作成し、それらのレコードにヘルスチェックを関連付けた場合、ヘルスチェックで予想できない結果が生じます。

位置情報レコードで、エンドポイントが正常でない場合、Route 53 は、より大きい、関連付けられた地理的リージョンのレコードを探します。例えば、米国の 1 つの州、米国、北米、およびすべての場所 ([Location] が [Default]) のレコードがあるとします。州のレコードのエンドポイントが正常でない場合、Route 53 は、正常なエンドポイントがあるレコードが見つかるまで、米国、北米、すべての場所のレコードを、この順序で確認します。すべての場所のレコードを確認しても、適用可能なレコードがすべて正常でない場合、Route 53 は最小の地理的リージョンのレコードの値を使用して DNS クエリに応答します。

記録 ID

位置情報レコードのグループ内で、このレコードを一意に識別する値を入力します。

位置情報エイリアスレコードに固有の値

位置情報エイリアスレコードを作成するときは、以下の値を指定します。

詳しくは、エイリアスレコードと非エイリアスレコードの選択 を参照してください。

トピック

- ルーティングポリシー
- レコード名
- レコードタイプ
- 値/トラフィックのルーティング先
- ロケーション
- 米国の州
- ヘルスチェック
- ターゲットの正常性の評価
- 記録 ID

ルーティングポリシー

[位置情報] を選択します。

レコード名

トラフィックをルーティングするドメインまたはサブドメインの名前を入力します。デフォルト値はホストゾーンの名前です。

> **Note**
>
> ホストゾーンと同じ名前のレコードを作成する場合は、[レコード名] フィールドに値 (@ 記号など) を入力しないでください。

位置情報レコードのグループで、すべてのレコードに同じ名前を入力します。

レコード名の詳細については、レコード名 を参照してください。

レコードタイプ

DNS レコードタイプ。詳細については、「サポートされる DNS レコードタイプ」を参照してください。

トラフィックをルーティングする AWS リソースに基づいて、該当する値を選択します。位置情報レコードのグループ内のすべてのレコードに同じ値を選択します。

API Gateway のカスタムリージョン API またはエッジ最適化 API

[A — IPv4 アドレス] を選択します。

Amazon VPC インターフェイスのエンドポイント

[A — IPv4 アドレス] を選択します。

CloudFront 配信

[A — IPv4 アドレス] を選択します。

ディストリビューションに対して IPv6 が有効になっている場合は、2 つのレコードを作成します。1 つは [タイプ] として [A — IPv4 アドレス] の値を持つもの、もう 1つは [AAAA — IPv6 アドレス] の値を持つものとします。

App Runner サービス

[A — IPv4 アドレス] を選択します。

ローカル化されたサブドメインがある Elastic Beanstalk 環境

[A — IPv4 アドレス] を選択します。

ELB ロードバランサー

[A — IPv4 アドレス] または [AAAA — IPv6 アドレス] を選択します。

Amazon S3 バケット

[A — IPv4 アドレス] を選択します。

OpenSearch Service

[A — IPv4 アドレス] または [AAAA — IPv6 アドレス] を選択します。

このホストゾーン内の別のレコード

エイリアスを作成するレコードのタイプを選択します。[NS] および [SOA] 以外のすべてのタイプがサポートされます。

> **Note**
>
> ホストゾーン (Zone Apex といいます) と同じ名前のエイリアスレコードを作成する場合、[タイプ] の値が [CNAME] のレコードにトラフィックをルーティングすることはできません。これは、トラフィックがルーティングされているレコードとエイリアスレコードのタイプが同じでなければならず、Zone Apex の CNAME レコードの作成はエイリアスレコードであってもサポートされていないためです。

値/トラフィックのルーティング先

リストから選択する値、または フィールドに入力する値は、トラフィックをルーティングする AWS リソースによって異なります。

ターゲットにできる AWS リソースの詳細については、「」を参照してください[への値/ルートトラフィック]。

特定の AWS リソースにトラフィックをルーティングするように Route 53 を設定する方法の詳細については、「」を参照してください[AWS リソースへのインターネットトラフィックのルーティング]。

ロケーション

クエリの発信元の場所に基づいて DNS クエリに応答するように Route 53 を設定する場合は、Route 53 がこのレコードの設定を使用して応答する対象の大陸または国を選択します。Route 53 が米国の各州について DNS クエリに応答する場合は、[ロケーション] リストから [米国] を選択し、[米国の州] リストから州を選択します。

プライベートホストゾーンの場合は、リソース AWS リージョン がある に最も近い大陸、国、またはサブディビジョンを選択します。例えば、リソースが us-east-1 にある場合であれば、北米、米国、またはバージニアを指定します。

> **Important**
>
> [ロケーション] に関する [デフォルト] の値を持つ位置情報レコードを 1 つ作成することをお勧めします。これにより、レコードを作成していない地理的場所および Route 53 が位置を識別できない IP アドレスをカバーできます。

[レコード名] および [レコードタイプ] の値が位置情報コードと同じである非位置情報レコードを作成することはできません。

詳細については、「位置情報ルーティング」を参照してください

Amazon Route 53 が各大陸に関連付ける国を次に示します。国コードは、ISO 3166 のものです。詳細については、Wikipedia の記事、「ISO 3166-1 alpha-2」を参照してください。

アフリカ (AF)

AO、BF、BI、BJ、BW、CD、CF、CG、CI、CM、CV、DJ、DZ、EG、ER、ET、GA、GH、GM、GN

南極 (AN)

AQ、GS、TF

アジア (AS)

AE、AF、AM、AZ、BD、BH、BN、BT、CC、CN、GE、HK、ID、IL、IN、IO、IQ、IR、JO、JP、KG

欧州 (EU)

AD、AL、AT、AX、BA、BE、BG、BY、CH、CY、CZ、DE、DK、EE、ES、FI、FO、FR、GB、GG、

> **Note**
> 一部のプロバイダーは、TR がアジアにあると見なしており、IP アドレスにはそれが反映されます。

北米 (NA)

AG、AI、AW、BB、BL、BM、BQ、BS、BZ、CA、CR、CU、CW、DM、DO、GD、GL、GP、GT、H

オセアニア (OC)

AS、AU、CK、FJ、FM、GU、KI、MH、MP、NC、NF、NR、NU、NZ、PF、PG、PN、PW、SB、TK

南米 (SA)

AR、BO、BR、CL、CO、EC、FK、GF、GY、PE、PY、SR、UY、VE

> **Note**
>
> Route 53 では、以下の国の位置情報レコードの作成をサポートしていません。ブーベ島 (BV)、クリスマス島 (CX)、西サハラ (EH)、ハード島とマクドナルド諸島 (HM)。これらの国の IP アドレスに関するデータは利用できません。

米国の州

クエリの発信元である米国の州に基づいて DNS クエリに応答するように Route 53 を設定する場合は、[米国の州] リストから州を選択します。米国の海外領土 (プエルトリコなど) は [Location (ロケーション)] リストに国として表示されます。

> **Important**
>
> 一部の IP アドレスは、米国と関連付けられていますが、個々の州とは関連付けられていません。米国のすべての州に対するレコードを作成する場合は、これらの関連付けられていない IP アドレスのクエリをルーティングするために、米国のレコードも作成することをお勧めします。米国のレコードを作成しない場合、Route 53 は関連付けられていない米国の IP アドレスからの DNS クエリに対して、デフォルトの位置情報レコードの設定 (作成している場合) または "応答なし" の応答を使用して応答します。

ヘルスチェック

Route 53 で、指定されたエンドポイントの正常性をチェックし、エンドポイントが正常であるときにのみ、このレコードを使用して DNS クエリに応答する場合は、ヘルスチェックを選択します。

Route 53 は、レコード内で指定されたエンドポイント、例えば、[値] フィールドの IP アドレスで指定されたエンドポイントの正常性はチェックしません。Route 53 は、レコードのヘルスチェックを選択したとき、ヘルスチェックで指定されたエンドポイントの正常性をチェックします。エンドポイントが正常であるかどうかを、Route 53 がどのように判断するかについては、「Amazon Route 53 でヘルスチェックの正常性を判断する方法」を参照してください。

ヘルスチェックをレコードに関連付けることに意味があるのは、Route 53 が複数のレコードの中から選択して DNS クエリに応答しており、その選択の一部をヘルスチェックのステータスに基づいて行うように Route 53 を設定する必要がある場合だけです。以下の設定でのみ、ヘルスチェックを使用してください。

- 名前、種類、およびルーティングポリシー (フェイルオーバーレコードや加重レコードなど) が同じレコードのグループ内のすべてのレコードのヘルスをチェックし、すべてのレコードのヘルスチェック ID を指定します。レコードのヘルスチェックが正常ではないエンドポイントを特定した場合、Route 53 はそのレコードの値を使用してクエリへの応答を停止します。
- フェイルオーバーエイリアス、位置情報エイリアス、レイテンシーエイリアス、IP ベースエイリアス、または加重エイリアスレコードのグループ内にあるエイリアスレコードまたはレコードの [Evaluate target health] (ターゲットのヘルスを評価) で、[Yes] (はい) を選択します。エイリアスレコードが同じホストゾーン内の非エイリアスレコードを参照する場合、参照先レコードのヘルスチェックも指定する必要があります。エイリアスレコードにヘルスチェックを関連付けた上で、[Evaluate Target Health] (ターゲットの正常性の評価) で [Yes] (はい) を選択した場合、これらの設定は両方とも有効になります。詳細については、「エイリアスレコードにヘルスチェックを関連付けるとどうなるか」を参照してください。

ヘルスチェックでドメイン名によってのみエンドポイントを指定する場合、エンドポイントごとにヘルスチェックを作成することをお勧めします。例えば、www.example.com のコンテンツを配信する各 HTTP サーバーについて、ヘルスチェックを作成します。[ドメイン名] の値には、レコードの名前 (example.com) ではなく、サーバーのドメイン名 (us-east-2-www.example.com など) を指定します。

> **Important**
>
> この構成で、[ドメイン名] の値がレコードの名前と一致するヘルスチェックを作成し、それらのレコードにヘルスチェックを関連付けた場合、ヘルスチェックで予想できない結果が生じます。

位置情報レコードで、エンドポイントが正常でない場合、Route 53 は、より大きい、関連付けられた地理的リージョンのレコードを探します。例えば、米国の 1 つの州、米国、北米、およびすべての場所 ([Location] が [Default]) のレコードがあるとします。州のレコードのエンドポイントが正常でない場合、Route 53 は、正常なエンドポイントがあるレコードが見つかるまで、米国、北米、すべての場所のレコードを、この順序で確認します。すべての場所のレコードを確認しても、適用可能なレコードがすべて正常でない場合、Route 53 は最小の地理的リージョンのレコードの値を使用して DNS クエリに応答します。

ターゲットの正常性の評価

Route 53 で、このレコードを使用して [エンドポイント] で指定されたリソースの正常性を確認することによって DNS クエリに応答するかどうかを判定する場合は、[Yes] を選択します。

次の点に注意してください。

API Gateway のカスタムリージョン API とエッジ最適化 API

エンドポイントが API Gateway カスタムリージョン API またはエッジ最適化 API である場合、[Evaluate target health] (ターゲットヘルスを評価) を [Yes] (はい) に設定するための特別な要件はありません。

CloudFront ディストリビューション

エンドポイントが CloudFront ディストリビューションの場合、[ターゲットの正常性の評価] を [Yes] に設定することはできません。

ローカル化されたサブドメインがある Elastic Beanstalk 環境

[エンドポイント] で Elastic Beanstalk 環境を指定し、その環境に ELB ロードバランサーが含まれている場合、Elastic Load Balancing はクエリをロードバランサーに登録されている正常な Amazon EC2 インスタンスにのみルーティングします。(複数の Amazon EC2 インスタンスが含まれている場合、環境には自動的に ELB ロードバランサーが含まれます。) [ターゲットの正常性の評価] を [Yes] に設定したとき、正常な Amazon EC2 インスタンスがない場合やロードバランサー自体が正常でない場合、Route 53 は他に利用可能なリソースがあれば、そこにクエリをルーティングします。

環境に 1 つの Amazon EC2 インスタンスが含まれている場合、特別な要件はありません。

ELB ロードバランサー

ヘルスチェックの動作はロードバランサーのタイプによって異なります。

- [Classic Load Balancers] – [エンドポイント] で ELB Classic Load Balancer を指定した場合、Elastic Load Balancing は、ロードバランサーに登録されている正常な Amazon EC2 インスタンスにのみクエリをルーティングします。[ターゲットの正常性の評価] を [Yes] に設定したとき、正常な EC2 インスタンスがない場合やロードバランサー自体が正常でない場合、Route 53 は他のリソースにクエリをルーティングします。
- アプリケーションと Network Load Balancer – ELB アプリケーションまたは Network Load Balancer を指定し、[ターゲットの正常性の評価] を Yes に設定すると、Route 53 は、ロードバランサーに関連付けられているターゲットグループの正常性に基づいて、クエリをロードバランサーにルーティングします。

- アプリケーションまたはNetwork Load Balancerを正常であると見なすには、ターゲットを含むすべてのターゲットグループに少なくとも 1 つの正常なターゲットが含まれている必要があります。ターゲットグループに異常なターゲットのみが含まれている場合、ロードバランサーは異常であるとみなされ、Route 53 はクエリを他のリソースにルーティングします。
- 登録されたターゲットを持たないターゲットグループは異常であるとみなされます。

> **Note**
>
> ロードバランサーを作成するときは、Elastic Load Balancing のヘルスチェックの設定を行います。これは Route 53 のヘルスチェックではありませんが、同様の機能を実行します。ELB ロードバランサーに登録する EC2 インスタンスに対しては Route 53 のヘルスチェックを作成しないでください。

S3 バケット

エンドポイントが S3 バケットである場合、[ターゲットの正常性の評価] を [Yes] に設定するための特別な要件はありません。

Amazon VPC インターフェイスのエンドポイント

エンドポイントが Amazon VPC インターフェイスエンドポイントである場合、[ターゲットの正常性の評価] を [Yes] に設定するための特別な要件はありません。

同じホストゾーンの他のレコード

Endpoint で指定した AWS リソースがレコードまたはレコードのグループ (加重レコードのグループなど) で、別のエイリアスレコードではない場合は、ヘルスチェックをエンドポイント内のすべてのレコードに関連付けることをお勧めします。詳細については、「ヘルスチェックを省略するとどうなるか」を参照してください。

記録 ID

位置情報レコードのグループ内で、このレコードを一意に識別する値を入力します。

地理的近接性レコードに固有の値

地理的近接性レコードを作成するときは、以下の値を指定します。

トピック

- ルーティングポリシー
- レコード名
- レコードタイプ
- TTL (秒)
- 値/トラフィックのルーティング先
- エンドポイントの場所
- Bias (バイアス)
- ヘルスチェック
- 記録 ID

ルーティングポリシー

[地理的近接性] を選択します。

レコード名

トラフィックをルーティングするドメインまたはサブドメインの名前を入力します。デフォルト値はホストゾーンの名前です。

> **Note**
>
> ホストゾーンと同じ名前のレコードを作成する場合は、[名前] フィールドに値 (@ 記号など) を入力しないでください。

地理的近接性レコードのグループで、すべてのレコードに同じ名前を入力します。

レコード名の詳細については、レコード名 を参照してください。

レコードタイプ

DNS レコードタイプ。詳細については、「サポートされる DNS レコードタイプ」を参照してください。

地理的近接性レコードのグループ内のすべてのレコードに同じ値を選択します。

TTL (秒)

DNS 再帰リゾルバーがこのレコードに関する情報をキャッシュする秒単位の時間。より長い値 (172,800 秒、2 日など) を指定した場合、DNS 再帰リゾルバーが Route 53 に対して行う必要がある呼び出しの数を減らします。これにより、レイテンシーが短縮され、Route 53 サービスの請求額が削減されます。詳細については、「Amazon Route 53 によりドメインのトラフィックをルーティングする方法」を参照してください。

ただし、TTL に長い値を使用する場合、再帰的なリゾルバーは、Route 53 に最新の情報を問い合わせるまでに、長い間キャッシュ内の値を使用するため、レコードに対する変更 (例えば、新しい IP アドレス) が有効になるまでの時間が長くなります。既に使用されているドメインまたはサブドメインの設定を変更する場合、最初は 300 秒など短い値を指定し、新しい設定が正しいことを確認したら、値を増やすことをお勧めします。

このレコードをヘルスチェックに関連付ける場合、ヘルスステータスの変化にクライアントがすばやく対応できるよう、60 秒以下の TTL を指定することをお勧めします。

値/トラフィックのルーティング先

IP アドレス、またはレコードタイプに応じた別の値を選択します。[レコードタイプ] の値として適切な値を入力します。[CNAME] を除くすべてのタイプは、複数の値を入力できます。各値は個別の行に入力します。

次の値にトラフィックをルーティングするか、次の値を指定できます。

- A — IPv4 アドレス
- AAAA — IPv6 アドレス
- CAA —認証局の承認
- CNAME — 正規名
- MX — メール交換
- NAPTR — 名前付け権限ポインタ
- PTR — ポインタ
- SPF — センダーポリシーフレームワーク
- SRV — サービスロケーター
- TXT — テキスト

上記の値の詳細については、「common values for Value/Route traffic to」(値/トラフィックのルーティング先) を参照してください。

エンドポイントの場所

次の方法のいずれかを使用して、リソースエンドポイント場所を指定できます。

カスタム座標

地理的領域の経度と緯度を指定します。

AWS リージョン

[場所] リストから使用可能なリージョンを選択します。

リージョンの詳細については、「AWS グローバルインフラストラクチャ」を参照してください。

AWS ローカルゾーングループ

[場所] リストから使用可能なローカルゾーングループを選択します。

ローカルゾーンの詳細については、「AWS ローカルゾーンユーザーガイド」の「利用可能なローカルゾーン」を参照してください。ローカルゾーングループは、通常、終了文字がないローカルゾーンです。例えば、ローカルゾーンが `us-east-1-bue-1a` の場合、ローカルゾーングループは `us-east-1-bue-1` です。

describe-availability-zones CLI コマンドを使用して、特定のローカルゾーンのローカルゾーングループを特定することもできます。

```
aws ec2 describe-availability-zones \
    --region us-west-2 \
    --all-availability-zones \
    --query "AvailabilityZones[?ZoneName=='us-west-2-den-1a']" \
    | grep "GroupName"
```

このコマンドは `"GroupName": "us-west-2-den-1"` を返して、ローカルゾーン `us-west-2-den-1a` がローカルゾーングループ `us-west-2-den-1` に属するように指定します。

[レコード名] および [レコードタイプ] の値が地理的近接性レコードと同じである非地理的近接性レコードを作成することはできません。

同じレコード名とレコードタイプに同じ場所を指定する 2 つの地理的近接性リソースレコードセットを作成することもできません。

Bias (バイアス)

バイアスは、リソースにトラフィックをルーティングする Route 53 から地理的領域のサイズを拡大または縮小します。正のバイアスは領域を拡張し、負のバイアスは領域を縮小します。詳細については、「Amazon Route 53 がバイアスを使用してトラフィックをルーティングする方法」を参照してください。

ヘルスチェック

Route 53 で、指定されたエンドポイントの正常性をチェックし、エンドポイントが正常であるときにのみ、このレコードを使用して DNS クエリに応答する場合は、ヘルスチェックを選択します。

Route 53 は、レコード内で指定されたエンドポイント、例えば、[値] フィールドの IP アドレスで指定されたエンドポイントの正常性はチェックしません。Route 53 は、レコードのヘルスチェックを選択したとき、ヘルスチェックで指定されたエンドポイントの正常性をチェックします。エンドポイントが正常であるかどうかを、Route 53 がどのように判断するかについては、「Amazon Route 53 でヘルスチェックの正常性を判断する方法」を参照してください。

ヘルスチェックをレコードに関連付けることに意味があるのは、Route 53 が複数のレコードの中から選択して DNS クエリに応答しており、その選択の一部をヘルスチェックのステータスに基づいて行うように Route 53 を設定する必要がある場合だけです。以下の設定でのみ、ヘルスチェックを使用してください。

- 名前、種類、およびルーティングポリシー (フェイルオーバーレコードや加重レコードなど) が同じレコードのグループ内のすべてのレコードのヘルスをチェックし、すべてのレコードのヘルスチェック ID を指定します。レコードのヘルスチェックが正常ではないエンドポイントを特定した場合、Route 53 はそのレコードの値を使用してクエリへの応答を停止します。
- フェイルオーバーエイリアス、位置情報エイリアス、地理的近接性エイリアス、レイテンシーエイリアス、IP ベースエイリアス、または加重エイリアスレコードのグループ内にある 1 つのエイリアスレコードまたは複数のレコードの [ターゲットの正常性の評価] で、[はい] を選択します。エイリアスレコードが同じホストゾーン内の非エイリアスレコードを参照する場合、参照先レコードのヘルスチェックも指定する必要があります。エイリアスレコードにヘルスチェックを関連付けた上で、[Evaluate Target Health] (ターゲットの正常性の評価) で [Yes] (はい) を選択した場合、これらの設定は両方とも有効になります。詳細については、「エイリアスレコードにヘルスチェックを関連付けるとどうなるか」を参照してください。

ヘルスチェックでドメイン名によってのみエンドポイントを指定する場合、エンドポイントごとにヘルスチェックを作成することをお勧めします。例えば、www.example.com のコンテンツを配信する各 HTTP サーバーについて、ヘルスチェックを作成します。[ドメイン名] の値には、レコードの名前 (example.com) ではなく、サーバーのドメイン名 (us-east-2-www.example.com など) を指定します。

> **Important**
>
> この構成で、[ドメイン名] の値がレコードの名前と一致するヘルスチェックを作成し、それらのレコードにヘルスチェックを関連付けた場合、ヘルスチェックで予想できない結果が生じます。

地理的近接性レコードの場合、エンドポイントが異常になると、正常が続いている最も近いエンドポイントを Route 53 が探します。

記録 ID

地理的近接性レコードのグループ内で、このレコードを一意に識別する値を入力します。

地理的近接性エイリアスレコードに固有の値

地理的近接性エイリアスレコードを作成するときは、以下の値を指定します。

詳細については、「エイリアスレコードと非エイリアスレコードの選択」を参照してください。

トピック

- ルーティングポリシー
- レコード名
- レコードタイプ
- 値/トラフィックのルーティング先
- エンドポイントの場所
- Bias (バイアス)
- ヘルスチェック
- ターゲットの正常性の評価
- 記録 ID

ルーティングポリシー

[地理的近接性] を選択します。

レコード名

トラフィックをルーティングするドメインまたはサブドメインの名前を入力します。デフォルト値はホストゾーンの名前です。

> **Note**
>
> ホストゾーンと同じ名前のレコードを作成する場合は、[レコード名] フィールドに値 (@ 記号など) を入力しないでください。

地理的近接性レコードのグループで、すべてのレコードに同じ名前を入力します。

レコード名の詳細については、レコード名 を参照してください。

レコードタイプ

DNS レコードタイプ。詳細については、「サポートされる DNS レコードタイプ」を参照してください。

トラフィックをルーティングする AWS リソースに基づいて、該当する値を選択します。地理的近接性レコードのグループ内のすべてのレコードに同じ値を選択します。

API Gateway のカスタムリージョン API またはエッジ最適化 API

[A — IPv4 アドレス] を選択します。

Amazon VPC インターフェイスのエンドポイント

[A — IPv4 アドレス] を選択します。

CloudFront 配信

[A — IPv4 アドレス] を選択します。

ディストリビューションに対して IPv6 が有効になっている場合は、2 つのレコードを作成します。1 つは [タイプ] として [A — IPv4 アドレス] の値を持つもの、もう 1つは [AAAA — IPv6 アドレス] の値を持つものとします。

App Runner サービス

[A — IPv4 アドレス] を選択します。

ローカル化されたサブドメインがある Elastic Beanstalk 環境

[A — IPv4 アドレス] を選択します。

ELB ロードバランサー

[A — IPv4 アドレス] または [AAAA — IPv6 アドレス] を選択します。

Amazon S3 バケット

[A — IPv4 アドレス] を選択します。

OpenSearch Service

[A — IPv4 アドレス] または [AAAA — IPv6 アドレス] を選択します。

このホストゾーン内の別のレコード

エイリアスを作成するレコードのタイプを選択します。[NS] および [SOA] 以外のすべてのタイプがサポートされます。

> **Note**
>
> ホストゾーン (Zone Apex といいます) と同じ名前のエイリアスレコードを作成する場合、[タイプ] の値が [CNAME] のレコードにトラフィックをルーティングすることはできません。これは、トラフィックがルーティングされているレコードとエイリアスレコードのタイプが同じでなければならず、Zone Apex の CNAME レコードの作成はエイリアスレコードであってもサポートされていないためです。

値/トラフィックのルーティング先

リストから選択する値、または フィールドに入力する値は、トラフィックをルーティングする AWS リソースによって異なります。

ターゲットにできる AWS リソースの詳細については、「」を参照してくださいへの値/ルートトラフィック。

特定の AWS リソースにトラフィックをルーティングするように Route 53 を設定する方法の詳細については、「」を参照してくださいAWS リソースへのインターネットトラフィックのルーティング。

エンドポイントの場所

次の方法のいずれかを使用して、リソースエンドポイント場所を指定できます。

カスタム座標

地理的領域の経度と緯度を指定します。

AWS リージョン

[場所] リストから使用可能なリージョンを選択します。

リージョンの詳細については、「AWS グローバルインフラストラクチャ」を参照してください。

AWS ローカルゾーングループ

[場所] リストから使用可能なローカルゾーンリージョンを選択します。

ローカルゾーンの詳細については、「AWS ローカルゾーンユーザーガイド」の「利用可能なローカルゾーン」を参照してください。ローカルゾーングループは、通常、終了文字がないロー

カルゾーンです。例えば、ローカルゾーンが us-east-1-bue-1a の場合、ローカルゾーングループは us-east-1-bue-1 です。

describe-availability-zones CLI コマンドを使用して、特定のローカルゾーンのローカルゾーングループを特定することもできます。

```
aws ec2 describe-availability-zones \
    --region us-west-2 \
    --all-availability-zones \
    --query "AvailabilityZones[?ZoneName=='us-west-2-den-1a']" \
    | grep "GroupName"
```

このコマンドは "GroupName": "us-west-2-den-1" を返して、ローカルゾーン us-west-2-den-1a がローカルゾーングループ us-west-2-den-1 に属するように指定します。

[レコード名] および [レコードタイプ] の値が地理的近接性レコードと同じである非地理的近接性レコードを作成することはできません。

同じレコード名とレコードタイプに同じ場所を指定する 2 つの地理的近接性リソースレコードセットを作成することもできません。

詳細については、available-local-zones.html を参照してください

Bias (バイアス)

バイアスは、リソースにトラフィックをルーティングする Route 53 から地理的領域のサイズを拡大または縮小します。正のバイアスは領域を拡張し、負のバイアスは領域を縮小します。詳細については、「Amazon Route 53 がバイアスを使用してトラフィックをルーティングする方法」を参照してください。

ヘルスチェック

Route 53 で、指定されたエンドポイントの正常性をチェックし、エンドポイントが正常であるときにのみ、このレコードを使用して DNS クエリに応答する場合は、ヘルスチェックを選択します。

Route 53 は、レコード内で指定されたエンドポイント、例えば、[値] フィールドの IP アドレスで指定されたエンドポイントの正常性はチェックしません。Route 53 は、レコードのヘルスチェックを選択したとき、ヘルスチェックで指定されたエンドポイントの正常性をチェックします。エンドポイントが正常であるかどうかを、Route 53 がどのように判断するかについては、「Amazon Route 53 でヘルスチェックの正常性を判断する方法」を参照してください。

ヘルスチェックをレコードに関連付けることに意味があるのは、Route 53 が複数のレコードの中から選択して DNS クエリに応答しており、その選択の一部をヘルスチェックのステータスに基づいて行うように Route 53 を設定する必要がある場合だけです。以下の設定でのみ、ヘルスチェックを使用してください。

- 名前、種類、およびルーティングポリシー (フェイルオーバーレコードや加重レコードなど) が同じレコードのグループ内のすべてのレコードのヘルスをチェックし、すべてのレコードのヘルスチェック ID を指定します。レコードのヘルスチェックが正常ではないエンドポイントを特定した場合、Route 53 はそのレコードの値を使用してクエリへの応答を停止します。
- フェイルオーバーエイリアス、位置情報エイリアス、地理的近接性エイリアス、レイテンシーエイリアス、IP ベースエイリアス、または加重エイリアスレコードのグループ内にある 1 つのエイリアスレコードまたは複数のレコードの [ターゲットの正常性の評価] で、[はい] を選択します。エイリアスレコードが同じホストゾーン内の非エイリアスレコードを参照する場合、参照先レコードのヘルスチェックも指定する必要があります。エイリアスレコードにヘルスチェックを関連付けた上で、[Evaluate Target Health] (ターゲットの正常性の評価) で [Yes] (はい) を選択した場合、これらの設定は両方とも有効になります。詳細については、「エイリアスレコードにヘルスチェックを関連付けるとどうなるか」を参照してください。

ヘルスチェックでドメイン名によってのみエンドポイントを指定する場合、エンドポイントごとにヘルスチェックを作成することをお勧めします。例えば、www.example.com のコンテンツを配信する各 HTTP サーバーについて、ヘルスチェックを作成します。[ドメイン名] の値には、レコードの名前 (example.com) ではなく、サーバーのドメイン名 (us-east-2-www.example.com など) を指定します。

> **Important**
>
> この構成で、[ドメイン名] の値がレコードの名前と一致するヘルスチェックを作成し、それらのレコードにヘルスチェックを関連付けた場合、ヘルスチェックで予想できない結果が生じます。

地理的近接性レコードの場合、エンドポイントが異常になると、正常が続いている最も近いエンドポイントを Route 53 が探します。

ターゲットの正常性の評価

Route 53 で、このレコードを使用して [エンドポイント] で指定されたリソースの正常性を確認することによって DNS クエリに応答するかどうかを判定する場合は、[Yes] を選択します。

次の点に注意してください。

API Gateway のカスタムリージョン API とエッジ最適化 API

エンドポイントが API Gateway カスタムリージョン API またはエッジ最適化 API である場合、[Evaluate target health] (ターゲットヘルスを評価) を [Yes] (はい) に設定するための特別な要件はありません。

CloudFront ディストリビューション

エンドポイントが CloudFront ディストリビューションの場合、[ターゲットの正常性の評価] を [Yes] に設定することはできません。

ローカル化されたサブドメインがある Elastic Beanstalk 環境

[エンドポイント] で Elastic Beanstalk 環境を指定し、その環境に ELB ロードバランサーが含まれている場合、Elastic Load Balancing はクエリをロードバランサーに登録されている正常な Amazon EC2 インスタンスにのみルーティングします。(複数の Amazon EC2 インスタンスが含まれている場合、環境には自動的に ELB ロードバランサーが含まれます。) [ターゲットの正常性の評価] を [Yes] に設定したとき、正常な Amazon EC2 インスタンスがない場合やロードバランサー自体が正常でない場合、Route 53 は他に利用可能なリソースがあれば、そこにクエリをルーティングします。

環境に 1 つの Amazon EC2 インスタンスが含まれている場合、特別な要件はありません。

ELB ロードバランサー

ヘルスチェックの動作はロードバランサーのタイプによって異なります。

- [Classic Load Balancers] – [エンドポイント] で ELB Classic Load Balancer を指定した場合、Elastic Load Balancing は、ロードバランサーに登録されている正常な Amazon EC2 インスタンスにのみクエリをルーティングします。[ターゲットの正常性の評価] を [Yes] に設定したとき、正常な EC2 インスタンスがない場合やロードバランサー自体が正常でない場合、Route 53 は他のリソースにクエリをルーティングします。
- アプリケーションと Network Load Balancer – ELB アプリケーションまたは Network Load Balancer を指定し、[ターゲットの正常性の評価] を Yes に設定すると、Route 53 は、ロードバランサーに関連付けられているターゲットグループの正常性に基づいて、クエリをロードバランサーにルーティングします。
  - アプリケーションまたはNetwork Load Balancerを正常であると見なすには、ターゲットを含むすべてのターゲットグループに少なくとも 1 つの正常なターゲットが含まれている必要があります。ターゲットグループに異常なターゲットのみが含まれている場合、ロードバランサーは異常であるとみなされ、Route 53 はクエリを他のリソースにルーティングします。

- 登録されたターゲットを持たないターゲットグループは異常であるとみなされます。

> **Note**
>
> ロードバランサーを作成するときは、Elastic Load Balancing のヘルスチェックの設定を行います。これは Route 53 のヘルスチェックではありませんが、同様の機能を実行します。ELB ロードバランサーに登録する EC2 インスタンスに対しては Route 53 のヘルスチェックを作成しないでください。

S3 バケット

エンドポイントが S3 バケットである場合、[ターゲットの正常性の評価] を [Yes] に設定するための特別な要件はありません。

Amazon VPC インターフェイスのエンドポイント

エンドポイントが Amazon VPC インターフェイスエンドポイントである場合、[ターゲットの正常性の評価] を [Yes] に設定するための特別な要件はありません。

同じホストゾーンの他のレコード

Endpoint で指定した AWS リソースがレコードまたはレコードのグループ (加重レコードのグループなど) で、別のエイリアスレコードではない場合は、ヘルスチェックをエンドポイント内のすべてのレコードに関連付けることをお勧めします。詳細については、「ヘルスチェックを省略するとどうなるか」を参照してください。

記録 ID

地理的近接性レコードのグループ内で、このレコードを一意に識別する値を入力します。

レイテンシーレコードに固有の値

レイテンシーレコードを作成するときは、以下の値を指定します。

トピック

- ルーティングポリシー
- レコード名
- レコードタイプ
- TTL (秒)
- 値/トラフィックのルーティング先
- リージョン
- ヘルスチェック
- 記録 ID

ルーティングポリシー

[レイテンシー] を選択します。

レコード名

トラフィックをルーティングするドメインまたはサブドメインの名前を入力します。デフォルト値はホストゾーンの名前です。

> **Note**
>
> ホストゾーンと同じ名前のレコードを作成する場合は、[レコード名] フィールドに値 (@ 記号など) を入力しないでください。

レイテンシーレコードのグループで、すべてのレコードに同じ名前を入力します。

レコード名の詳細については、レコード名 を参照してください。

レコードタイプ

DNS レコードタイプ。詳細については、「サポートされる DNS レコードタイプ」を参照してください。

Route 53 が DNS クエリに応答する方法に基づいて、タイプの値を選択します。

レイテンシーレコードのグループ内のすべてのレコードに同じ値を選択します。

TTL (秒)

DNS 再帰リゾルバーがこのレコードに関する情報をキャッシュする秒単位の時間。より長い値 (172800 秒、2 日など) を指定した場合、DNS 再帰リゾルバーが Route 53 に対して行う必要がある呼び出しの数を減らします。これにより、レイテンシーが短縮され、Route 53 サービスの請求額が削減されます。詳細については、「Amazon Route 53 によりドメインのトラフィックをルーティングする方法」を参照してください。

ただし、TTL に長い値を指定すると、レコードの変更 (新しい IP アドレスなど) が有効になるまでに時間がかかります。再帰リゾルバーは、Route 53 に最新情報を要求する前に、キャッシュ内の値を長期間使用します。既に使用されているドメインまたはサブドメインの設定を変更する場合は、まず 300 秒などの短い値を指定し、新しい設定が正しいことを確認したら値を増やします。

このレコードをヘルスチェックに関連付ける場合は、クライアントがヘルスステータスの変化に迅速に応答するように、TTL を 60 秒以下に指定します。

値/トラフィックのルーティング先

IP アドレス、またはレコードタイプに応じた別の値を選択します。[レコードタイプ] の値として適切な値を入力します。[CNAME] を除くすべてのタイプは、複数の値を入力できます。各値は個別の行に入力します。

次の値にトラフィックをルーティングするか、次の値を指定できます。

- A — IPv4 アドレス
- AAAA — IPv6 アドレス
- CAA —認証局の承認
- CNAME — 正規名
- MX — メール交換
- NAPTR — 名前付け権限ポインタ
- PTR — ポインタ
- SPF — センダーポリシーフレームワーク
- SRV — サービスロケーター

- TXT — テキスト

上記の値の詳細については、「common values for Value/Route traffic to」(値/トラフィックのルーティング先) を参照してください。

リージョン

このレコードで指定されたリソースが存在する Amazon EC2 リージョン。Route 53 によって、指定したその他の値に基づく Amazon EC2 リージョンが推奨されます。これは、プライベートホストゾーンにも適用されます。この値は変更しないでください。

次の点に注意してください。

- 作成できるレイテンシーレコードは、各 Amazon EC2 リージョンにつき 1 つだけです。
- すべての Amazon EC2 リージョンに対してレイテンシーレコードを作成する必要はありません。レイテンシーレコードを作成したリージョンの中から、レイテンシーの最も小さいリージョンが Route 53 によって選択されます。
- [レコード名] および [レコードタイプ] の値がレイテンシーレコードと同じである非レイテンシーレコードを作成することはできません。
- cn-north-1 リージョンのタグ付きのレコードを作成した場合、Route 53 は、レイテンシーにかかわらず、常にこのレコードを使用して、中国内からのクエリに応答します。

レイテンシーレコードの使用の詳細については、「レイテンシーに基づくルーティング」を参照してください。

ヘルスチェック

Route 53 で、指定されたエンドポイントの正常性をチェックし、エンドポイントが正常であるときにのみ、このレコードを使用して DNS クエリに応答する場合は、ヘルスチェックを選択します。

Route 53 は、レコード内で指定されたエンドポイント、例えば、[値] フィールドの IP アドレスで指定されたエンドポイントの正常性はチェックしません。Route 53 は、レコードのヘルスチェックを選択したとき、ヘルスチェックで指定されたエンドポイントの正常性をチェックします。エンドポイントが正常であるかどうかを、Route 53 がどのように判断するかについては、「Amazon Route 53 でヘルスチェックの正常性を判断する方法」を参照してください。

ヘルスチェックとレコードの関連付けは、Route 53 が DNS クエリに応答するレコードを 2 つ以上選択していて、Route 53 がヘルスチェックのステータスに部分的に基づいて選択する場合に便利です。以下の設定でのみ、ヘルスチェックを使用してください。

- 名前、種類、およびルーティングポリシー (フェイルオーバーレコードや加重レコードなど) が同じレコードのグループ内のすべてのレコードのヘルスをチェックし、すべてのレコードのヘルスチェック ID を指定します。レコードのヘルスチェックが正常ではないエンドポイントを特定した場合、Route 53 はそのレコードの値を使用してクエリへの応答を停止します。
- フェイルオーバーエイリアス、位置情報エイリアス、レイテンシーエイリアス、IP ベースエイリアス、または加重エイリアスレコードのグループ内にあるエイリアスレコードまたはレコードの [Evaluate target health] (ターゲットのヘルスを評価) で、[Yes] (はい) を選択します。エイリアスレコードが同じホストゾーン内の非エイリアスレコードを参照する場合、参照先レコードのヘルスチェックも指定する必要があります。エイリアスレコードにヘルスチェックを関連付けた上で、[Evaluate Target Health] (ターゲットの正常性の評価) で [Yes] (はい) を選択した場合、これらの設定は両方とも有効になります。詳細については、「エイリアスレコードにヘルスチェックを関連付けるとどうなるか」を参照してください。

ヘルスチェックでエンドポイントをドメイン名でのみ指定する場合は、エンドポイントごとに個別のヘルスチェックを作成します。例えば、www.example.com のコンテンツを配信する各 HTTP サーバーについて、ヘルスチェックを作成します。[ドメイン名] の値には、レコードの名前 (example.com) ではなく、サーバーのドメイン名 (us-east-2-www.example.com など) を指定します。

> **Important**
>
> この構成で、[ドメイン名] の値がレコードの名前と一致するヘルスチェックを作成し、それらのレコードにヘルスチェックを関連付けた場合、ヘルスチェックで予想できない結果が生じます。

記録 ID

レイテンシーレコードのグループ内で、このレコードを一意に識別する値を入力します。

レイテンシーエイリアスレコードに固有の値

レイテンシーエイリアスレコードを作成するときは、以下の値を指定します。

詳細については、「エイリアスレコードと非エイリアスレコードの選択」を参照してください。

トピック

- ルーティングポリシー
- レコード名
- レコードタイプ
- 値/トラフィックのルーティング先
- リージョン
- ヘルスチェック
- ターゲットの正常性の評価
- 記録 ID

ルーティングポリシー

[レイテンシー] を選択します。

レコード名

トラフィックをルーティングするドメインまたはサブドメインの名前を入力します。デフォルト値はホストゾーンの名前です。

> **Note**
>
> ホストゾーンと同じ名前のレコードを作成する場合は、[レコード名] フィールドに値 (@ 記号など) を入力しないでください。

レイテンシーレコードのグループで、すべてのレコードに同じ名前を入力します。

レコード名の詳細については、レコード名 を参照してください。

レコードタイプ

DNS レコードタイプ。詳細については、「サポートされる DNS レコードタイプ」を参照してください。

トラフィックをルーティングする AWS リソースに基づいて、該当する値を選択します。

API Gateway のカスタムリージョン API またはエッジ最適化 API

[A — IPv4 アドレス] を選択します。

Amazon VPC インターフェイスのエンドポイント

[A — IPv4 アドレス] を選択します。

CloudFront 配信

[A — IPv4 アドレス] を選択します。

ディストリビューションに対して IPv6 が有効になっている場合は、2 つのレコードを作成します。1 つは [タイプ] として [A — IPv4 アドレス] の値を持つもの、もう 1つは [AAAA — IPv6 アドレス] の値を持つものとします。

App Runner サービス

[A — IPv4 アドレス] を選択します。

ローカル化されたサブドメインがある Elastic Beanstalk 環境

[A — IPv4 アドレス] を選択します。

ELB ロードバランサー

[A — IPv4 アドレス] または [AAAA — IPv6 アドレス] を選択します。

Amazon S3 バケット

[A — IPv4 アドレス] を選択します。

OpenSearch Service

[A — IPv4 アドレス] または [AAAA — IPv6 アドレス] を選択します。

このホストゾーン内の別のレコード

エイリアスを作成するレコードのタイプを選択します。[NS] および [SOA] 以外のすべてのタイプがサポートされます。

> **Note**
>
> ホストゾーン (Zone Apex といいます) と同じ名前のエイリアスレコードを作成する場合、[タイプ] の値が [CNAME] のレコードにトラフィックをルーティングすることはでき

ません。これは、トラフィックがルーティングされているレコードとエイリアスレコードのタイプが同じでなければならず、Zone Apex の CNAME レコードの作成はエイリアスレコードであってもサポートされていないためです。

レイテンシーレコードのグループ内のすべてのレコードに同じ値を選択します。

値/トラフィックのルーティング先

リストから選択する値、または フィールドに入力する値は、トラフィックをルーティングする AWS リソースによって異なります。

ターゲットにできる AWS リソースの詳細については、値/ルートトラフィックのエイリアスレコードの一般的な値を参照してください。

特定の AWS リソースにトラフィックをルーティングするように Route 53 を設定する方法の詳細については、「」を参照してくださいAWS リソースへのインターネットトラフィックのルーティング。

リージョン

このレコードで指定されたリソースが存在する Amazon EC2 リージョン。Route 53 によって、指定したその他の値に基づく Amazon EC2 リージョンが推奨されます。これは、プライベートホストゾーンにも適用されます。この値は変更しないことをお勧めします。

次の点に注意してください。

- 作成できるレイテンシーレコードは、各 Amazon EC2 リージョンにつき 1 つだけです。
- すべての Amazon EC2 リージョンに対してレイテンシーレコードを作成する必要はありません。レイテンシーレコードを作成したリージョンの中から、レイテンシーの最も小さいリージョンが Route 53 によって選択されます。
- [レコード名] および [レコードタイプ] の値がレイテンシーレコードと同じである非レイテンシーレコードを作成することはできません。
- cn-north-1 リージョンのタグ付きのレコードを作成した場合、Route 53 は、レイテンシーにかかわらず、常にこのレコードを使用して、中国内からのクエリに応答します。

レイテンシーレコードの使用の詳細については、「レイテンシーに基づくルーティング」を参照してください。

ヘルスチェック

Route 53 で、指定されたエンドポイントの正常性をチェックし、エンドポイントが正常であるときにのみ、このレコードを使用して DNS クエリに応答する場合は、ヘルスチェックを選択します。

Route 53 は、レコード内で指定されたエンドポイント、例えば、[値] フィールドの IP アドレスで指定されたエンドポイントの正常性はチェックしません。Route 53 は、レコードのヘルスチェックを選択したとき、ヘルスチェックで指定されたエンドポイントの正常性をチェックします。エンドポイントが正常であるかどうかを、Route 53 がどのように判断するかについては、「Amazon Route 53 でヘルスチェックの正常性を判断する方法」を参照してください。

ヘルスチェックをレコードに関連付けることに意味があるのは、Route 53 が複数のレコードの中から選択して DNS クエリに応答しており、その選択の一部をヘルスチェックのステータスに基づいて行うように Route 53 を設定する必要がある場合だけです。以下の設定でのみ、ヘルスチェックを使用してください。

- 名前、種類、およびルーティングポリシー (フェイルオーバーレコードや加重レコードなど) が同じレコードのグループ内のすべてのレコードのヘルスをチェックし、すべてのレコードのヘルスチェック ID を指定します。レコードのヘルスチェックが正常ではないエンドポイントを特定した場合、Route 53 はそのレコードの値を使用してクエリへの応答を停止します。
- フェイルオーバーエイリアス、位置情報エイリアス、レイテンシーエイリアス、IP ベースエイリアス、または加重エイリアスレコードのグループ内にあるエイリアスレコードまたはレコードの [Evaluate target health] (ターゲットのヘルスを評価) で、[Yes] (はい) を選択します。エイリアスレコードが同じホストゾーン内の非エイリアスレコードを参照する場合、参照先レコードのヘルスチェックも指定する必要があります。エイリアスレコードにヘルスチェックを関連付けた上で、[Evaluate Target Health] (ターゲットの正常性の評価) で [Yes] (はい) を選択した場合、これらの設定は両方とも有効になります。詳細については、「エイリアスレコードにヘルスチェックを関連付けるとどうなるか」を参照してください。

ヘルスチェックでドメイン名によってのみエンドポイントを指定する場合、エンドポイントごとにヘルスチェックを作成することをお勧めします。例えば、www.example.com のコンテンツを配信する各 HTTP サーバーについて、ヘルスチェックを作成します。[ドメイン名] の値には、レコードの名前 (example.com) ではなく、サーバーのドメイン名 (us-east-2-www.example.com など) を指定します。

> **Important**
>
> この構成で、[ドメイン名] の値がレコードの名前と一致するヘルスチェックを作成し、それらのレコードにヘルスチェックを関連付けた場合、ヘルスチェックで予想できない結果が生じます。

ターゲットの正常性の評価

Route 53 で、このレコードを使用して [エンドポイント] で指定されたリソースの正常性を確認することによって DNS クエリに応答するかどうかを判定する場合は、[Yes] を選択します。

次の点に注意してください。

API Gateway のカスタムリージョン API とエッジ最適化 API

エンドポイントが API Gateway カスタムリージョン API またはエッジ最適化 API である場合、[ターゲットの正常性の評価] を [Yes] に設定するための特別な要件はありません。

CloudFront ディストリビューション

エンドポイントが CloudFront ディストリビューションの場合、[ターゲットの正常性の評価] を [Yes] に設定することはできません。

ローカル化されたサブドメインがある Elastic Beanstalk 環境

[エンドポイント] で Elastic Beanstalk 環境を指定し、その環境に ELB ロードバランサーが含まれている場合、Elastic Load Balancing はクエリをロードバランサーに登録されている正常な Amazon EC2 インスタンスにのみルーティングします。(複数の Amazon EC2 インスタンスが含まれている場合、環境には自動的に ELB ロードバランサーが含まれます。) [ターゲットの正常性の評価] を [Yes] に設定したとき、正常な Amazon EC2 インスタンスがない場合やロードバランサー自体が正常でない場合、Route 53 は他に利用可能なリソースがあれば、そこにクエリをルーティングします。

環境に 1 つの Amazon EC2 インスタンスが含まれている場合、特別な要件はありません。

ELB ロードバランサー

ヘルスチェックの動作はロードバランサーのタイプによって異なります。

- [Classic Load Balancers] – [エンドポイント] で ELB Classic Load Balancer を指定した場合、Elastic Load Balancing は、ロードバランサーに登録されている正常な Amazon EC2 インスタンスにのみクエリをルーティングします。[ターゲットの正常性の評価] を [Yes] に設

定したとき、正常な EC2 インスタンスがない場合やロードバランサー自体が正常でない場合、Route 53 は他のリソースにクエリをルーティングします。

- アプリケーションと Network Load Balancer – ELB アプリケーションまたは Network Load Balancer を指定し、[ターゲットの正常性の評価] を Yes に設定すると、Route 53 は、ロードバランサーに関連付けられているターゲットグループの正常性に基づいて、クエリをロードバランサーにルーティングします。
  - アプリケーションまたはNetwork Load Balancerを正常であると見なすには、ターゲットを含むすべてのターゲットグループに少なくとも 1 つの正常なターゲットが含まれている必要があります。ターゲットグループに異常なターゲットのみが含まれている場合、ロードバランサーは異常であるとみなされ、Route 53 はクエリを他のリソースにルーティングします。
  - 登録されたターゲットを持たないターゲットグループは異常であるとみなされます。

> **Note**
>
> ロードバランサーを作成するときは、Elastic Load Balancing のヘルスチェックの設定を行います。これは Route 53 のヘルスチェックではありませんが、同様の機能を実行します。ELB ロードバランサーに登録する EC2 インスタンスに対しては Route 53 のヘルスチェックを作成しないでください。

S3 バケット

エンドポイントが S3 バケットである場合、[ターゲットの正常性の評価] を [Yes] に設定するための特別な要件はありません。

Amazon VPC インターフェイスのエンドポイント

エンドポイントが Amazon VPC インターフェイスエンドポイントである場合、[ターゲットの正常性の評価] を [Yes] に設定するための特別な要件はありません。

同じホストゾーンの他のレコード

Endpoint で指定した AWS リソースがレコードまたはレコードのグループ (加重レコードのグループなど) で、別のエイリアスレコードではない場合は、ヘルスチェックをエンドポイント内のすべてのレコードに関連付けることをお勧めします。詳細については、「ヘルスチェックを省略するとどうなるか」を参照してください。

記録 ID

レイテンシーレコードのグループ内で、このレコードを一意に識別する値を入力します。

IP ベースレコード特有の値

IP ベースレコードを作成する際は、以下の値を指定します。

> **Note**
>
> プライベートホストゾーン内に IP ベースレコードを作成することは可能ですが、動作は保証されていません。

トピック

- ルーティングポリシー
- レコード名
- レコードタイプ
- TTL (秒)
- 値/トラフィックのルーティング先
- ロケーション
- ヘルスチェック
- 記録 ID

ルーティングポリシー

[IP-based] (IP ベース) を選択します。

レコード名

トラフィックをルーティングするドメインまたはサブドメインの名前を入力します。デフォルト値はホストゾーンの名前です。

> **Note**
>
> ホストゾーンと同じ名前のレコードを作成する場合は、[レコード名] フィールドに値 (@ 記号など) を入力しないでください。

IP ベースレコードのグループ内で、すべてのレコードに同じ名前を入力します。

CNAME レコード

[レコードタイプ] の値が [CNAME] のレコードを作成する場合、レコードの名前をホストゾーンの名前と同じにすることはできません。

特殊文字

a ~ z、0 ~ 9、- (ハイフン) 以外の文字を指定する方法、および国際化されたドメイン名を指定する方法については、「DNS ドメイン名の形式」を参照してください。

ワイルドカード文字

名前にはアスタリスク (*) を使用できます。DNSは、名前の中の位置に応じて、「*」をワイルドカードまたはアスタリスク (ASCII 42) として処理します。詳細については、「ホストゾーンおよびレコード名のアスタリスク (*) を使用する」を参照してください。

レコードタイプ

DNS レコードタイプ。詳細については、「サポートされる DNS レコードタイプ」を参照してください。

Route 53 が DNS クエリに応答する方法に基づいて、タイプの値を選択します。

IP ベースレコードのグループ内のすべてのレコードに対し、同じ値を選択します。

TTL (秒)

DNS 再帰リゾルバーがこのレコードに関する情報をキャッシュする秒単位の時間。より長い値 (172,800 秒、2 日など) を指定した場合、DNS 再帰リゾルバーが Route 53 に対して行う必要がある呼び出しの数を減らします。これにより、レイテンシーが短縮され、Route 53 サービスの請求額が削減されます。詳細については、「Amazon Route 53 によりドメインのトラフィックをルーティングする方法」を参照してください。

ただし、TTL に長い値を指定すると、レコードの変更 (新しい IP アドレスなど) が有効になるまでに時間がかかります。再帰リゾルバーは、Route 53 に最新情報を要求する前に、キャッシュ内の値を長期間使用します。既に使用されているドメインまたはサブドメインの設定を変更する場合は、まず 300 秒などの短い値を指定し、新しい設定が正しいことを確認したら値を増やします。

このレコードをヘルスチェックに関連付ける場合は、クライアントがヘルスステータスの変化に迅速に応答するように、TTL を 60 秒以下に指定します。

値/トラフィックのルーティング先

IP アドレス、またはレコードタイプに応じた別の値を選択します。[レコードタイプ] の値として適切な値を入力します。[CNAME] を除くすべてのタイプは、複数の値を入力できます。各値は個別の行に入力します。

次の値にトラフィックをルーティングするか、次の値を指定できます。

- A — IPv4 アドレス
- AAAA — IPv6 アドレス
- CAA —認証局の承認
- CNAME — 正規名
- MX — メール交換
- NAPTR — 名前付け権限ポインタ
- PTR — ポインタ
- SPF — センダーポリシーフレームワーク
- SRV — サービスロケーター
- TXT — テキスト

上記の値の詳細については、値/トラフィックのルーティング先「common values for Value/Route traffic to」(値/トラフィックのルーティング先) を参照してください。

ロケーション

ユーザーがこのレコード内で指定し、また CIDR ロケーション内の CIDR ブロック値によっても指定されるリソースがある、CIDR ロケーションの名前。

IP ベースレコードの使用の詳細については、「IP ベースルーティング」を参照してください。

ヘルスチェック

Route 53 で、指定されたエンドポイントの正常性をチェックし、エンドポイントが正常であるときにのみ、このレコードを使用して DNS クエリに応答する場合は、ヘルスチェックを選択します。

Route 53 は、レコード内で指定されたエンドポイント、例えば、[値] フィールドの IP アドレスで指定されたエンドポイントの正常性はチェックしません。Route 53 は、レコードのヘルスチェックを選択したとき、ヘルスチェックで指定されたエンドポイントの正常性をチェックします。エンドポイ

ントが正常であるかどうかを、Route 53 がどのように判断するかについては、「Amazon Route 53 でヘルスチェックの正常性を判断する方法」を参照してください。

ヘルスチェックとレコードの関連付けは、Route 53 が DNS クエリに応答するレコードを 2 つ以上選択していて、Route 53 がヘルスチェックのステータスに部分的に基づいて選択する場合に便利です。以下の設定でのみ、ヘルスチェックを使用してください。

- 名前、種類、およびルーティングポリシー (フェイルオーバーレコードや加重レコードなど) が同じレコードのグループ内のすべてのレコードのヘルスをチェックし、すべてのレコードのヘルスチェック ID を指定します。レコードのヘルスチェックが正常ではないエンドポイントを特定した場合、Route 53 はそのレコードの値を使用してクエリへの応答を停止します。
- フェイルオーバーエイリアス、位置情報エイリアス、IP ベースエイリアス、レイテンシーエイリアス、または加重エイリアスレコードのグループ内のレコード、またはエイリアスレコードのための [Evaluate target health] (ターゲットの正常性の評価) で、[Yes] (はい) を選択します。エイリアスレコードが同じホストゾーン内の非エイリアスレコードを参照する場合、参照先レコードのヘルスチェックも指定する必要があります。エイリアスレコードにヘルスチェックを関連付けた上で、[Evaluate Target Health] (ターゲットの正常性の評価) で [Yes] (はい) を選択した場合、これらの設定は両方とも有効になります。詳細については、「エイリアスレコードにヘルスチェックを関連付けるとどうなるか」を参照してください。

ヘルスチェックでエンドポイントをドメイン名でのみ指定する場合は、エンドポイントごとに個別のヘルスチェックを作成します。例えば、www.example.com のコンテンツを配信する各 HTTP サーバーについて、ヘルスチェックを作成します。[ドメイン名] の値には、レコードの名前 (example.com) ではなく、サーバーのドメイン名 (us-east-2-www.example.com など) を指定します。

> **Important**
>
> この構成で、[ドメイン名] の値がレコードの名前と一致するヘルスチェックを作成し、それらのレコードにヘルスチェックを関連付けた場合、ヘルスチェックで予想できない結果が生じます。

記録 ID

IP ベースレコードのグループ内で、このレコードを一意に識別する値を入力します。

IP ベースエイリアスレコードに特有の値

IP ベースエイリアスレコードを作成する際は、以下の値を指定します。

> **Note**
>
> プライベートホストゾーン内に IP ベースエイリアスレコードを作成することは可能ですが、サポートはされていません。

詳細については、「エイリアスレコードと非エイリアスレコードの選択」を参照してください。

トピック

- ルーティングポリシー
- レコード名
- レコードタイプ
- 値/トラフィックのルーティング先
- ロケーション
- ヘルスチェック
- ターゲットの正常性の評価
- 記録 ID

ルーティングポリシー

[IP-based] (IP ベース) を選択します。

> **Note**
>
> プライベートホストゾーン内に IP ベースエイリアスレコードを作成することは可能ですが、サポートはされていません。

レコード名

トラフィックをルーティングするドメインまたはサブドメインの名前を入力します。デフォルト値はホストゾーンの名前です。

> **Note**
>
> ホストゾーンと同じ名前のレコードを作成する場合は、[レコード名] フィールドに値 (@ 記号など) を入力しないでください。

IP ベースレコードのグループ内で、すべてのレコードに同じ名前を入力します。

CNAME レコード

[レコードタイプ] の値が [CNAME] のレコードを作成する場合、レコードの名前をホストゾーンの名前と同じにすることはできません。

CloudFront ディストリビューションと Amazon S3 バケットへのエイリアス

指定する値は、トラフィックをルーティングする AWS リソースによって異なります。

- CloudFront ディストリビューション – ディストリビューションには、レコードの名前と一致する代替ドメイン名が含まれる必要があります。例えば、レコード名が acme.example.com の場合、CloudFront ディストリビューションには代替ドメイン名の 1 つとして acme.example.com が含まれる必要があります。詳細については、Amazon CloudFront デベロッパーガイドの「代替ドメイン名 (CNAME) を使用する」を参照してください。
- Amazon S3 バケット – レコード名は、Amazon S3 バケット名と一致する必要があります。例えば、 バケット名が [acme.example.com] である場合、このレコード名も [acme.example.com] である必要があります。

  また、ウェブサイトホスティング用にバケットを設定する必要があります。詳細については、Amazon Simple Storage Service ユーザーガイドのウェブサイトホスティング用にバケットを設定するを参照してください。

特殊文字

a ~ z、0 ~ 9、- (ハイフン) 以外の文字を指定する方法、および国際化されたドメイン名を指定する方法については、「DNS ドメイン名の形式」を参照してください。

ワイルドカード文字

名前にはアスタリスク (*) を使用できます。DNSは、名前の中の位置に応じて、「*」をワイルドカードまたはアスタリスク (ASCII 42) として処理します。詳細については、「ホストゾーンおよびレコード名のアスタリスク (*) を使用する」を参照してください。

レコードタイプ

DNS レコードタイプ。詳細については、「サポートされる DNS レコードタイプ」を参照してください。

トラフィックをルーティングする AWS リソースに基づいて、該当する値を選択します。IP ベースレコードのグループ内のすべてのレコードに対し、同じ値を選択します。

API Gateway のカスタムリージョン API またはエッジ最適化 API

[A — IPv4 アドレス] を選択します。

Amazon VPC インターフェイスのエンドポイント

[A — IPv4 アドレス] を選択します。

CloudFront 配信

[A — IPv4 アドレス] を選択します。

ディストリビューションに対して IPv6 が有効になっている場合は、2 つのレコードを作成します。1 つは [タイプ] として [A — IPv4 アドレス] の値を持つもの、もう 1つは [AAAA — IPv6 アドレス] の値を持つものとします。

App Runner サービス

[A — IPv4 アドレス] を選択します。

ローカル化されたサブドメインがある Elastic Beanstalk 環境

[A — IPv4 アドレス] を選択します。

ELB ロードバランサー

[A — IPv4 アドレス] または [AAAA — IPv6 アドレス] を選択します。

Amazon S3 バケット

[A — IPv4 アドレス] を選択します。

OpenSearch Service

[A — IPv4 アドレス] または [AAAA — IPv6 アドレス] を選択します。

このホストゾーン内の別のレコード

エイリアスを作成するレコードのタイプを選択します。[NS] および [SOA] 以外のすべてのタイプがサポートされます。

> **Note**
>
> ホストゾーン (Zone Apex といいます) と同じ名前のエイリアスレコードを作成する場合、[タイプ] の値が [CNAME] のレコードにトラフィックをルーティングすることはできません。これは、トラフィックがルーティングされているレコードとエイリアスレコードのタイプが同じでなければならず、Zone Apex の CNAME レコードの作成はエイリアスレコードであってもサポートされていないためです。

値/トラフィックのルーティング先

リストから選択する値、または フィールドに入力する値は、トラフィックをルーティングする AWS リソースによって異なります。

ターゲットにできる AWS リソースの詳細については、値/ルートトラフィックのエイリアスレコードの一般的な値を参照してください。

特定の AWS リソースにトラフィックをルーティングするように Route 53 を設定する方法の詳細については、「」を参照してくださいAWS リソースへのインターネットトラフィックのルーティング。

ロケーション

Route 53 による DNS クエリへの応答を、そのクエリの発信元の場所に基づいて行われるように設定する場合は、Route 53 がこのレコードの設定を使用して応答する対象の CIDR ロケーションを選択します。

> **Important**
>
> [Location] (ロケーション) の値を「Default」(デフォルト) とした IP ベースレコードを、1 つ作成することをお勧めします。これにより、レコードを作成していないロケーション、および Route 53 がロケーションを識別できない IP アドレスをカバーできます。

[Record name] (レコード名) および [Record type] (レコードタイプ) に IP ベースレコードと同じ値を指定して、非 IP ベースのレコードを作成することはできません。

詳細については、「IP ベースルーティング」を参照してください。

ヘルスチェック

Route 53 で、指定されたエンドポイントの正常性をチェックし、エンドポイントが正常であるときにのみ、このレコードを使用して DNS クエリに応答する場合は、ヘルスチェックを選択します。

Route 53 は、レコード内で指定されたエンドポイント、例えば、[値] フィールドの IP アドレスで指定されたエンドポイントの正常性はチェックしません。Route 53 は、レコードのヘルスチェックを選択したとき、ヘルスチェックで指定されたエンドポイントの正常性をチェックします。エンドポイントが正常であるかどうかを、Route 53 がどのように判断するかについては、「Amazon Route 53 でヘルスチェックの正常性を判断する方法」を参照してください。

ヘルスチェックをレコードに関連付けることに意味があるのは、Route 53 が複数のレコードの中から選択して DNS クエリに応答しており、その選択の一部をヘルスチェックのステータスに基づいて行うように Route 53 を設定する必要がある場合だけです。以下の設定でのみ、ヘルスチェックを使用してください。

- 名前、種類、およびルーティングポリシー (フェイルオーバーレコードや加重レコードなど) が同じレコードのグループ内のすべてのレコードのヘルスをチェックし、すべてのレコードのヘルスチェック ID を指定します。レコードのヘルスチェックが正常ではないエンドポイントを特定した場合、Route 53 はそのレコードの値を使用してクエリへの応答を停止します。
- フェイルオーバーエイリアス、位置情報エイリアス、IP ベースルーティングエイリアス、レイテンシーエイリアス、または加重エイリアスレコードのグループ内のレコード、またはエイリアスレコードのための [Evaluate target health] (ターゲットの正常性の評価) で、[Yes] (はい) を選択します。エイリアスレコードが同じホストゾーン内の非エイリアスレコードを参照する場合、参照先レコードのヘルスチェックも指定する必要があります。エイリアスレコードにヘルスチェックを関連付けた上で、[Evaluate Target Health] (ターゲットの正常性の評価) で [Yes] (はい) を選択した場合、これらの設定は両方とも有効になります。詳細については、「エイリアスレコードにヘルスチェックを関連付けるとどうなるか」を参照してください。

ヘルスチェックでドメイン名によってのみエンドポイントを指定する場合、エンドポイントごとにヘルスチェックを作成することをお勧めします。例えば、www.example.com のコンテンツを配信する各 HTTP サーバーについて、ヘルスチェックを作成します。[ドメイン名] の値には、レコードの名前 (example.com) ではなく、サーバーのドメイン名 (us-east-2-www.example.com など) を指定します。

> **Important**
>
> この構成で、[ドメイン名] の値がレコードの名前と一致するヘルスチェックを作成し、それらのレコードにヘルスチェックを関連付けた場合、ヘルスチェックで予想できない結果が生じます。

IP ベースエイリアスレコードでエンドポイントが正常でない場合、Route 53 より大きな関連付けられているロケーションからレコードを探します。例えば、米国の 1 つの州、米国、北米、およびすべての場所 ([Location] が [Default]) のレコードがあるとします。州のレコードのエンドポイントが正常でない場合、Route 53 は、正常なエンドポイントがあるレコードが見つかるまで、米国、北米、すべての場所のレコードを、この順序で確認します。すべての場所のレコードを確認しても、適用可能なレコードがすべて正常でない場合、Route 53 は最小の地理的リージョンのレコードの値を使用して DNS クエリに応答します。

ターゲットの正常性の評価

Route 53 で、このレコードを使用して [エンドポイント] で指定されたリソースの正常性を確認することによって DNS クエリに応答するかどうかを判定する場合は、[Yes] を選択します。

次の点に注意してください。

API Gateway のカスタムリージョン API とエッジ最適化 API

エンドポイントが API Gateway カスタムリージョン API またはエッジ最適化 API である場合、[ターゲットの正常性の評価] を [Yes] に設定するための特別な要件はありません。

CloudFront ディストリビューション

エンドポイントが CloudFront ディストリビューションの場合、[ターゲットの正常性の評価] を [Yes] に設定することはできません。

ローカル化されたサブドメインがある Elastic Beanstalk 環境

[エンドポイント] で Elastic Beanstalk 環境を指定し、その環境に ELB ロードバランサーが含まれている場合、Elastic Load Balancing はクエリをロードバランサーに登録されている正常な Amazon EC2 インスタンスにのみルーティングします。(複数の Amazon EC2 インスタンスが含まれている場合、環境には自動的に ELB ロードバランサーが含まれます。) [ターゲットの正常性の評価] を [Yes] に設定したとき、正常な Amazon EC2 インスタンスがない場合やロードバランサー自体が正常でない場合、Route 53 は他に利用可能なリソースがあれば、そこにクエリをルーティングします。

環境に 1 つの Amazon EC2 インスタンスが含まれている場合、特別な要件はありません。

ELB ロードバランサー

ヘルスチェックの動作はロードバランサーのタイプによって異なります。

- [Classic Load Balancers] – [エンドポイント] で ELB Classic Load Balancer を指定した場合、Elastic Load Balancing は、ロードバランサーに登録されている正常な Amazon EC2 インスタンスにのみクエリをルーティングします。[ターゲットの正常性の評価] を [Yes] に設定したとき、正常な EC2 インスタンスがない場合やロードバランサー自体が正常でない場合、Route 53 は他のリソースにクエリをルーティングします。
- アプリケーションと Network Load Balancer – ELB アプリケーションまたは Network Load Balancer を指定し、[ターゲットの正常性の評価] を Yes に設定すると、Route 53 は、ロードバランサーに関連付けられているターゲットグループの正常性に基づいて、クエリをロードバランサーにルーティングします。
  - アプリケーションまたはNetwork Load Balancerを正常であると見なすには、ターゲットを含むすべてのターゲットグループに少なくとも 1 つの正常なターゲットが含まれている必要があります。ターゲットグループに異常なターゲットのみが含まれている場合、ロードバランサーは異常であるとみなされ、Route 53 はクエリを他のリソースにルーティングします。
  - 登録されたターゲットを持たないターゲットグループは異常であるとみなされます。

> **Note**
>
> ロードバランサーを作成するときは、Elastic Load Balancing のヘルスチェックの設定を行います。これは Route 53 のヘルスチェックではありませんが、同様の機能を実行します。ELB ロードバランサーに登録する EC2 インスタンスに対しては Route 53 のヘルスチェックを作成しないでください。

S3 バケット

エンドポイントが S3 バケットである場合、[ターゲットの正常性の評価] を [Yes] に設定するための特別な要件はありません。

Amazon VPC インターフェイスのエンドポイント

エンドポイントが Amazon VPC インターフェイスエンドポイントである場合、[ターゲットの正常性の評価] を [Yes] に設定するための特別な要件はありません。

同じホストゾーンの他のレコード

Endpoint で指定した AWS リソースがレコードまたはレコードのグループ (加重レコードのグループなど) であるが、別のエイリアスレコードではない場合は、ヘルスチェックをエンドポイント内のすべてのレコードに関連付けることをお勧めします。詳細については、「ヘルスチェックを省略するとどうなるか」を参照してください。

記録 ID

IP ベースレコードのグループ内で、このレコードを一意に識別する値を入力します。

複数値回答レコードに固有の値

複数値回答レコードを作成するときは、以下の値を指定します。

> **Note**
>
> 複数値回答エイリアスレコードの作成はサポートされていません。

トピック

- ルーティングポリシー
- レコード名
- レコードタイプ
- TTL (秒)
- 値/トラフィックのルーティング先
- ヘルスチェック
- 記録 ID

ルーティングポリシー

[複数値回答] を選択します。

レコード名

トラフィックをルーティングするドメインまたはサブドメインの名前を入力します。デフォルト値はホストゾーンの名前です。

> **Note**
>
> ホストゾーンと同じ名前のレコードを作成する場合は、[レコード名] フィールドに値 (@ 記号など) を入力しないでください。

複数値レコードのグループで、すべてのレコードに同じ名前を入力します。

レコード名の詳細については、レコード名 を参照してください。

レコードタイプ

DNS レコードタイプ。詳細については、「サポートされる DNS レコードタイプ」を参照してください。

[NS] と [CNAME] を除く任意の値を選択します。

複数値回答レコードのグループ内のすべてのレコードに同じ値を選択します。

TTL (秒)

DNS 再帰リゾルバーがこのレコードに関する情報をキャッシュする秒単位の時間。より長い値 (172,800 秒、2 日など) を指定した場合、DNS 再帰リゾルバーが Route 53 に対して行う必要がある呼び出しの数を減らします。これにより、レイテンシーが短縮され、Route 53 サービスの請求額が削減されます。詳細については、「Amazon Route 53 によりドメインのトラフィックをルーティングする方法」を参照してください。

ただし、TTL に長い値を使用する場合、再帰的なリゾルバーは、Route 53 に最新の情報を問い合わせるまでに、長い間キャッシュ内の値を使用するため、レコードに対する変更 (例えば、新しい IP アドレス) が有効になるまでの時間が長くなります。既に使用されているドメインまたはサブドメインの設定を変更する場合、最初は 300 秒など短い値を指定し、新しい設定が正しいことを確認したら、値を増やすことをお勧めします。

このレコードをヘルスチェックに関連付ける場合は、クライアントがヘルスステータスの変化に迅速に応答するように、TTL を 60 秒以下に指定することをお勧めします。

> **Note**
>
> 同じ名前とタイプの複数値回答レコードを複数作成し、コンソールを使用している場合、[TTL] に異なる値を指定すると、Route 53 は、すべてのレコードの [TTL] 値を、指定された最後の値に変更します。

値/トラフィックのルーティング先

IP アドレス、またはレコードタイプに応じた別の値を選択します。[レコードタイプ] の値として適切な値を入力します。複数の値を入力する場合は、各値を個別の行に入力してください。

次の値にトラフィックをルーティングするか、次の値を指定できます。

- A — IPv4 アドレス

- AAAA — IPv6 アドレス
- CAA —認証局の承認
- MX — メール交換
- NAPTR — 名前付け権限ポインタ
- PTR — ポインタ
- SPF — センダーポリシーフレームワーク
- SRV — サービスロケーター
- TXT — テキスト

上記の値の詳細については、「common values for Value/Route traffic to」(値/トラフィックのルーティング先) を参照してください。

ヘルスチェック

Route 53 で、指定されたエンドポイントの正常性をチェックし、エンドポイントが正常であるときにのみ、このレコードを使用して DNS クエリに応答する場合は、ヘルスチェックを選択します。

Route 53 は、レコード内で指定されたエンドポイント、例えば、[値] フィールドの IP アドレスで指定されたエンドポイントの正常性はチェックしません。Route 53 は、レコードのヘルスチェックを選択したとき、ヘルスチェックで指定されたエンドポイントの正常性をチェックします。エンドポイントが正常であるかどうかを、Route 53 がどのように判断するかについては、「Amazon Route 53 でヘルスチェックの正常性を判断する方法」を参照してください。

ヘルスチェックをレコードに関連付けることに意味があるのは、Route 53 が複数のレコードの中から選択して DNS クエリに応答しており、その選択の一部をヘルスチェックのステータスに基づいて行うように Route 53 を設定する必要がある場合だけです。以下の設定でのみ、ヘルスチェックを使用してください。

- 名前、種類、およびルーティングポリシー (フェイルオーバーレコードや加重レコードなど) が同じレコードのグループ内のすべてのレコードのヘルスをチェックし、すべてのレコードのヘルスチェック ID を指定します。レコードのヘルスチェックが正常ではないエンドポイントを特定した場合、Route 53 はそのレコードの値を使用してクエリへの応答を停止します。
- フェイルオーバーエイリアス、位置情報エイリアス、レイテンシーエイリアス、または加重エイリアスレコードのグループ内のレコード、またはエイリアスレコードに対する [ターゲットの正常性の評価] に [Yes]を選択します。エイリアスレコードが同じホストゾーン内の非エイリアスレコードを参照する場合、参照先レコードのヘルスチェックも指定する必要があります。エイリアスレ

コードにヘルスチェックを関連付けた上で、[Evaluate Target Health] (ターゲットの正常性の評価) で [Yes] (はい) を選択した場合、これらの設定は両方とも有効になります。詳細については、「エイリアスレコードにヘルスチェックを関連付けるとどうなるか」を参照してください。

ヘルスチェックでドメイン名によってのみエンドポイントを指定する場合、エンドポイントごとにヘルスチェックを作成することをお勧めします。例えば、www.example.com のコンテンツを配信する各 HTTP サーバーについて、ヘルスチェックを作成します。[ドメイン名] の値には、レコードの名前 (example.com) ではなく、サーバーのドメイン名 (us-east-2-www.example.com など) を指定します。

> **Important**
>
> この構成で、[ドメイン名] の値がレコードの名前と一致するヘルスチェックを作成し、それらのレコードにヘルスチェックを関連付けた場合、ヘルスチェックで予想できない結果が生じます。

記録 ID

複数値回答レコードのグループに、このレコードを一意に識別する値を入力します。

加重レコードに固有の値

加重レコードを作成するときは、以下の値を指定します。

トピック

- ルーティングポリシー
- レコード名
- レコードタイプ
- TTL (秒)
- 値/トラフィックのルーティング先
- Weight
- ヘルスチェック
- 記録 ID

ルーティングポリシー

[Weighted] を選択します。

レコード名

トラフィックをルーティングするドメインまたはサブドメインの名前を入力します。デフォルト値はホストゾーンの名前です。

> **Note**
>
> ホストゾーンと同じ名前のレコードを作成する場合は、[レコード名] フィールドに値 (@ 記号など) を入力しないでください。

加重レコードのグループで、すべてのレコードに同じ名前を入力します。

レコード名の詳細については、レコード名 を参照してください。

レコードタイプ

DNS レコードタイプ。詳細については、「サポートされる DNS レコードタイプ」を参照してください。

加重レコードのグループ内のすべてのレコードに同じ値を選択します。

TTL (秒)

DNS 再帰リゾルバーがこのレコードに関する情報をキャッシュする秒単位の時間。より長い値 (172,800 秒、2 日など) を指定した場合、DNS 再帰リゾルバーが Route 53 に対して行う必要がある呼び出しの数を減らします。これにより、レイテンシーが短縮され、Route 53 サービスの請求額が削減されます。詳細については、「Amazon Route 53 によりドメインのトラフィックをルーティングする方法」を参照してください。

ただし、TTL に長い値を指定すると、レコードの変更 (新しい IP アドレスなど) が有効になるまでに時間がかかります。再帰リゾルバーは、Route 53 に最新情報を要求する前に、キャッシュ内の値を長期間使用します。既に使用されているドメインまたはサブドメインの設定を変更する場合は、まず 300 秒などの短い値を指定し、新しい設定が正しいことを確認したら値を増やします。

このレコードをヘルスチェックに関連付ける場合は、クライアントがヘルスステータスの変化に迅速に応答するように、TTL を 60 秒以下に指定します。

この加重レコードのグループに含まれるすべてのレコードについて、[TTL] に同じ値を指定する必要があります。

> **Note**
>
> 同じ名前とタイプを持つ 2 つ以上の加重レコードを作成し、TTL に異なる値を指定すると、Route 53 はすべてのレコードの TTL の値を最後に設定した値に変更します。

加重レコードのグループに、ELB ロードバランサーにトラフィックをルーティングする 1 つ以上の加重エイリアスレコードが含まれている場合は、同じ名前とタイプを持つすべての非エイリアス加重レコードに対して 60 秒の TTL を指定します。60 秒 (ロードバランサーの TTL) 以外の値を指定すると、[Weight (重み)] に指定する値の効果が変わります。

値/トラフィックのルーティング先

IP アドレス、またはレコードタイプに応じた別の値を選択します。[レコードタイプ] の値として適切な値を入力します。[CNAME] を除くすべてのタイプは、複数の値を入力できます。各値は個別の行に入力します。

次の値にトラフィックをルーティングするか、次の値を指定できます。

- A — IPv4 アドレス

- AAAA — IPv6 アドレス
- CAA —認証局の承認
- CNAME — 正規名
- MX — メール交換
- NAPTR — 名前付け権限ポインタ
- PTR — ポインタ
- SPF — センダーポリシーフレームワーク
- SRV — サービスロケーター
- TXT — テキスト

上記の値の詳細については、「common values for Value/Route traffic to」(値/トラフィックのルーティング先) を参照してください。

Weight

Route 53 が現在のレコードを使用して応答する DNS クエリの割合を決定する値。Route 53 は、同じ DNS 名とタイプの組み合わせがあるレコードの重みの合計を計算します。その後、Route 53 はリソースの重みと合計の比率に基づいてクエリに応答します。

[レコード名] および [レコードタイプ] の値が加重レコードと同じである非加重レコードを作成することはできません。

0 ~ 255 の整数を入力します。リソースへのルーティングを停止するには、重みを 0 に設定します。グループ内のすべてのレコードに対して [Weight (重み)] を 0 に設定した場合、トラフィックは等しい確率ですべてのリソースにルーティングされます。これにより、加重レコードのグループのルーティングを無効にしないようにできます。

加重レコードにヘルスチェックを割り当てる場合、[Weight (重み)] を 0 に設定した結果は異なります。詳細については、「ヘルスチェックが設定されている場合に Amazon Route 53 がレコードを選択する方法」を参照してください。

ヘルスチェック

Route 53 で、指定されたエンドポイントの正常性をチェックし、エンドポイントが正常であるときにのみ、このレコードを使用して DNS クエリに応答する場合は、ヘルスチェックを選択します。

Route 53 は、レコード内で指定されたエンドポイント、例えば、[値] フィールドの IP アドレスで指定されたエンドポイントの正常性はチェックしません。Route 53 は、レコードのヘルスチェックを

選択したとき、ヘルスチェックで指定されたエンドポイントの正常性をチェックします。エンドポイントが正常であるかどうかを、Route 53 がどのように判断するかについては、「Amazon Route 53 でヘルスチェックの正常性を判断する方法」を参照してください。

ヘルスチェックとレコードの関連付けは、Route 53 が DNS クエリに応答するレコードを 2 つ以上選択していて、Route 53 がヘルスチェックのステータスに部分的に基づいている場合にのみ便利です。以下の設定でのみ、ヘルスチェックを使用してください。

- 名前、種類、およびルーティングポリシー (フェイルオーバーレコードや加重レコードなど) が同じレコードのグループ内のすべてのレコードのヘルスをチェックし、すべてのレコードのヘルスチェック ID を指定します。レコードのヘルスチェックで異常なエンドポイントが指定されている場合、Route 53 はそのレコードの値を使用してクエリへの応答を停止します。
- フェイルオーバーエイリアス、位置情報エイリアス、レイテンシーエイリアス、IP ベースエイリアス、または加重エイリアスレコードのグループ内にあるエイリアスレコードまたはレコードの [Evaluate target health] (ターゲットのヘルスを評価) で、[Yes] (はい) を選択します。エイリアスレコードが同じホストゾーン内の非エイリアスレコードを参照する場合、参照先レコードのヘルスチェックも指定する必要があります。エイリアスレコードにヘルスチェックを関連付けた上で、[Evaluate Target Health] (ターゲットの正常性の評価) で [Yes] (はい) を選択した場合、これらの設定は両方とも有効になります。詳細については、「エイリアスレコードにヘルスチェックを関連付けるとどうなるか」を参照してください。

ヘルスチェックでエンドポイントをドメイン名でのみ指定する場合は、エンドポイントごとに個別のヘルスチェックを作成します。例えば、www.example.com のコンテンツを配信する各 HTTP サーバーについて、ヘルスチェックを作成します。[ドメイン名] の値には、レコードの名前 (example.com) ではなく、サーバーのドメイン名 (us-east-2-www.example.com など) を指定します。

> **Important**
>
> この構成で、[ドメイン名] の値がレコードの名前と一致するヘルスチェックを作成し、それらのレコードにヘルスチェックを関連付けた場合、ヘルスチェックで予想できない結果が生じます。

記録 ID

加重レコードのグループ内で、このレコードを一意に識別する値を入力します。

加重エイリアスレコードに固有の値

加重エイリアスレコードを作成するときは、以下の値を指定します。詳細については、「エイリアスレコードと非エイリアスレコードの選択」を参照してください。

トピック

- ルーティングポリシー
- レコード名
- レコードタイプ
- 値/トラフィックのルーティング先
- Weight
- ヘルスチェック
- ターゲットの正常性の評価
- 記録 ID

ルーティングポリシー

[加重] を選択します。

レコード名

トラフィックをルーティングするドメインまたはサブドメインの名前を入力します。デフォルト値はホストゾーンの名前です。

> **Note**
>
> ホストゾーンと同じ名前のレコードを作成する場合は、[名前] フィールドに値 (@ 記号など) を入力しないでください。

加重レコードのグループで、すべてのレコードに同じ名前を入力します。

レコード名の詳細については、レコード名 を参照してください。

レコードタイプ

DNS レコードタイプ。詳細については、「サポートされる DNS レコードタイプ」を参照してください。

トラフィックをルーティングする AWS リソースに基づいて、該当する値を選択します。

API Gateway のカスタムリージョン API またはエッジ最適化 API

[A — IPv4 アドレス] を選択します。

Amazon VPC インターフェイスのエンドポイント

[A — IPv4 アドレス] を選択します。

CloudFront 配信

[A — IPv4 アドレス] を選択します。

ディストリビューションに対して IPv6 が有効になっている場合は、2 つのレコードを作成します。1 つは [タイプ] として [A — IPv4 アドレス] の値を持つもの、もう 1つは [AAAA — IPv6 アドレス] の値を持つものとします。

App Runner サービス

[A — IPv4 アドレス] を選択します。

ローカル化されたサブドメインがある Elastic Beanstalk 環境

[A — IPv4 アドレス] を選択します。

ELB ロードバランサー

[A — IPv4 アドレス] または [AAAA — IPv6 アドレス] を選択します。

Amazon S3 バケット

[A — IPv4 アドレス] を選択します。

OpenSearch Service

[A — IPv4 アドレス] または [AAAA — IPv6 アドレス] を選択します。

このホストゾーン内の別のレコード

エイリアスを作成するレコードのタイプを選択します。[NS] および [SOA] 以外のすべてのタイプがサポートされます。

> **Note**
>
> ホストゾーン (Zone Apex といいます) と同じ名前のエイリアスレコードを作成する場合、[タイプ] の値が [CNAME] のレコードにトラフィックをルーティングすることはでき

ません。これは、トラフィックがルーティングされているレコードとエイリアスレコードのタイプが同じでなければならず、Zone Apex の CNAME レコードの作成はエイリアスレコードであってもサポートされていないためです。

加重レコードのグループ内のすべてのレコードに同じ値を選択します。

値/トラフィックのルーティング先

リストから選択する値、または フィールドに入力する値は、トラフィックをルーティングする AWS リソースによって異なります。

ターゲットにできる AWS リソースの詳細については、値/ルートトラフィックのエイリアスレコードの一般的な値を参照してください。

特定の AWS リソースにトラフィックをルーティングするように Route 53 を設定する方法の詳細については、「」を参照してくださいAWS リソースへのインターネットトラフィックのルーティング。

Weight

Route 53 が現在のレコードを使用して応答する DNS クエリの割合を決定する値。Route 53 は、同じ DNS 名とタイプの組み合わせがあるレコードの重みの合計を計算します。その後、Route 53 はリソースの重みと合計の比率に基づいてクエリに応答します。

[レコード名] および [レコードタイプ] の値が加重レコードと同じである非加重レコードを作成することはできません。

0 ~ 255 の整数を入力します。リソースへのルーティングを無効にするには、[Weight (重み)] に 0 を設定します。グループ内のすべてのレコードに対して [Weight (重み)] を 0 に設定した場合、トラフィックは等しい確率ですべてのリソースにルーティングされます。これにより、加重レコードのグループのルーティングを誤って無効にする心配がなくなります。

加重レコードにヘルスチェックを割り当てる場合、[Weight (重み)] を 0 に設定した結果は異なります。詳細については、「ヘルスチェックが設定されている場合に Amazon Route 53 がレコードを選択する方法」を参照してください。

ヘルスチェック

Route 53 で、指定されたエンドポイントの正常性をチェックし、エンドポイントが正常であるときにのみ、このレコードを使用して DNS クエリに応答する場合は、ヘルスチェックを選択します。

Route 53 は、レコード内で指定されたエンドポイント、例えば、[値] フィールドの IP アドレスで指定されたエンドポイントの正常性はチェックしません。Route 53 は、レコードのヘルスチェックを選択したとき、ヘルスチェックで指定されたエンドポイントの正常性をチェックします。エンドポイントが正常であるかどうかを、Route 53 がどのように判断するかについては、「Amazon Route 53 でヘルスチェックの正常性を判断する方法」を参照してください。

ヘルスチェックをレコードに関連付けることに意味があるのは、Route 53 が複数のレコードの中から選択して DNS クエリに応答しており、その選択の一部をヘルスチェックのステータスに基づいて行うように Route 53 を設定する必要がある場合だけです。以下の設定でのみ、ヘルスチェックを使用してください。

- 名前、種類、およびルーティングポリシー (フェイルオーバーレコードや加重レコードなど) が同じレコードのグループ内のすべてのレコードのヘルスをチェックし、すべてのレコードのヘルスチェック ID を指定します。レコードのヘルスチェックが正常ではないエンドポイントを特定した場合、Route 53 はそのレコードの値を使用してクエリへの応答を停止します。
- フェイルオーバーエイリアス、位置情報エイリアス、レイテンシーエイリアス、IP ベースエイリアス、または加重エイリアスレコードのグループ内にあるエイリアスレコードまたはレコードの [Evaluate target health] (ターゲットのヘルスを評価) で、[Yes] (はい) を選択します。エイリアスレコードが同じホストゾーン内の非エイリアスレコードを参照する場合、参照先レコードのヘルスチェックも指定する必要があります。エイリアスレコードにヘルスチェックを関連付けた上で、[Evaluate Target Health] (ターゲットの正常性の評価) で [Yes] (はい) を選択した場合、これらの設定は両方とも有効になります。詳細については、「エイリアスレコードにヘルスチェックを関連付けるとどうなるか」を参照してください。

ヘルスチェックでドメイン名によってのみエンドポイントを指定する場合、エンドポイントごとにヘルスチェックを作成することをお勧めします。例えば、www.example.com のコンテンツを配信する各 HTTP サーバーについて、ヘルスチェックを作成します。[ドメイン名] の値には、レコードの名前 (example.com) ではなく、サーバーのドメイン名 (us-east-2-www.example.com など) を指定します。

> **Important**
>
> この構成で、[ドメイン名] の値がレコードの名前と一致するヘルスチェックを作成し、それらのレコードにヘルスチェックを関連付けた場合、ヘルスチェックで予想できない結果が生じます。

ターゲットの正常性の評価

Route 53 で、このレコードを使用して [エンドポイント] で指定されたリソースの正常性を確認することによって DNS クエリに応答するかどうかを判定する場合は、[Yes] を選択します。

次の点に注意してください。

API Gateway のカスタムリージョン API とエッジ最適化 API

エンドポイントが API Gateway カスタムリージョン API またはエッジ最適化 API である場合、[Evaluate target health] (ターゲットヘルスを評価) を [Yes] (はい) に設定するための特別な要件はありません。

CloudFront ディストリビューション

エンドポイントが CloudFront ディストリビューションの場合、[ターゲットの正常性の評価] を [Yes] に設定することはできません。

ローカル化されたサブドメインがある Elastic Beanstalk 環境

[エンドポイント] で Elastic Beanstalk 環境を指定し、その環境に ELB ロードバランサーが含まれている場合、Elastic Load Balancing はクエリをロードバランサーに登録されている正常な Amazon EC2 インスタンスにのみルーティングします。(複数の Amazon EC2 インスタンスが含まれている場合、環境には自動的に ELB ロードバランサーが含まれます。) [ターゲットの正常性の評価] を [Yes] に設定したとき、正常な Amazon EC2 インスタンスがない場合やロードバランサー自体が正常でない場合、Route 53 は他に利用可能なリソースがあれば、そこにクエリをルーティングします。

環境に 1 つの Amazon EC2 インスタンスが含まれている場合、特別な要件はありません。

ELB ロードバランサー

ヘルスチェックの動作はロードバランサーのタイプによって異なります。

- [Classic Load Balancers] – [エンドポイント] で ELB Classic Load Balancer を指定した場合、Elastic Load Balancing は、ロードバランサーに登録されている正常な Amazon EC2 インスタンスにのみクエリをルーティングします。[ターゲットの正常性の評価] を [Yes] に設定したとき、正常な EC2 インスタンスがない場合やロードバランサー自体が正常でない場合、Route 53 は他のリソースにクエリをルーティングします。
- アプリケーションと Network Load Balancer – ELB アプリケーションまたは Network Load Balancer を指定し、[ターゲットの正常性の評価] を Yes に設定すると、Route 53 は、ロードバランサーに関連付けられているターゲットグループの正常性に基づいて、クエリをロードバランサーにルーティングします。

- アプリケーションまたはNetwork Load Balancerを正常であると見なすには、ターゲットを含むすべてのターゲットグループに少なくとも 1 つの正常なターゲットが含まれている必要があります。ターゲットグループに異常なターゲットのみが含まれている場合、ロードバランサーは異常であるとみなされ、Route 53 はクエリを他のリソースにルーティングします。
- 登録されたターゲットを持たないターゲットグループは異常であるとみなされます。

> **Note**
>
> ロードバランサーを作成するときは、Elastic Load Balancing のヘルスチェックの設定を行います。これは Route 53 のヘルスチェックではありませんが、同様の機能を実行します。ELB ロードバランサーに登録する EC2 インスタンスに対しては Route 53 のヘルスチェックを作成しないでください。

S3 バケット

エンドポイントが S3 バケットである場合、[ターゲットの正常性の評価] を [Yes] に設定するための特別な要件はありません。

Amazon VPC インターフェイスのエンドポイント

エンドポイントが Amazon VPC インターフェイスエンドポイントである場合、[ターゲットの正常性の評価] を [Yes] に設定するための特別な要件はありません。

同じホストゾーンの他のレコード

Endpoint で指定した AWS リソースがレコードまたはレコードのグループ (加重レコードのグループなど) で、別のエイリアスレコードではない場合は、ヘルスチェックをエンドポイント内のすべてのレコードに関連付けることをお勧めします。詳細については、「ヘルスチェックを省略するとどうなるか」を参照してください。

記録 ID

加重レコードのグループ内で、このレコードを一意に識別する値を入力します。

ゾーンファイルをインポートしてレコードを作成する

別の DNS サービスプロバイダーから移行していて、そのプロバイダーが現在の DNS 設定をゾーンファイルにエクスポートできる場合は、そのゾーンファイルをインポートすることで、Amazon Route 53 ホストゾーンのすべてのレコードをすばやく作成できます。

> **Note**
>
> ゾーンファイルは、BIND と呼ばれる標準形式を使用して、レコードをテキスト形式で表示します。ゾーンファイルの形式については、Wikipedia のゾーンファイルのエントリを参照してください。詳細については、RFC 1034、ドメイン名 - 概念と施設セクション 3.6.1、および RFC 1035、ドメイン名 - 実装と仕様セクション 5 を参照してください。

ゾーンファイルをインポートしてレコードを作成する場合は、次の点に注意してください。

- ゾーンファイルは、RFC に準拠した形式である必要があります。
- ゾーンファイル内のレコードのドメイン名は、ホストゾーンの名前に一致する必要があります。
- Route 53 では、`$ORIGIN` と `$TTL` のキーワードがサポートされます。ゾーンファイルに `$GENERATE` または `$INCLUDE` のキーワードが含まれる場合、インポートは失敗し、Route 53 からエラーが返されます。
- ゾーンファイルをインポートしたとき、Route 53 はゾーンファイル内の SOA レコードを無視します。Route 53 では、ホストゾーンと同じ名前を持つ NS レコードもすべて無視されます。
- 最大 1000 個のレコードをインポートすることができます。
- ゾーンファイルに表示されるレコードが既にホストゾーンに含まれている場合、インポートプロセスは失敗し、レコードは作成されません。
- バックスラッシュ文字を含む TXT レコードの場合、ゾーンファイルインポートプロセスは特定のバックスラッシュシーケンスをコントロール文字として解釈します。TXT レコード値にリテラルバックスラッシュ文字を含めるには:
  - ゾーンファイルで二重バックスラッシュ (`\\\\`) を使用し、最終的な TXT レコードで 1 つのリテラルバックスラッシュを表します。
  - 例えば、TXT レコードに `\\jYTDWqH...` (リテラルバックスラッシュと j を持つ) を含める必要がある場合、ゾーンファイルに `\\\\jYTDWqH...` を指定します。

  これは、リテラルバックスラッシュ文字を含んだ ACME チャレンジレコードやその他の TXT レコードにおいて特に重要です。
- 長い TXT レコード (DKIM レコードなど) の場合、ゾーンファイルのインポートプロセスでは、コンテンツを複数の文字列に分割できます。複数の文字列を持つ TXT レコードを作成するには:
  - ゾーンファイルで、同じレコード名とタイプで別々の行を使用します。

Example

```
example.com. 300 IN TXT "v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC"
example.com. 300 IN TXT
 "7fCC6C13dM9tXuJmUBH7D4Vw8y1ByJ8z9QX2fvLm3pN4sR5tU6vW7xY8zA9bC0dE1f"
example.com. 300 IN TXT
 "G2hI3jK4lM5nO6pQ7rS8tU9vW0xY1zA2bC3dE4fG5hI6jK7lM8nO9pQ0rS1tU2vW3x"
```

インポートプロセスでは、これらが複数の文字列を持つ単一の TXT レコードに自動的に結合されます。各文字列には最大 65,535 文字を含めることができます。長い文字列を単一の引用符で囲まれた値に連結しないでください。

- ゾーンファイルを確認して、必要に応じてレコード名に末尾のドットが含まれているか除外されているかを確認することをお勧めします。
  - ゾーンファイル内のレコードの名前の末尾がドットである場合 (`example.com.`)、その名前はインポートプロセスによって完全修飾ドメイン名と解釈され、その名前で Route 53 レコードが作成されます。
  - ゾーンファイル内のレコードの名前の末尾がドットでない場合 (`www`)、その名前はインポートプロセスによってゾーンファイル内のドメイン名 (`example.com`) と連結され、連結後の名前 (`www.example.com`) で Route 53 レコードが作成されます。

エクスポートプロセスがレコードの完全修飾ドメイン名に末尾のドットを追加しない場合、Route 53 インポートプロセスはレコードの名前にドメイン名を追加します。たとえば、レコードをホストゾーン `example.com` にインポートし、ゾーンファイルの MX レコードの名前は `mail.example.com` で末尾のドットがない場合、Route 53 インポートプロセスでは `mail.example.com.example.com` という名前の MX レコードが作成されます。

> **Important**
>
> CNAME、MX、PTR、および SRV レコードの場合も、RDATA 値に含まれるドメイン名にこの動作が適用されます。たとえば、`example.com` のゾーンファイルがあるとします。ゾーンファイル内の CNAME レコード (`support`、末尾にドットなし) に RDATA 値 `www.example.com` (同様に末尾にドットなし) が含まれている場合、インポートプロセスによって、`www.example.com.example.com` にトラフィックをルーティングする `support.example.com` という名前の Route 53 レコードが作成されます。ゾーンファイルをインポートする前に、RDATA 値を確認し、必要に応じて更新してください。バック

スラッシュ文字を含む TXT レコードの場合は、ゾーンファイルで二重バックスラッシュ (\\\\) を使用してリテラルバックスラッシュを表します。

Route 53 はレコードのゾーンファイルへのエクスポートをサポートしていません。

> **Note**
>
> ホストゾーンと同じ名前のレコードを作成する場合は、[名前] フィールドに値 (@ 記号など) を入力しないでください。

ゾーンファイルをインポートしてレコードを作成するには

1. ドメインを現在処理している DNS サービスプロバイダーからゾーンファイルを取得します。プロセスと条件はプロバイダーによって異なります。レコードをゾーンファイルまたは BIND ファイルにエクスポートまたは保存する方法については、プロバイダーのインターフェイスおよびドキュメントを参照してください。

   プロセスが明確でない場合は、現在の DNS プロバイダーにレコードリストまたはゾーンファイルデータのサポートを依頼してみてください。
2. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
3. ナビゲーションペインで [Hosted zones] を選択します。
4. [ホストゾーン] ページで、新しいホストゾーンを作成します。
   a. [ホストゾーンの作成] を選択します。
   b. ドメインの名前 (およびオプションでコメント) を入力します。
   c. [作成] を選択します。
5. [ゾーンファイルのインポート] を選択します。
6. [ゾーンファイルのインポート] ペインで、ゾーンファイルの内容を [ゾーンファイル] テキストボックスに貼り付けます。
7. [Import] を選択します。

> **Note**
>
> ゾーンファイル内のレコードの数によっては、レコードが作成されるまで数分かかる場合があります。

8. ドメインに別の DNS サービスを使用している場合 (ドメインを別のレジストラに登録している場合に一般的)、DNS サービスを Route 53 に移動します。このステップが完了すると、レジストラはドメインの DNS クエリの DNS サービス として Route 53 を識別し、クエリは Route 53 DNS サーバーに移行し始めます。(通常、以前の DNS サービスのデータが DNS リゾルバーにキャッシュされるため、DNS クエリが Route 53 に送信されるまでに 1 ~ 2 日遅延があります)。詳細については、「Amazon Route 53 を既存ドメインの DNS サービスとして使用する」を参照してください。

レコードの編集

以下の手順では、Amazon Route 53 コンソールを使用してレコードを編集する方法について説明します。Route 53 API を使用してレコードを編集する方法については、Amazon Route 53 API リファレンスの「ChangeResourceRecordSets」を参照してください。

> **Note**
>
> レコードの変更が Route 53 DNS サーバーに伝達されるまでにしばらく時間がかかります。現在、変更が伝達されたことを確認するには、GetChange API アクションを使用する方法しかありません。通常、変更は 60 秒以内にすべての Route 53 ネームサーバーに伝播されます。

Route 53 コンソールを使用してレコードを編集するには

1. エイリアスレコードを編集しない場合は、ステップ 2 に進みます。

   Elastic Load Balancing Classic Load Balancer、Application Load Balancer、または Network Load Balancer にトラフィックをルーティングするエイリアスレコードを編集する場合、別のアカウントで Route 53 ホストゾーンとロードバランサーを作成していたら、手順「Elastic Load Balancing ロードバランサーの DNS 名を取得する」を実行してロードバランサーの DNS 名を取得します。

他の AWS リソースのエイリアスレコードを編集する場合は、ステップ 2 に進みます。

2. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
3. ナビゲーションペインで [Hosted zones] を選択します。
4. [ホストゾーン] ページで、編集するレコードが含まれているホストゾーンの行を選択します。
5. 編集するレコードの行を選択し、[レコードの編集] ペインに変更を入力します。
6. 適切な値を入力します。詳細については、「Amazon Route 53 レコードの作成時または編集時に指定する値」を参照してください
7. [Save changes] (変更の保存) をクリックします。
8. レコードを複数編集する場合は、ステップ 5 ~ 7 を繰り返します。

レコードの削除

次の手順では、Route 53 コンソールを使用してレコードを削除する方法を説明します。Route 53 API を使用してレコードを削除する方法については、Amazon Route 53 API リファレンスの「ChangeResourceRecordSets」を参照してください。

> **Note**
>
> レコードの変更が Route 53 DNS サーバーに伝達されるまでにしばらく時間がかかります。現在、変更が伝達されたことを確認するには、GetChange API アクションを使用する方法しかありません。通常、変更は 60 秒以内にすべての Route 53 ネームサーバーに伝播されます。

レコードを削除するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. [ホストゾーン] ページで、削除するレコードが含まれているホストゾーンの行を選択します。
3. レコードのリストで、削除するレコードを選択します。

   複数の連続するレコードを選択するには、最初の行を選択し、Shift キーを押したまま最後の行を選択します。複数の連続しないレコードを選択するには、最初の行を選択し、Ctrl キーを押したまま追加の行を選択します。

[タイプ] の値が [NS] または [SOA] のレコードを削除することはできません。

4. [Delete (削除)] を選択します。
5. [削除] を選択してダイアログボックスを閉じます。

レコードの一覧表示

以下の手順は、Amazon Route 53 コンソールを使用してホストゾーンのレコードを一覧表示する方法を説明しています。Route 53 API を使用してレコードを一覧表示する方法については、「Amazon Route 53 API リファレンス」の「ListResourceRecordSets」を参照してください。

レコードを一覧表示するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [Hosted zones] を選択します。
3. [Hosted Zones] ページで、ホストゾーンの名前を選択します。
4. 検索モードを変更するには、[レコード] テーブルの右上にある歯車アイコンを選択します。オプションのいずれかを選択します。

   - 自動

     このモードでは、サービスは多数のレコードに基づくフィルターを使用します。2,000 レコードまではフル、2,000 レコードを超える場合は高速になります

   - フル

     このモードでは、すべての検索フィルターが使用できますが、その場合検索のパフォーマンスが低下する可能性があります。

   - 高速

     このモードでは、一部の高度な機能は使用できませんが、検索は速くなります。

特定のレコードのみを表示するには、レコードのリストの上に検索語を入力します。自動モードでは、検索動作は、ホストゾーンに最大 2,000 個のレコードがあるか、2,000 個を超えるレコードがあるかによって異なります。

最大 2,000 レコードおよびフルモード

- 特定の値を含んでいるレコードを表示するには、サーチバーに値を入力し [Enter] を押します。例えば、192.0 で始まる IP アドレスを持つレコードを表示するには、[Search (検索)] フィールドにその値を入力して Enter を押します。
- DNS レコードタイプが同じレコードのみを表示するには、ドロップダウンリストで [レコードタイプ] を選択し、レコードタイプを入力します。
- エイリアスレコードのみを表示するには、ドロップダウンリストで [エイリアス] を選択し、**Yes** と入力します。
- 加重レコードのみを表示するには、ドロップダウンリストで [ルーティングポリシー] を選択し、**WEIGHTED** と入力します。

2,000 を超えるレコードおよび高速モード

- レコード値ではなく、レコード名でのみ検索できます。また、レコードタイプ、エイリアスレコードまたは加重レコードに基づいてフィルタリングすることはできません。

  この操作を行うには、[フィルター] テキストボックスにカーソルを置き、[プロパティ]、[レコード名] の順に選択します。
- 3 つのラベル (ドットで区切られた 3 つの部分) を持つレコードの場合は、検索フィールドに値を入力して [Enter] を押すと、Route 53 コンソールで、レコード名の右から 3 番目のラベルの末尾にワイルドカードを追加した検索が自動的に実行されます。例えば、ホストゾーン example.com に、record1.example.com ~ record100.example.com の 100 個のレコードが含まれているとします。(Record1 は右から 3 番目のラベルです。) ここで、以下の値を検索した場合の動作を示します。
  - record1 – Route 53 コンソールで record1*.example.com が検索されます。record1.example.com、record10.example.com ~ record19.example.com、および record100.example.com が返されます。
  - record1.example.com – 前の例と同様に、コンソールで record1*.example.com が検索され、同じレコードが返されます。
  - 1 – コンソールで 1*.example.com が検索されます。返されるレコードはありません。
  - example – コンソールで example*.example.com が検索されます。返されるレコードはありません。
  - example.com – この場合、コンソールでワイルドカード検索は実行されません。ホストゾーンのすべてのレコードが返されます。
  - 自動検索モード — この検索モードを使用する場合、検索できるようにするために、先にレコード名などのプロパティを指定しておく必要があります。

> **Note**
>
> 右から 3 番目のラベルに 1 つ以上のハイフンが含まれている場合 (third-label.example.com など) で、3 番目のラベルのハイフンの直前までの部分 (この例では third) を検索した場合、Route 53 から返されるレコードはありません。代わりに、ハイフンを含める (third- で検索) か、ハイフン直前の文字を省略 (third) します。

- 4 つ以上のラベルを持つレコードの場合は、レコードの正確な名前を指定する必要があります。ワイルドカード検索はサポートされていません。例えば、ホストゾーンに label4.record1.example.com という名前のレコードが含まれている場合、検索フィールドに [label4.record1.example.com] と指定した場合にのみ、そのレコードを見つけることができます。

Amazon Route 53 での DNSSEC 署名の設定

ドメインネームシステムセキュリティ拡張 (DNSSEC) 署名により、DNS リゾルバーは DNS 応答が Amazon Route 53 から送信され、改ざんされていないことを検証できます。DNSSEC 署名を使用すると、ホストゾーンへのすべての応答は、公開キー暗号化を使用して署名されます。DNSSEC の概要については、「AWS re:Invent 2021 - Amazon Route 53: A year in review」の DNSSEC セクションを参照してください。

この章では、Route 53 の DNSSEC 署名を有効にする方法、キー署名キー (KSKs) の操作方法、および問題のトラブルシューティング方法について説明します。で DNSSEC 署名を使用する AWS マネジメントコンソール か、 API を使用してプログラムで操作できます。CLI または SDK を使用して Route 53 を操作する方法の詳細については、「Amazon Route 53 を設定する」を参照してください。

DNSSEC 署名を有効にする前に、以下の点に注意してください。

- ゾーンの停止を防ぎ、ドメインが使用できなくなる問題を回避するには、DNSSEC エラーにすばやく対処し解決する必要があります。DNSSECInternalFailure または DNSSECKeySigningKeysNeedingAction エラーが検出されるたびにアラートを受け取ることができる、CloudWatch アラームをセットアップしておくことを強くお勧めします。詳細については、「Amazon CloudWatch を使用したホストゾーンのモニタリング」を参照してください。
- DNSSEC には、キー署名キー (KSK) とゾーン署名キー (ZSK) の 2 種類のキーがあります。Route 53 の DNSSEC 署名での各 KSK は、お客様が所有する AWS KMS 内の非対称カスタ

マーマネージドキーに基づいています。必要に応じて行うローテーションを初めとして、KSK管理の責任はお客様が持ちます。ZSK 管理は Route 53 によって実行されます。

- ホストゾーンで DNSSEC 署名を有効にすると、Route 53 は TTL を 1 週間に制限します。ホストゾーンのレコードに対して TTL を 1 週間以上設定しても、エラーは発生しません。ただし、Route 53 では、レコードに対して 1 週間の TTL が強制されます。TTL が 1 週間未満のレコードと、DNSSEC 署名が有効になっていない他のホストゾーンのレコードは、この影響を受けません。
- DNSSEC 署名を使用する場合、マルチベンダー構成はサポートされません。ホワイトラベルネームサーバー (別称: バニティネームサーバー、プライベートネームサーバー) を構成している場合は、それらのネームサーバーが単一の DNS プロバイダーから提供されていることを確認します。
- 一部の DNS プロバイダーは、権威 DNS 内で委任署名者 (DS) レコードをサポートしていません。親ゾーンが DS クエリをサポートしていない (DS クエリ応答に AA フラグを設定していない) DNS プロバイダーによってホストされている場合、子ゾーンで DNSSEC を有効にすると、その子ゾーンに関する解決が不能になります。ご利用の DNS プロバイダーで、DS レコードがサポートされていることを確認してください。
- ゾーン所有者以外の別のユーザーがゾーン内のレコードを追加または削除できるように、IAM アクセス許可を設定すると便利です。例えば、ゾーンの所有者は KSK を追加して署名を有効にし、キーのローテーションを担当することができます。同時に、他のユーザーがホストゾーンで他のレコードの操作を担当することも可能です。IAM ポリシーの例については、「ドメインレコード所有者のアクセス許可の例」を参照してください。
- TLD に DNSSEC サポートがあるかどうかを確認するには、「Amazon Route 53 に登録できる最上位ドメイン」を参照してください。

トピック

- DNSSEC 署名を有効にし、信頼チェーンを確立します。
- DNSSEC 署名の無効化
- DNSSEC のためのカスタマー管理キーの使用
- キー署名キー (KSK) の使用
- Route 53 での KMS キーと ZSK 管理
- Route 53 での DNSSEC の非存在証明
- DNSSEC 署名のトラブルシューティング

DNSSEC 署名を有効にし、信頼チェーンを確立します。

増分手順はホストゾーンの所有者と親ゾーンの管理者に適用されます。これは同一の当事者でもかまいません。ただし、そうでない場合、ゾーンの所有者は親ゾーンの管理者に通知して協力する必要があります。

ゾーンを署名して信頼チェーンに含めるため、この記事の手順に従うことをお勧めします。次の手順では、DNSSEC へのオンボーディングのリスクを最小限に抑えます。

> **Note**
>
> 始める前に、「Amazon Route 53 での DNSSEC 署名の設定」で前提条件を確認してください。

以下のセクションで説明する通り、DNSSEC 署名を有効にする場合、3 つの手順を実行します。

トピック

- ステップ 1: DNSSEC 署名を有効化する準備
- ステップ 2: DNSSEC 署名を有効にして KSK を作成
- ステップ 3: 信頼チェーンを確立

ステップ 1: DNSSEC 署名を有効化する準備

準備手順では、ゾーンの可用性を監視して署名の有効化から委任署名者 (DS) レコードの挿入までの待機時間を短縮することで、DNSSEC へのオンボーディングのリスクを最小限に抑えることができます。

DNSSEC 署名を有効にする準備を行うには

1. ゾーンの可用性を監視します。

   ドメイン名の可用性をゾーンで監視できます。これにより、DNSSEC 署名を有効にした後、ステップのロールバックを必要とする問題に対処できます。クエリログを使用してトラフィックが最も多いドメイン名を監視できます。クエリ ログのセットアップの詳細については、「Amazon Route 53 のモニタリング」をご参照ください。

監視はシェルスクリプトまたはサードパーティサービスを通じて実行できます。ただし、ロールバックが必要か否かを判断する唯一のシグナルとして見なしてはなりません。また、ドメインが利用できない理由で顧客からフィードバックを得る場合があります。

2. ゾーンの最大 TTL を下げます。

   ゾーンの最大 TTL は、ゾーン内の最長 TTL レコードです。以下のゾーン例では、ゾーンの最大 TTL は 1 日 (86400 秒) です。

   ゾーンレコードの例

名前	TTL	レコードクラス	レコードタイプ	データレコード
example.com。	900	IN	SOA	ns1.example.com。hostmaster.example.com。2002022401 10800 15 604800 300
example.com。	900	IN	NS	ns1.example.com。
route53.example.com。	86400	IN	TXT	**some txt record**

   ゾーンの最大 TTL を下げると、署名を有効にしてから Delegation Signer (DS) レコードを挿入するまでの待機時間を短縮できます。ゾーンの最大 TTL を 1 時間 (3600 秒) に下げることをお勧めします。その後、リゾルバーで署名付きレコードのキャッシュに問題がある場合は、わずか 1 時間後にロールバックできます。

   ロールバック: TTL の変更を元に戻します。

3. SOA TTL および SOA の最小フィールドを下げます。

SOA 最小フィールドは、SOA レコードデータの最後のフィールドです。以下の SOA レコードの例では、最小フィールドの値は 5 分 (300 秒) です。

SOA レコードの例

名前	TTL	レコードクラス	レコードタイプ	データレコード
example.com。	900	IN	SOA	ns1.example.com。hostmaster.example.com。2002022401 10800 15 604800 300

SOA TTL および SOA の最小フィールドは、リゾルバーがネガティブな回答を記憶する期間を決定します。署名を有効にすると、Route 53 ネームサーバーはネガティブな回答に対して NSEC レコードを返し始めます。NSEC には、リゾルバーがネガティブな回答を合成する際に使用する可能性がある情報が含まれています。NSEC 情報により、リゾルバーが名前に対してネガティブな回答を仮定したことによってロールバックが必要な場合、リゾルバーが仮定を停止するまで SOA TTL の最大値および SOA 最小フィールドに達するまで待つのみで解決します。

ロールバック方法: SOA の変更を元に戻します。

4. TTL および SOA の最小フィールドの変更が有効であることを確認します。

   GetChange を使用して、これまでの変更がすべての Route 53 DNS サーバーに反映されたことを確認します。

ステップ 2: DNSSEC 署名を有効にして KSK を作成

Route 53 コンソールで AWS CLI または を使用して、DNSSEC 署名を有効にし、キー署名キー (KSK) を作成できます。

- CLI
- コンソール

KMS キーの指定または作成には、いくつかの要件があります。詳細については、「DNSSEC のためのカスタマー管理キーの使用」を参照してください。

CLI

既に持っているキーを使用、または以下のように hostedzone_id、cmk_arn、ksk_name、unique_string 用の値を使用して AWS CLI コマンドを実行してキーを作成します (リクエストをユニークにするため):

```
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
```

カスタマーマネージドキーの詳細については、「DNSSEC のためのカスタマー管理キーの使用」をご参照ください。CreateKeySigningKey も併せてご参照ください。

DNSSEC 署名を有効にするには、 に独自の値を使用して、次のような AWS CLI コマンドを実行しますhostedzone_id。

```
aws --region us-east-1 route53 enable-hosted-zone-dnssec \
   --hosted-zone-id $hostedzone_id
```

詳細については enable-hosted-zone-dnssec および EnableHostedZoneDNSSEC をご参照ください。

Console

DNSSEC 署名を有効にして KSK を作成するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで、[ホストゾーン] をクリックし、DNSSEC 署名を有効にするホストゾーンを選択します。
3. [DNSSEC signing] (DNSSEC 署名) タブで、[Enable DNSSEC signing] (DNSSEC 署名を有効にする) を選択します。

> **Note**
>
> このセクションで [Disable DNSSEC signing] (DNSSEC 署名を無効にする) というオプションが表示されている場合は、DNSSEC 署名を有効にするための最初のステップが既に完了しています。DNSSEC のホストゾーンの信頼チェーンが確立されている、あるいは既に存在していることを確認し、作業を完了します。詳細については、「ステップ 3: 信頼チェーンを確立」を参照してください。

4. 「キー署名キー (KSK) 作成」セクションで「新しい KSK を作成する」を選択し、「KSK 名を指定する」で、Route 53 が作成する KSK の名前を入力します。名前には、文字、数字、アンダースコア (_) のみを含めることができます。また、名前は一意である必要があります。
5. [Customer managed CMK] (カスタマー管理 CMK)で、KSK の作成時に Route 53 で使用される、カスタマー管理キーを選択します。既存のカスタマー管理キーを使用して DNSSEC 署名に適用することも、新しいカスタマー管理キーを作成して使用することもできます。

   カスタマー管理キーの指定または作成には、いくつかの要件があります。詳細については、「DNSSEC のためのカスタマー管理キーの使用」を参照してください。
6. カスタマー管理キーのエイリアスを入力します。新しいカスタマーマネージドキーを使用する場合は、カスタマーマネージドキーのエイリアスを入力すると、Route 53 によって自動的に作成されます。

   > **Note**
   >
   > Route 53 にカスタマー管理キーを作成させる場合、個別のカスタマー管理キーごとに料金が発生することにご注意ください。詳細については、AWS Key Management Service の料金を参照してください。
7. [DNSSEC 署名を有効にする] をクリックします。

ゾーン署名を有効にした後、以下の手順を実行します (コンソールあるいは CLI を使用した場合を問わず):

1. ゾーン署名が有効であることを確認します。

を使用した場合は AWS CLI、EnableHostedZoneDNSSEC()呼び出しの出力からオペレーション ID を使用して get-change または GetChange を実行し、すべての Route 53 DNS サーバーがレスポンスに署名していることを確認します (ステータス = INSYNC)。

2. 最低でも前ゾーンの最大 TTL を待ちます。

   リゾルバーがキャッシュから署名されていないレコードをすべてフラッシュするまで待ちます。これを実現するため、最低でも前ゾーンの最大 TTL を待つ必要があります。上記の example.com ゾーンの場合、待機時間は 1 日です。

3. 顧客問題のレポートを監視します。

   ゾーン署名を有効にした後、顧客がネットワークデバイスおよびリゾルバーに関連する問題に直面し始める可能性があります。推奨される監視期間は 2 週間です。

   直面する問題例を以下の通り、紹介します:

   - 一部のネットワークデバイスは DNS 応答容量を 512 バイト未満に制限できますが、一部の署名応答としては小さすぎます。これらのネットワークデバイスは、より大きな DNS 応答容量を許可するために再設定する必要があります。
   - 一部のネットワークデバイスは、DNS 応答について詳細な検査を行い、DNSSEC に使用されるレコードなど、理解しない特定のものを削除します。これらのデバイスは再設定する必要があります。
   - 顧客の一部のリゾルバーは、ネットワークがサポートする UDP 応答よりも大量に受け入れることができると主張しています。ネットワーク機能をテストしてリゾルバーを適切に設定できます。詳細については、DNS Reply Size Test Server (DNS 応答容量テストサーバー) をご参照ください。

ロールバック方法:DisableHostedZoneDNSSEC を呼び出した後、ステップ 1: DNSSEC 署名を有効化する準備 の手順をロールバックします。

ステップ 3: 信頼チェーンを確立

Route 53 のホストゾーンで DNSSEC 署名を有効にした後に、ホストゾーンの信頼チェーンを確立して DNSSEC 署名のセットアップを完了します。これを行うには、Route 53 から提供される情報を使用しながら、自分のホストゾーンの親ホストゾーンで Delegation Signer (DS) レコードを作成します。ドメインが登録されている場所に応じて、Route 53 内または別のドメインレジストラにある親ホストゾーンに、DS レコードを追加します。

DNSSEC 署名のために信頼チェーンを確立するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで、[ホストゾーン] をクリックした後、 DNSSEC の信頼チェーンを確立するホストゾーンを選択します。最初に DNSSEC 署名を有効にする必要があります。
3. [DNSSEC signing] (DNSSEC 署名) タブを開き、[DNSSEC signing] (DNSSEC 署名) の [View information to create DS record] (DS レコードを作成するための情報を表示) を選択します。

   > **Note**
   >
   > このセクションで [View information to create DS record] (DSレコードを作成するための情報を表示] が表示されていない場合は、信頼チェーンを確立する前に DNSSEC 署名を有効にする必要があります。[Enable DNSSEC signing] (DNSSEC 署名を有効にする) を選択して ステップ 2: DNSSEC 署名を有効にして KSK を作成 の記載された手順を完了した後、これらの手順に戻って信頼チェーンを確立します。

4. ドメインが登録されている場所に応じ、[信頼チェーンを確立] から、[Route 53 レジストラ] または [他のドメインレジストラ] を選択します。
5. ステップ 3 で指定された値を使用して、Route 53 の親ホストゾーンの DS レコードを作成します。ドメインが Route 53 でホストされていない場合、表示された値をドメインレジストラのウェブサイトで使用して DS レコードを作成します。

   親ゾーンの信頼チェーンを確立します。

   - ドメインが Route 53 で管理されている場合、次の手順に従います。

     署名アルゴリズム (ECDSAP256SHA256 および type 13) とダイジェストアルゴリズム (SHA-256 およびタイプ 2) が正しく設定されたことを確認します。

     Route 53 がレジストラである場合、Route 53 コンソールで以下の操作を実行します:

     1. [Key type] (キータイプ)、[Signing algorithm] (署名アルゴリズム)、および [Public key] (パブリックキー) の各値を書き留めます。ナビゲーションペインで [Registered Domains] をクリックします。
     2. ドメインを選択し、[DNSSEC keys] (DNSSEC キー) タブで [Add key] (キーの追加) を選択します。

3. [Manage DNSSEC keys] (DNSSEC キー管理) ダイアログボックス内のドロップダウンメニューから、[Route 53 registrar] (Route 53 レジストラ) の適切な [Key type] (キータイプ) と [Algorithm] (アルゴリズム) を選択します。
4. Route 53 レジストラの [パブリックキー] をコピーします。[Manage DNSSEC keys] (DNSSEC キー管理) ダイアログボックス内の [Public key] (パブリックキー) ボックスに値を貼り付けます。
5. [Add] (追加) を選択します。

   Route 53 は、パブリックキーから親ゾーンに DS レコードを追加します。例えば、ドメインが `example.com` の場合、DS レコードが .com DNS ゾーンに追加されます。

- ドメインが別のレジストリで管理されている場合は、「別のドメインレジストラ」セクションの手順に従います。

  以下の手順をスムーズに進める場合、親ゾーンに低い DS TTL を導入します。変更をロールバックする必要がある場合、DS TTL を 5 分 (300 秒) に設定してリカバリの高速化をお勧めします。

  - 子ゾーンの信頼チェーンを確立します。

    親ゾーンが別のレジストリで管理されている場合、レジストラに連絡してゾーンに DS レコードを導入するように依頼してください。通常、DS レコードの TTL は調整できません。

  - 親ゾーンが Route 53 でホストされている場合、親ゾーンの所有者に連絡してゾーンに DS レコードを導入するように依頼してください。

    親ゾーンの所有者に `$ds_record_value` を提供します。コンソールの [View Information to create DS record] (情報を確認して DS レコードを作成) をクリックして [DS record] (DS レコード) フィールドをコピー、または GetDNSSEC API を呼び出して「DSRecord」フィールドの値を取得します。

    ```
    aws --region us-east-1 route53 get-dnssec
                --hosted-zone-id $hostedzone_id
    ```

    親ゾーンの所有者は、Route 53 コンソールまたは CLI を使用してレコードを挿入できます。

    - を使用して DS レコードを挿入するには AWS CLI、親ゾーンの所有者が次の例のような JSON ファイルを作成して名前を付けます。親ゾーンの所有者は、ファイルに `inserting_ds.json` のような名前を付けることがあります。

```
{
    "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"
                        }
                    ]
                }
            }
        ]
    }
}
```

次に、以下のコマンドを実行します。

```
aws --region us-east-1 route53 change-resource-record-sets
            --cli-input-json file://inserting_ds.json
```

- コンソールを使用して DS レコードを挿入するには、

  Route 53 コンソール (https://console.aws.amazon.com/route53/) を開きます。

  ナビゲーションペインで [Hosted zones] (ホストゾーン) とホストゾーン名を選択し、[Create record] (レコード作成) ボタンを押します。[Routing policy] (ルーティングポリシー) で [Simple routing] (簡易ルーティング) を選択していることを確認します。

  [Record name] (レコード名) フィールドに `$zone_name` と同じ名前を入力し、[Record type] (レコードタイプ) ドロップダウンから DS を選択します。次に [Value] (値) フィールドに `$ds_record_value` の値を入力して [Create records] (レコード作成) を選択します。

ロールバック方法: 親ゾーンから DS を削除して DS TTL を待った後、信頼を確立するための手順にロールバックします。親ゾーンが Route 53 でホストされている場合、親ゾーンの所有者は JSON ファイル内の UPSERT の Action を DELETE に変更して上記の例の CLI を再実行できます。

6. ドメインレコードの TTL に基づいて、更新が全体に反映されるのを待ちます。

   親ゾーンが Route 53 DNS サービス上にある場合、親ゾーンの所有者は GetChange API でプロパゲーション全体を確認できます。

   または、親ゾーンの DS レコードを定期的に調査することが可能であり、DS レコードの挿入が完全にプロパゲートされる確率を上げるため、さらに 10 分待ちます。DS 挿入をスケジュールしているレジストラもいることにご留意ください (例えば 1 日 1 回など)。

親ゾーンに委任署名者 (DS) レコードを導入すると、DS を取得した検証済みリゾルバーがゾーンからのレスポンスの検証を開始します。

信頼を確立する手順をスムーズに進めるため、以下の手順を実行します:

1. NS TTL の最大値を求めます。

   ゾーンに関連付けられた NS レコードが 2 つのセットあります。

   - NS レコードの委任 - これは、親ゾーンが保持しているお客様ゾーンの NS レコードです。次の Unix コマンドを実行することでこれを検索できます (ゾーンが example.com の場合、親ゾーンは com です):

     ```
     dig -t NS com
     ```

     いずれの NS レコードを 1 つを選択して以下を実行します:

     ```
     dig @one of the NS records of your parent zone -t NS example.com
     ```

     例:

     ```
     dig @b.gtld-servers.net. -t NS example.com
     ```

   - ゾーン内 NS レコード - これはゾーン内の NS レコードです。以下の Unix コマンドを実行すると探せます。

```
dig @one of the NS records of your zone -t NS example.com
```

例:

```
dig @ns-0000.awsdns-00.co.uk. -t NS example.com
```

両ゾーンの最大 TTL に注目してください。

2. NS TTL の最大値を待ちます。

   DS を挿入前の段階では、リゾルバーは署名付きレスポンスを取得しますが、署名を検証しません。DS レコードが挿入されると、リゾルバーはゾーンの NS レコードの有効期限が切れるまでそのレコードを表示しません。リゾルバーが NS レコードを再フェッチすると、DS レコードも返されます。

   お客様の顧客が非同期クロックのホスト内でリゾルバーを実行している場合、クロックが正しい時刻から 1 時間以内の誤差があることを確認してください。

   このステップを完了すると、すべての DNSSEC 対応リゾルバーがゾーンを検証します。

3. 名前解決を確認します。

   ゾーンを検証するリゾルバーに問題がないことにご留意してください。顧客が問題を報告するために必要な時間も考慮してください。

   最大 2 週間監視することをお勧めします。

4. (任意) DS および NS TTL を長くします。

   セットアップがよろしければ、変更した TTL および SOA 内容を保存できます。Route 53 は署名済みゾーンの TTL を 1 週に制限することにご留意ください。詳細については、「Amazon Route 53 での DNSSEC 署名の設定」を参照してください。

   DS TTL を変更が可能な場合、1 時間に設定することをお勧めします。

DNSSEC 署名の無効化

Route 53 で DNSSEC 署名を無効にする手順は、ホストゾーンが属する信頼チェーンによって異なります。

例えば、信頼チェーンの一部として、自分のホストゾーンには、Delegation Signer (DS) レコードを持つ親ゾーンが存在する場合があります。またホストゾーンは、DNSSEC 署名を有効にしてい

る子ゾーンの親ゾーンにもなり得るが、信頼チェーンの別の部分となっている場合も考えられます。DNSSEC 署名を無効にする手順を実行する前に、使用しているホストゾーンの信頼チェーン全体を調べて判断します。

DNSSEC 署名を有効にしているホストゾーンの信頼チェーンは、署名を無効にする際に慎重に元に戻す必要があります。信頼チェーンからホストゾーンを削除するには、このホストゾーンを含む信頼チェーンに対して配置されているすべての DS レコードを削除します。つまり、以下の操作を、順番に実行する必要があります。

1. 信頼チェーンの一部である (それぞれの) 子ゾーンについて、親のホストゾーンにある DS レコードをすべて削除します。
2. 親ゾーンから DS レコードを削除します。信頼の島 (親ゾーンに DS レコードがなく、このゾーンの子ゾーンの DS レコードもありません) がある場合、この手順をスキップします。
3. 信頼チェーンからゾーンを削除する際に、DS レコードの削除が不可能な場合には、親ゾーンから NS レコードを削除します。詳細については、「ドメインのネームサーバーおよびグルーレコードの追加あるいは変更」を参照してください。

次の増分手順は、ゾーン内の DNS 可用性の問題を回避するために個別手順の有効性を監視することを実現します。

DNSSEC 署名を無効にするには

1. ゾーンの可用性を監視します。

   ドメイン名の可用性をゾーンで監視できます。これにより、DNSSEC 署名を有効にした後、ステップのロールバックを必要とする問題に対処できます。クエリログを使用してトラフィックが最も多いドメイン名を監視できます。クエリログのセットアップの詳細については、「Amazon Route 53 のモニタリング」をご参照ください。

   監視はシェルスクリプトまたは有料サービスを通じて実行できます。ただし、ロールバックが必要か否かを判断する唯一のシグナルとして見なしてはなりません。また、ドメインが利用できない理由で顧客からフィードバックを得る場合があります。

2. 現在の DS TTL を検索します。

   以下の Unix コマンドを実行して DS TTL を検索できます:

   ```
   dig -t DS example.com example.com
   ```

3. NS TTL の最大値を求めます。

ゾーンに関連付けられた NS レコードが 2 つのセットあります。

- NS レコードの委任 - これは、親ゾーンが保持しているお客様ゾーンの NS レコードです。以下の Unix コマンドを実行してこれを検索できます:

  まず親ゾーンの NS を検索します (ゾーンが example.com の場合、親ゾーンは com です):

  ```
  dig -t NS com
  ```

  いずれの NS レコードを 1 つを選択して以下を実行します:

  ```
  dig @one of the NS records of your parent zone -t NS example.com
  ```

  例:

  ```
  dig @b.gtld-servers.net. -t NS example.com
  ```

- ゾーン内 NS レコード - これはゾーン内の NS レコードです。以下の Unix コマンドを実行すると探せます。

  ```
  dig @one of the NS records of your zone -t NS example.com
  ```

  例:

  ```
  dig @ns-0000.awsdns-00.co.uk. -t NS example.com
  ```

  両ゾーンの最大 TTL に注目してください。

4. 親ゾーンから DS レコードを削除します。

   親ゾーンの所有者に連絡して DS レコードを削除するように依頼します。

   ロールバック方法: DS レコードを再度挿入して DS 挿入が有効であることを確認し、すべてのリゾルバーが再検証を開始する前に最大 NS (DS ではない) TTL を待ちます。

5. DS の削除が有効であることを確認します。

   親ゾーンが Route 53 DNS サービス上にある場合、親ゾーンの所有者は GetChange API でプロパゲーション全体を確認できます。

   または、親ゾーンの DS レコードを定期的に調査することが可能であり、DS レコードの削除が完全にプロパゲートされる確率を上げるため、さらに 10 分待ちます。一部のレジストラは DS の削除をスケジュール (例えば、1 日 1 回など) していることをご留意ください。

6. DS TTL を待つ。

   すべてのリゾルバーがキャッシュにある DS レコードの有効期限が切れるまで待ちます。

7. DNSSEC 署名を無効にしてキー署名キー (KSK) を無効にします。

   - CLI
   - コンソール

   CLI

   DisableHostedZoneDNSSEC および DeactivateKeySigningKey API を呼び出します。

   例:

   ```
   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

   DNSSEC 署名を無効にするには

   1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
   2. ナビゲーションペインで、[ホストゾーン]をクリックし、DNSSEC 署名を無効にするホストゾーンを選択します。
   3. [DNSSEC signing] (DNSSEC 署名) タブで、[Disable DNSSEC signing] (DNSSEC 署名を無効にする) を選択します。
   4. [Disable DNSSEC signing] (DNSSEC 署名を無効にする) ページで、ゾーンにおける DNSSEC 署名の無効化のシナリオに応じて、次のいずれかのオプションを選択します。
      - 親ゾーンのみ – このゾーンには、DS レコードを持つ親ゾーンがあります。このシナリオでは、親ゾーンの DS レコードを削除する必要があります。

- 子ゾーンのみ – このゾーンには、1 つまたは複数の子ゾーンが属する信頼チェーンのための DS レコードがあります。このシナリオでは、このゾーンの DS レコードを削除する必要があります。
- 親ゾーンと子ゾーン – このゾーンには、1 つまたは複数の子ゾーンが属する信頼チェーンのための DS レコード、および DS レコードを持つ親ゾーンの両方があります。このシナリオでは次の操作を順に実行します。

  a. このゾーンの DS レコードを削除します。

  b. 親ゾーンの DS レコードを削除します。

  信頼の島がある場合、この手順をスキップできます。

5. ステップ 4 で削除する各 DS レコードの TTL の数値を特定し、最も長い TTL 期間が終了していることを確認します。
6. チェックボックスを選択して、手順を順番通りに実行したことを確認します。
7. 次に示すように、フィールドに「disable」と入力してから、[Disable] (無効化) を選択します。

キー署名キー (KSK) を無効にする場合

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [Hosted zones] (ホストゾーン) を選択し、キー署名キー (KSK) を無効にするホストゾーンを選択します。
3. [Key-signing keys (KSKs)] (キー署名キー (KSK)) セクションで無効にする KSK を選択します。次に [Actions] (アクション) の下で [Edit KSK] (KSKの編集) を選択し、[KSK status] (KSKステータス) を [Inactive] (非アクティブ) に設定して [Save KSK] (KSKを保存) を選択します。

ロールバック方法: ActivateKeySigningKey および EnableHostedZoneDNSSEC API を呼び出します。

例:

```
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. ゾーン署名の無効化が有効になっていることを確認します。

   EnableHostedZoneDNSSEC( ) の呼び出しに使用した ID で GetChange を実行し、すべての Route 53 DNS サーバーが応答の署名を停止していることを確認します (ステータス = INSYNC)。

9. 名前解決を確認します。

   リゾルバーがゾーンを検証する問題がないことを確認する必要があります。顧客が問題を報告するために必要な時間も 1 ~ 2 週間ぐらい考慮してください。

10. (オプション) クリーンアップする。

    署名を再度有効にしない場合、DeleteKeySigningKey を使用して KSKs をクリーンアップし、対応するカスタマーマネージドキーを削除してコストを削減できます。

DNSSEC のためのカスタマー管理キーの使用

Amazon Route 53 で DNSSEC 署名を有効にすると、Route 53 によってキー署名キー (KSK) が作成されます。KSK を作成するには、Route 53 は DNSSEC をサポートする AWS Key Management Service でカスタマーマネージドキーを使用する必要があります。このセクションでは、DNSSEC を使用する際に役立つカスタマー管理キーの詳細と要件について説明します。

DNSSEC でカスタマー管理キーを使用する場合は、以下の点に注意してください。

- DNSSEC 署名で使用するカスタマー管理キーは、米国東部 (バージニア北部) リージョンに置かれている必要があります。
- カスタマー管理キーは、非対称カスタマー管理キーであり、また ECC_NIST_P256 のキースペックである必要があります。これらのカスタマー管理キーは、署名と検証にのみ使用されます。非対称カスタマーマネージドキーの作成については、「 AWS Key Management Service デベロッパーガイド」の「非対称カスタマーマネージドキーの作成」を参照してください。既存のカスタマーマネージドキーの暗号化設定を見つける方法については、「 AWS Key Management Service デベロッパーガイド」の「カスタマーマネージドキーの暗号化設定の表示」を参照してください。

- Route 53 の DNSSEC で使用するカスタマーマネージドキーを自分で作成する場合は、Route 53 に必要なアクセス許可を付与する特定のキーポリシーステートメントを定義する必要があります。Route 53 が KSK を作成する際には、カスタマー管理キーへのアクセスが可能である必要があります。詳細については、「DNSSEC 署名に必要な Route 53 カスタマー管理キーアクセス許可」を参照してください。
- Route 53 は、追加の AWS KMS アクセス許可なしで DNSSEC 署名で使用するカスタマーマネージドキー AWS KMS を で作成できます。ただし、作成後にキーを編集する場合は、特定のアクセス許可が必要です。ユーザーに必須な特定のアクセス許可は `kms:UpdateKeyDescription`、`kms:UpdateAlias`、および `kms:PutKeyPolicy` です。
- カスタマー管理キーをユーザーが作成したか、あるいは Route 53 により作成されたかにかかわらず、カスタマー管理キーごとに個別の料金が適用されることにご注意ください。詳細については、AWS Key Management Service 料金表を参照してください。

キー署名キー (KSK) の使用

DNSSEC 署名を有効にすると、Route 53 によってキー署名キー (KSK) が作成されます。Route 53 ではホストゾーンごとに最大 2 つの KSK を使用できます。DNSSEC 署名を有効にした後は、KSK の追加、削除、または編集が行えます。

KSK を使用する場合は、次の点に注意してください。

- KSK を削除する際には、先に KSK を編集して、そのステータスを [非アクティブ] に設定する必要があります。
- ホストゾーンで DNSSEC 署名を有効にすると、Route 53 は TTL を 1 週間に制限します。ホストゾーンのレコードの TTL を 1 週間以上に設定した場合でもエラーは発生しませんが、Route 53 は TTL を 1 週間に強制します。
- ゾーンの停止を防ぎ、ドメインが使用できなくなる問題を回避するには、DNSSEC エラーにすばやく対処し解決する必要があります。`DNSSECInternalFailure` または `DNSSECKeySigningKeysNeedingAction` エラーが検出されるたびにアラートを受け取ることができる、CloudWatch アラームをセットアップしておくことを強くお勧めします。詳細については、「Amazon CloudWatch を使用したホストゾーンのモニタリング」を参照してください
- このセクションで説明する KSK 操作を使用すると、ゾーンの KSK をローテーションさせることができます。詳細およびステップバイステップの例については、ブログ記事 Configuring DNSSEC signing and validation with Amazon Route 53 の、「DNSSEC Key Rotation」を参照してください。

で KSKs を使用するには AWS マネジメントコンソール、以下のセクションのガイダンスに従ってください。

キー署名キー (KSK) の追加

DNSSEC 署名を有効にすると、Route 53 によってキー署名キー (KSK) が作成されます。KSK は個別に追加することもできます。Route 53 ではホストゾーンごとに最大 2 つの KSK を使用できます。

KSK の作成時には、KSK で使用するカスタマー管理キーを作成するための Route 53 を指定またはリクエストする必要があります。カスタマー管理キーの指定または作成には、いくつかの要件があります。詳細については、「DNSSEC のためのカスタマー管理キーの使用」を参照してください。

以下のステップに従って、 AWS マネジメントコンソールに KSK を追加します。

KSK を追加するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで、[ホストゾーン] をクリックした後で、ホストゾーンを選択します。
3. [DNSSEC signing] (DNSSEC 署名) タブを開き、[Key-signing keys (KSKs)] (キー署名キー (KSK)) で [Switch to advanced view] (詳細表示に切り替える) を選択し、さらに [Actions] (アクション) で [Edit KSK] (KSK の編集) を選択します。
4. KSK で、Route 53 が作成する KSK の名前を入力します。名前には、文字、数字、アンダースコア (_) のみを含めることができます。また、名前は一意である必要があります。
5. DNSSEC 署名に適用されるカスタマーマネージドキーのエイリアスを入力するか、Route 53 が作成する新しいカスタマーマネージドキーのエイリアスを入力します。

   > **Note**
   >
   > Route 53 にカスタマー管理キーを作成させる場合、個別のカスタマー管理キーごとに料金が発生することにご注意ください。詳細については、AWS Key Management Service 料金表を参照してください。

6. [KSK を作成] をクリックします。

キー署名キー (KSK) の編集

KSK のステータスを編集して [Active] (アクティブ) または [Inactive] (非アクティブ) とすることができます。KSK がアクティブな場合、Route 53 はその KSK を DNSSEC 署名に使用します。KSK を削除する際には、先に KSK を編集して、そのステータスを [非アクティブ] に設定する必要があります。

以下のステップに従って、 AWS マネジメントコンソールで KSK を編集します。

KSK を編集するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで、[ホストゾーン] をクリックした後で、ホストゾーンを選択します。
3. [DNSSEC signing] (DNSSEC 署名) タブの [Key-signing keys (KSKs)] (キー署名キー (KSK)) の下にある [Switch to advanced view] (詳細表示に切替) を選択し、さらに [Actions] (アクション) の下にある [Edit KSK] (KSK の編集) を選択します。
4. KSK に対し必要な更新を行った上で、[Save] (保存) を選択します。

キー署名キー (KSK) の削除

KSK を削除する際には、先に KSK を編集して、そのステータスを [非アクティブ] に設定する必要があります。

KSK の削除が必要となる理由の 1 つに、定期的に行うキーのローテーション作業があります。暗号キーについては、定期的にローテーションすることがベストプラクティスです。組織によっては、キーをローテーションさせる頻度に関する標準的な取り決めをしている場合があります。

ここでのステップに従って、 AWS マネジメントコンソールの KSK を削除します。

KSK を削除するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで、[ホストゾーン] をクリックした後で、ホストゾーンを選択します。
3. [DNSSEC signing] (DNSSEC 署名) タブを開き、[Key-signing keys (KSKs)] (キー署名キー (KSK)) で [Switch to advanced view] (詳細表示に切り替える) を選択し、さらに [Actions] (アクション) で [Edit KSK] (KSK の編集) を選択します。

4. ガイダンスに従って、KSK の削除を確認します。

Route 53 での KMS キーと ZSK 管理

このセクションでは、Route 53 が DNSSEC 署名対応ゾーンに使用する現在の手法について説明します。

> **Note**
>
> Route 53 は、変更される可能性がある次のルールを使用します。将来変更があっても、お客様のゾーンまたは Route 53 のセキュリティ体制が減少することはありません。

Route 53 が KSK AWS KMS に関連付けられた を使用する方法

DNSSEC では、KSK を使用して DNSKEY リソースレコードセットのリソースレコード署名 (RRSIG) を生成します。すべての `ACTIVE` KSK は RRSIG 世代で使用されます。Route 53 は、関連付けられた KMS キーで `Sign` AWS KMS API を呼び出して RRSIG を生成します。詳細については、「AWS KMS API ガイド」の「署名」を参照してください。これらの RRSIG は、ゾーンのリソースレコードセットの制限には数えられません。

RRSIG には有効期限があります。RRSIG の有効期限が切れるのを防ぐため、RRSIG は 1 ~ 7 日ごとに再生成して定期的に更新されます。

RRSIG は、次のいずれかの API を呼び出すたびに更新されます。

- ActivateKeySigningKey
- CreateKeySigningKey
- DeactivateKeySigningKey
- DeleteKeySigningKey
- DisableHostedZoneDNSSEC
- EnableHostedZoneDNSSEC

Route 53 が更新を実行するたびに、関連付けられた KMS キーにアクセスできなくなった場合に備えて、数日後まで使用できる 15 個 の RRSIG を生成します。KMS キーコストの見積もりについては、定期的な更新が 1 日に 1 回行われると考えることができます。KMS キーポリシーを誤って変更すると、KMS キーにアクセスできなくなる可能性があります。アクセスで

きない KMS キーは、関連付けられた KSK のステータスを ACTION_NEEDED に設定します。最後の RRSIG の有効期限が切れた後、リゾルバーの検証でルックアップが失敗し始めるため、DNSSECKeySigningKeysNeedingAction エラーが検出されたときには CloudWatch アラームを設定して、この状態をモニタリングすることを強くお勧めします。詳細については、「Amazon CloudWatch を使用したホストゾーンのモニタリング」を参照してください。

Route 53 がゾーンの ZSK を管理する方法

DNSSEC の署名が有効になっている新しいホストゾーンには、それぞれ 1 つの ACTIVE ゾーン署名キー (ZSK) があります。ZSK はホストゾーンごとに別々に生成され、Route 53 が所有しています。現在のキーアルゴリズムは ECDSAP256SHA256 です。

署名開始から 7～30 日以内に、ゾーンで通常の ZSK ローテーションの実行を開始します。現在、Route 53 は事前公開キーロールオーバー方式を使用しています。詳細については、「Pre-Publish Zone Signing Key Rollover (事前公開ゾーン署名キーのロールオーバー)」を参照してください。この方法では、ゾーンに別の ZSK を導入します。ローテーションは 7～30 日ごとに繰り返されます。

Route 53 はゾーンの ZSK の変更を考慮するために DNSKEY リソースレコードセットの RRSIG を再生成できないため、ゾーンの KSK のいずれかが ACTION_NEEDED ステータスである場合、Route 53 は ZSK のローテーションを一時停止します。ZSK ローテーションは、条件がクリアされた後に自動的に再開されます。

Route 53 での DNSSEC の非存在証明

> **Note**
>
> Route 53 は、変更される可能性がある次のルールを使用します。将来変更があっても、お客様のゾーンまたは Route 53 のセキュリティ体制が減少することはありません。

DNSSEC には、次の 3 種類の非存在証明があります。

- クエリ名に一致するレコードが存在しないことの証明。
- クエリタイプに一致するタイプが存在しないことの証明。
- レスポンスにレコードを生成するために使用されるワイルドカードレコードが存在することの証明。

Route 53 は、BL メソッドを使用して、クエリ名と一致するレコードが存在しないことの証明を実装します。詳細については「BL」を参照してください。これは、証明をコンパクトに表現し、ゾーンウォーキングを防ぐ方法です。

クエリ名と一致するレコードは存在するものの、クエリタイプが存在しない場合 (クエリの対象は、web.example.com/AAAA であるのに、web.example.com/A しか存在しないなど)、サポートされているすべてのリソースレコードタイプを含む最小の NSEC (次にセキュアな) レコードを返します。

Route 53 がワイルドカードレコードから結果を生成する場合、そのレスポンスには後に続くセキュアレコード、あるいはワイルドカードの NSEC レコードは付属しません。このような NSEC レコードは、レスポンスのリソースレコード署名 (RRSIG) が別のレスポンスを偽装するために再利用されないように、一部の実装 (通常はオフライン署名を実行する実装) で使用されます。Route 53 では、別のレスポンスで再利用できないレスポンスに固有の RRSIG を生成する非 DnsKey のレコードに、オンライン署名を使用しています。

DNSSEC 署名のトラブルシューティング

このセクションの情報は、DNSSEC 署名の有効化、無効化、およびキー署名キー (KSK) の使用に関する問題を解決するのに役立ちます。

DNSSEC の有効化

DNSSEC 署名を有効化する前に、「Amazon Route 53 での DNSSEC 署名の設定」で前提条件を確認してください。

DNSSEC の無効化

DNSSEC を安全に無効化するために、Route 53 は、ターゲットゾーンが信頼チェーン内にあるかどうかを確認します。ターゲットゾーンの親に、そのターゲットゾーンの NS レコードと DS レコードがあることも確認します。NS と DS のクエリ時に SERVFAIL 応答が返されるなど、ターゲットゾーンがパブリックに解決できない場合には、Route 53 は DNSSEC を安全に無効化できるかどうかを判断できません。親ゾーンに接続し、これらの問題を修正した上で、DNSSEC の無効化を再試行します。

KSK のステータスが [Action needed] (アクションが必要) になっています

Route 53 DNSSEC が対応する へのアクセスを失った場合 (アクセス許可の変更または削除により)、KSK はステータスを必要なアクション AWS KMS key (または `ACTION_NEEDED` KeySigningKey ステータス) に変更できます AWS KMS key 。

KSK のステータスが [Action needed] (実行が必要) の場合、最終的に DNSSEC 検証リゾルバーを使用する顧客でゾーン停止が発生し、本番ゾーンが解決不能になることを防ぐため、迅速に対処しなければなりません。

問題を解決する場合、KSK の基になっているカスタマーマネージドキーが有効であり、適切なアクセス許可が付与されていることをご確認ください。必要な許可の詳細については、「DNSSEC 署名に必要な Route 53 カスタマー管理キーアクセス許可」を参照してください。

KSK を修正したら、「」で説明されているように AWS CLI、コンソールまたは を使用して再度アクティブ化しますステップ 2: DNSSEC 署名を有効にして KSK を作成。

今後この問題を回避するには、「」で提案されているように、KSK の状態を追跡する Amazon CloudWatch メトリクスを追加することを検討してくださいAmazon Route 53 での DNSSEC 署名の設定。

KSK のステータスが [Internal failure] (内部エラー) になっています

KSK のステータスが [Internal failure] (内部障害) の場合 (または KeySigningKey ステータスで `INTERNAL_FAILURE`)、この問題が解決されるまで他の DNSSEC エンティティを操作することはできません。この KSK または他の KSK での作業を含め、DNSSEC 署名での操作を行う前に対策を取る必要があります。

この問題を解決するには、KSK のアクティブ化または非アクティブ化を再試行します。

API を使う際にこの問題を解決する場合、署名 (EnableHostedZoneDNSSEC) の有効化、または署名の無効化 (DisableHostedZoneDNSSEC) を試みます。

[Internal failure] (内部エラー) の問題には、迅速に対処することが重要です。この問題が解決されるまで、[Internal failure] (内部エラー) を修正するためのオペレーションを除き、ホストゾーンに対して他の変更を加えることはできません。

AWS Cloud Map を使用してレコードとヘルスチェックを作成する

インターネットトラフィックまたは Amazon VPC トラフィックをアプリケーションコンポーネントまたはマイクロサービスにルーティングするには、 を使用します AWS Cloud Map。DNS レコードと、オプションでヘルスチェックが自動的に作成されます。詳細については、AWS Cloud Map デベロッパーガイドを参照してください。

DNS の制約と動作

DNS メッセージングは、ホストゾーンおよびレコードの作成方法と使用方法に影響を与える要素に依存します。このセクションでは、これらの要素について説明します。

最大レスポンスサイズ

DNS 標準に準拠するために、UDP 経由で送信されるレスポンスのサイズはわずか 512 バイトです。512 バイトを超えるレスポンスは切り捨てられ、リゾルバーは TCP 経由でリクエストを再発行する必要があります。リゾルバーが EDNS0 (RFC 2671 で定義) をサポートし、EDNS0 オプションを Amazon Route 53 にアドバタイズする場合、Route 53 では UDP 経由のレスポンスのサイズを 4096 バイトまで許可し切り捨ては行われません。

Authority セクションの処理

クエリが正常に実行された場合、Route 53 は、関連するホストゾーンのネームサーバー (NS) レコードを、DNS レスポンスの Authority セクションに追加します。名前が検出されなかった場合 (NXDOMAIN レスポンス)、Route 53 は、関連するホストゾーンの Start of Authority (SOA) レコード (RFC 1035 で定義) を、DNS レスポンスの Authority セクションに追加します。

Additional セクションの処理

Route 53 は、レコードを Additional セクションに追加します。レコードが既知のものであり、適切なレコードである場合は、サービスによって、Answer セクションにある MX、CNAME、NS、SRV の各レコードのターゲットに対応した A レコードまたは AAAA レコードが追加されます。これらの DNS レコードタイプの詳細については、「サポートされる DNS レコードタイプ」を参照してください。

関連トピック

Route 53 へのドメイン登録 (DNS ホスティングだけでなく) の移管については、以下のトピックを参照してください。

- ドメイン移管の移管前チェックリスト – 一般的な転送の失敗を避けるため、ドメインを転送する前にこのチェックリストを完了してください。
- ドメイン登録の Amazon Route 53 への移管 – 別のレジストラから Route 53 へドメイン登録を移管するためのステップバイステップのプロセス。
- ドメインの移管 – AWS アカウント間の転送を含む、すべてのドメイン転送オプションの概要。

DNS トラフィックのルーティングにトラフィックフローを使用する

トラフィックフローは、大規模で複雑な設定でレコードを作成および維持するプロセスを大幅に簡素化します。

ホストゾーンでの関連レコードの管理は、次のような状況では困難な場合があります。

- 同じドメインのトラフィックを処理するウェブサーバーなど、同じオペレーションを実行する多くのリソースがある場合。
- エイリアスレコードと、レイテンシー、フェールオーバー、加重などの Route 53 ルーティングポリシーの組み合わせを使用して、レコードの複雑なツリーを作成する場合。

トラフィックフローの利点

レコードとその関係の追跡を容易にするために、トラフィックフローは、次の機能を使用して DNS レコードの作成を簡素化します。

Visual editor (ビジュアルエディタ)

Traffic Flow ビジュアルエディタを使用すると、複雑なレコードツリーを作成し、レコード間の関係を確認できます。例えば、レイテンシーエイリアスレコードが加重レコードを参照し、加重レコードが複数の AWS リージョン内のリソースを参照する設定を作成できます。各設定はトラフィックポリシーと呼ばれます。トラフィックポリシーはいくつでも無料で作成できます。

バージョニング

複数のバージョンのトラフィックポリシーを作成できるため、設定が変更されたときに最初からやり直す必要はありません。古いバージョンは、削除するまで存続します。トラフィックポリシーあたり 1000 バージョンというデフォルト制限があります。オプションで、各バージョンに説明を追加することができます。

レコードの自動作成と更新

トラフィックポリシーは、数十または数百のレコードを表すことができます。トラフィックフローでは、トラフィックポリシーレコードを作成することで、これらのすべてのレコードを自動的に作成できます。ツリーのルート (example.com や www.example.com など) にホストゾー

ンとレコード名を指定すると、ツリーに他のすべてのレコードが自動的に作成されます。ルートレコード - トラフィックポリシーレコード - は、ホストゾーンのレコードのリストに表示されます。Route 53 は他のすべてのレコードを非表示にします。

トラフィックポリシーの新しいバージョンを作成する場合、以前のトラフィックポリシーバージョンを使用して作成したトラフィックポリシーレコードを選択的に更新できます。トラフィックポリシーレコードを更新すると、Route 53 はツリー内の他のすべてのレコードを自動的に更新します。トラフィックポリシーレコードを再度更新して、以前のバージョンのトラフィックポリシーを使用することにより、変更をすばやくロールバックすることもできます。

> **Note**
>
> トラフィックフローを使用して、パブリックホストゾーンでのみレコードを作成できます。

地理的近接性ルーティングポリシー

トラフィックフローを使用すると、トラフィックフロービジュアルエディタの地理的近接性マップを使用して、トラフィックが各グローバルエンドポイントにどのようにルーティングされるかをより直感的に理解できます。詳細については、「地理的近接性ルーティング」を参照してください。

異なるホストゾーンの複数のレコードの再利用

トラフィックポリシーを使用して、複数のパブリックホストゾーンにレコードを自動的に作成できます。例えば、複数のドメイン名に同じウェブサーバーを使用している場合、同じトラフィックポリシーを使用して、example.com、example.org、example.net などのホストゾーンにトラフィックポリシーレコードを作成できます。

クライアントが example.com や www.example.com などのルートレコードの名前のクエリを送信すると、Route 53 は、対応するトラフィックポリシーレコードの作成に使用したトラフィックポリシーの設定に基づいてクエリに応答します。

トラフィックポリシーレコードごとに月額料金が発生します。詳細については、Amazon Route 53 の料金表の「トラフィックフロー」セクションを参照してください。

これらの料金を最小限に抑えるために、そのホストゾーン内のトラフィックポリシーレコードを参照するエイリアスレコードを 1 つ以上ホストゾーンに作成することができます。例え

ば、example.com のトラフィックポリシーレコードを作成し、そのトラフィックポリシーレコードを参照する www.example.com のエイリアスレコードを作成できます。

トラフィックポリシーの作成と管理

トピック

- トラフィックポリシーの作成
- トラフィックポリシーを作成するときに指定する値
- 地理的近接性の設定の効果を示す地図の表示
- トラフィックポリシーの追加のバージョンの作成
- JSON ドキュメントを使用してトラフィックポリシーを作成する
- トラフィックポリシーバージョンおよび関連するポリシーレコードの表示
- トラフィックポリシーバージョンとトラフィックポリシーの削除

トラフィックポリシーの作成

トラフィックポリシーを作成するには、以下の手順を実行します。

> **Note**
>
> Route 53 は Traffic Flow コンソールを更新しています。旧コンソールは移行期間中も引き続きご使用いただけます。

お使いのコンソールのタブを選択します。

- 新しいコンソール
- 旧コンソール

New console

トラフィックポリシーを作成するには

1. 設定を設計します。複雑な DNS ルーティング設定の仕組みの詳細については、DNS フェイルオーバーの設定 の「Amazon Route 53 ヘルスチェックの作成」を参照してください。

2. 設定の設計に基づいて、エンドポイントで使用するヘルスチェックを作成します。
3. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
4. ナビゲーションペインで、[Traffic policies] を選択します。
5. [Create traffic policy] を選択します。
6. 名前を入力し、必要に応じて説明を入力して [Next] (次へ) を選択します。
7. エディタの [プロパティ] ペインで DNS リソースレコードタイプを選択します。このタイプは、このトラフィックポリシー用に作成したすべてのリソースレコードに割り当てられます。

   [確認] を選択します。詳細については、「トラフィックポリシーを作成するときに指定する値」を参照してください。
8. エディタページで、[接続先] を選択し、[新しいルーティングルール]、[新しいエンドポイント]、[既存のルーティングルール]、[既存のエンドポイント] のいずれかを選択します。[新しいルーティングルール] を選択した場合は、[プロパティ] ペインでルーティングルールを選択し、[確認] を選択します。次に、[プロパティ] ペインに適切な値を入力します。ポリシーが完了するまで、このプロセスを繰り返します。各接続タイプの値の詳細については、「トラフィックポリシーを作成するときに指定する値」を参照してください。

   トラフィックポリシーのルール、エンドポイント、ブランチは、次の方法で削除できます。

   - ルールまたはエンドポイントを削除するには、エディタでルールまたはエンドポイントを選択し、[プロパティ] ペインで [削除] を選択します。

     > **Important**
     >
     > 子ルールおよび子エンドポイントがあるルールを削除すると、Amazon Route 53 はそれらの子もすべて削除します。

   - 2 つのルールが同じ子ルールまたは子エンドポイントに接続されていて、片方の接続を削除する場合、削除する接続を選択し、その接続の [Properties] (プロパティ) ペインの [Delete] (削除) を選択します。
9. [Create policy] (ポリシーの作成) を選択します。
10. [Create policy records] (ポリシーレコードの作成) ページで、新しいトラフィックポリシーを使用して 1 つのホストゾーンに 1 つ以上のポリシーレコードを作成します。詳細については、「ポリシーレコードを作成または更新する場合に指定する値」を参照してください。後

で、同じホストゾーンまたは追加のホストゾーンでポリシーレコードを作成することもできます。

ポリシーレコードを今すぐ作成しない場合は、キャンセルを選択すると、コンソールに現在の AWS アカウントを使用して作成したトラフィックポリシーとポリシーレコードのリストが表示されます。

11. 前述のステップでポリシーレコードの設定を指定した場合、[Create policy records] (ポリシーレコードの作成) を選択します。

Old console

トラフィックポリシーを作成するには

1. 設定を設計します。複雑な DNS ルーティング設定の仕組みの詳細については、DNS フェイルオーバーの設定 の「Amazon Route 53 ヘルスチェックの作成」を参照してください。
2. 設定の設計に基づいて、エンドポイントで使用するヘルスチェックを作成します。
3. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
4. ナビゲーションペインで、[Traffic policies] を選択します。
5. [Create traffic policy] を選択します。
6. [Name policy] ページで、適切な値を指定します。詳細については、「トラフィックポリシーを作成するときに指定する値」を参照してください。
7. [Next] (次へ) を選択します。
8. [Create traffic policy (トラフィックポリシーの作成) policy name (ポリシー名) v1] ページで、該当する値を指定します。詳細については、「トラフィックポリシーを作成するときに指定する値」を参照してください。

トラフィックポリシーのルール、エンドポイント、ブランチは、次の方法で削除できます。

- ルールまたはエンドポイントを削除するには、ボックスの右上隅にある x を選択します。

> **Important**
>
> 子ルールおよび子エンドポイントがあるルールを削除すると、Amazon Route 53 はそれらの子もすべて削除します。

- 2 つのルールを同じ子ルールまたはエンドポイントに接続し、いずれかの接続を削除する場合は、削除する接続にカーソルを置き、その接続の x を選択します。

9. [Create traffic policy] を選択します。
10. オプション: [Create policy records with traffic policy (トラフィックポリシーによるポリシーレコードの作成)] ページで、新しいトラフィックポリシーを使用して 1 つのホストゾーンに 1 つ以上のポリシーレコードを作成します。詳細については、「ポリシーレコードを作成または更新する場合に指定する値」を参照してください。後で、同じホストゾーンまたは追加のホストゾーンでポリシーレコードを作成することもできます。

    今すぐポリシーレコードを作成しない場合は、このステップをスキップを選択すると、コンソールに現在の AWS アカウントを使用して作成したトラフィックポリシーとポリシーレコードのリストが表示されます。
11. 前述のステップでレコードポリシーの設定を指定した場合、[Create policy record] を選択します。

トラフィックポリシーを作成するときに指定する値

> **Note**
>
> Route 53 は Traffic Flow コンソールを更新しています。旧コンソールは移行期間中も引き続きご使用いただけます。次のリストは、特に明記されていない限り、両方のコンソールに適用されます。

トラフィックポリシーを作成するときは、以下の値を指定します。

-
-
-
-
-
-
-
-

ポリシー名

トラフィックポリシーを説明する名前を入力します。この値は、コンソールのトラフィックポリシーのリストに表示されます。一度作成したトラフィックポリシーの名前は変更できません。

バージョン

この値は、トラフィックポリシーまたは既存のポリシーの新しいバージョンを作成すると、Amazon Route 53 によって自動的に割り当てられます。

バージョンの説明

トラフィックポリシーのこのバージョンに適用されるに説明を入力します。この値は、コンソールのトラフィックポリシーバージョンの一覧に表示されます。

DNS タイプ

このトラフィックポリシーバージョンを使用してポリシーレコードを作成する際に、すべてのレコードに Amazon Route 53 が割り当てる DNS タイプを選択します。サポートされているタイプのリストについては、「サポートされる DNS レコードタイプ」を参照してください。

> **Important**
>
> 既存のトラフィックポリシーの新しいバージョンを作成する場合、DNS タイプを変更できます。ただし、ポリシーレコードを編集して、ポリシーレコードを作成するときに使用したトラフィックポリシーバージョンとは異なる DNS タイプのトラフィックポリシーバージョンを選択することはできません。例えば、[DNS type] が A のトラフィックポリシーバージョンを使用してポリシーレコードを作成した場合、ポリシーレコードを編集して、[DNS type] が他の値のトラフィックポリシーバージョンを選択することはできません。

トラフィックを次の AWS リソースにルーティングする場合は、該当する値を選択します。

- CloudFront ディストリビューション – [A: IPv4 形式の IP アドレス] または [AAAA: IPv6 形式の IP アドレス] を選択します。

> **Note**
>
> CloudFront エイリアスエンドポイントは、ヘルスチェックの評価をサポートしていません。ただし、CloudFront エンドポイントをモニタリングするヘルスチェックを作成できます。詳細については、「ヘルスチェックの作成と更新」を参照してください。

- ELB Application Load Balancer – [A: IPv4 形式の IP アドレス] または [AAAA: IPv6 形式の IP アドレス] を選択します。
- ELB Classic Load Balancer – [A: IPv4 形式の IP アドレス] または [AAAA: IPv6 形式の IP アドレス] を選択します。
- ELB Network Load Balancer – [A: IPv4 形式の IP アドレス] または [AAAA: IPv6 形式の IP アドレス] を選択します。
- Elastic Beanstalk 環境: [A: IPv4 形式の IP アドレス] を選択します。
- ウェブサイトエンドポイントとして設定された Amazon S3 バケット: [A: IP address in IPv4 format] (A: IPv4 形式の IP アドレス) を選択します。

に接続します。

設定の設計に基づいて該当するルールまたはエンドポイントを選択します。

フェイルオーバールール

あるリソースが利用できるときは、それがすべてのトラフィックを処理し、そのリソースが利用できないときは別のリソースがすべてのトラフィックを処理するという、アクティブ/パッシブフェイルオーバーを設定する場合に、このオプションを選択します。

詳細については、「アクティブ/パッシブ (フェイルオーバー)。」を参照してください。

> **Note**
>
> デフォルトでは、ターゲットの状態の評価がチェックされます。エイリアスレコードを介してトラフィックがルーティングされるターゲットエンドポイントの状態を評価します。エンドポイントがエイリアスレコードを介して DNS トラフィックを受信しない場合は、このオプションをオフにして、エンドポイントのヘルスをモニタリングするヘルスチェックを作成します。詳細については、「ヘルスチェックの作成と更新」を参照してください。

位置情報ルール

ユーザーの位置に基づいて Amazon Route 53 が DNS クエリに応答するようにしたい場合に、このオプションを選択します。

詳細については、「位置情報ルーティング」を参照してください。

[Geolocation rule] を選択する場合は、リクエストの発信元となる国またはアメリカの州も選択します。

> **Note**
>
> デフォルトでは、ターゲットの状態の評価がチェックされます。エイリアスレコードを介してトラフィックがルーティングされるターゲットエンドポイントの状態を評価します。エンドポイントがエイリアスレコードを介して DNS トラフィックを受信しない場合は、このオプションをオフにして、エンドポイントのヘルスをモニタリングするヘルスチェックを作成します。詳細については、「ヘルスチェックの作成と更新」を参照してください。

レイテンシールール

複数の Amazon EC2 データセンターに同じ機能を実行するリソースがあり、最もレイテンシーが良いリソースを使って Route 53 が DNS クエリに応答するようにしたい場合に、このオプションを選択します。

[レイテンシールール] を選択する場合は、 AWS リージョンも選択します。

詳細については、「レイテンシーに基づくルーティング」を参照してください。

> **Note**
>
> デフォルトでは、ターゲットの状態の評価がチェックされます。エイリアスレコードを介してトラフィックがルーティングされるターゲットエンドポイントの状態を評価します。エンドポイントがエイリアスレコードを介して DNS トラフィックを受信しない場合は、このオプションをオフにして、エンドポイントのヘルスをモニタリングするヘルスチェックを作成します。詳細については、「ヘルスチェックの作成と更新」を参照してください。

地理的近接性ルール

このオプションは、Route 53 がリソースの口ケーション、および必要に応じて指定したバイアスに基づいて DNS クエリに応答するようにする場合に選択します。このバイアスにより、リソースにより多くのトラフィックを送信するか、リソースからより多くのトラフィックを遠ざけることができます。

[Geoproximity rule] を選択する場合は、次の値を入力します。

エンドポイントの場所

適用可能な値を選択します。

- カスタム (座標を入力) – エンドポイントが AWS リソースでない場合は、カスタム (座標を入力) を選択します。
- AWS リージョン - エンドポイントが AWS リソースの場合は、リソース AWS リージョンを作成した を選択します。
- AWS ローカルゾーン – エンドポイントが AWS リソースの場合は、リソースを作成した AWS ローカルゾーンを選択します。

Local Zones を使用する場合は、まず AWS Local Zones を有効にする必要があります。詳細については、「AWS Local Zones ユーザーガイド」の「Getting started with Local Zones」を参照してください。

使用可能なローカルゾーンについては、「AWS Local Zones ロケーション」を参照してください。

AWS リージョン とローカルゾーンの違いについては、Amazon EC2 ユーザーガイド」の「リージョンとゾーン」を参照してください。

> **Important**
>
> 1 つの地理的近接性ルーティングポリシーに、地理的に同じ大都市圏内に位置する 2 つ以上の場所を含めることはできません。
> さらに、米国西部 (オレゴン) AWS リージョン や米国ポートランドなどの一部の およびローカルゾーンは、同じ地理的近接性ルーティングポリシー内で使用するために互いに近すぎます。同じ大都市圏内の複数の場所にトラフィックをルーティングする必要がある場合は、エリア内の 2 つのエンドポイントに対して 50/50 加重ルーティングルール (WRR) を作成する地理的近接性ルーティングポリシーを定義します。これにより、これらのエンドポイント間でトラフィックが均等に分散されます。

座標

[Endpoint location] (エンドポイントの場所) に [Custom (enter coordinates)] (カスタム (座標の入力)) を選択する場合は、リソースの場所の緯度と経度を入力します。次の点に注意してください。

- 緯度は南緯 (負) または北緯 (正) で表します。有効な値の範囲は -90 度から 90 度です。
- 経度は西経 (負) または東経 (正) で表します。有効な値の範囲は -180 度から 180 度です。
- 緯度と経度は一部のオンラインマップアプリケーションで入手できます。例えば Google マップでは、その場所の URL に緯度と経度が指定されています。

  https://www.google.com/maps/@47.6086111,-122.3409953,20z
- 小数点以下第二位 (例: [47.63]) まで入力できます。それよりも細かく値を指定した場合、Route 53 はこの値を小数点以下第二位までで切り捨てます。緯度と経度は赤道上で、0.01 度が約 0.69 マイルです。

Bias (バイアス)

Route 53 がリソースにルーティングするトラフィックの発信元の地理的リージョンのサイズを必要に応じて変更するには、[バイアス] の値を指定します。

- Route 53 がリソースにルーティングするトラフィックの発信元の地理的リージョンのサイズを拡大するには、バイアスに 1 から 99 までの正の整数を指定します。Route 53 は隣接するリージョンのサイズを縮小します。
- Route 53 がリソースにルーティングするトラフィックの発信元の地理的リージョンのサイズを縮小するには、-1 から -99 までの負のバイアスを指定します。Route 53 は隣接するリージョンのサイズを拡大します。

> **Important**
>
> [Bias (バイアス)] は、他のリソースの場所に基づく相対値であり、距離に基づいた絶対値ではありません。その結果、変更の効果を予測することは簡単ではありません。例えば、リソースの場所によっては、バイアスを 10 から 15 に変更することで、ニューヨーク市都市部からの大量のトラフィックが増減することになります。バイアスを小規模に変更して結果を評価してから、必要に応じてさらに変更を行うことをお勧めします。

詳細については、「地理的近接性ルーティング」を参照してください。

> **Note**
>
> デフォルトでは、ターゲットの状態の評価がチェックされます。エイリアスレコードを介してトラフィックがルーティングされるターゲットエンドポイントの状態を評価します。エンドポイントがエイリアスレコードを介して DNS トラフィックを受信しない場合は、このオプションをオフにして、エンドポイントのヘルスをモニタリングするヘルスチェックを作成します。詳細については、「ヘルスチェックの作成と更新」を参照してください。

複数値回答のルール

ほぼランダムに選択された 8 つまでの正常な回答を Route 53 から DNS クエリに返すには、このオプションを選択します。

詳細については、「複数値回答ルーティング」を参照してください。

> **Note**
>
> デフォルトでは、ターゲットの状態の評価がチェックされます。エイリアスレコードを介してトラフィックがルーティングされるターゲットエンドポイントの状態を評価します。エンドポイントがエイリアスレコードを介して DNS トラフィックを受信しない場合は、このオプションをオフにして、エンドポイントのヘルスをモニタリングするヘルスチェックを作成します。詳細については、「ヘルスチェックの作成と更新」を参照してください。

加重ルール

同じ機能を実行する複数のリソース (同じウェブサイトを対象とする複数のウェブサーバーなど) があり、それらのリソースに対するトラフィックを指定した比率 (あるサーバーに 1/3、もう 1 つのサーバーに 2/3 など) で Route 53 がルーティングするようにしたい場合は、このオプションを選択します。

[Weighted rule (加重ルール)] を選択する場合は、このルールに適用する重みを入力します。

詳細については、「加重ルーティング」を参照してください。

> **Note**
>
> デフォルトでは、ターゲットの状態の評価がチェックされます。エイリアスレコードを介してトラフィックがルーティングされるターゲットエンドポイントの状態を評価します。エンドポイントがエイリアスレコードを介して DNS トラフィックを受信しない場合は、このオプションをオフにして、エンドポイントのヘルスをモニタリングするヘルスチェックを作成します。詳細については、「ヘルスチェックの作成と更新」を参照してください。

Endpoint

DNS クエリのルーティング先となる CloudFront ディストリビューションや Elastic Load Balancing ロードバランサーなどのリソースを指定する場合に、このオプションを選択します。

既存のルール

このトラフィックポリシーの既存のルールに DNS クエリをルーティングする場合に、このオプションを選択します。例えば、2 つ以上の位置情報ルールを作成して、異なる国のクエリを同じフェイルオーバールールにルーティングすることができます。その後、このフェイルオーバールールはクエリを 2 つの Elastic Load Balancing ロードバランサーにルーティングすることもできます。

このオプションはトラフィックポリシーにルールが含まれていない場合は使用できません。

既存のエンドポイント

既存のエンドポイントに DNS クエリをルーティングする場合に、このオプションを選択します。例えば、2 つのフェイルオーバールールがある場合、両方の [On failover] (セカンダリ) オプションの DNS クエリを同じ Elastic Load Balancing ロードバランサーにルーティングすることができます。

このオプションはトラフィックポリシーにエンドポイントが含まれていない場合は使用できません。

値の型

適用可能なオプションを選択します。

CloudFront 配信

CloudFront ディストリビューションにトラフィックをルーティングする場合に、このオプションを選択します。このオプションは、[DNS タイプ] に [A: IPv4 形式の IP アドレス] を選択した場合、または [DNS タイプ] に [AAAA: IPv6 形式の IP アドレス] を選択した場合にのみ使用できます。

> **Note**
>
> CloudFront エイリアスエンドポイントは、ヘルスチェックの評価をサポートしていません。ただし、CloudFront エンドポイントをモニタリングするヘルスチェックを作成できます。詳細については、「ヘルスチェックの作成と更新」を参照してください。

ELB Application load balancer

このオプションは、Elastic Load Balancing Application Load Balancer にトラフィックをルーティングする場合に選択します。このオプションは、[DNS type] (DNS タイプ) に [A: IP address in IPv4 format] (A: IPv4 形式の IP アドレス) または [AAAA: IP address in IPv6 format] (AAAA: IPv6 形式の IP アドレス) を選択した場合のみ指定できます。

ELB Classic load balancer

このオプションは、Elastic Load Balancing Classic Load Balancer にトラフィックをルーティングする場合に選択します。このオプションは、[DNS type] (DNS タイプ) に [A: IP address in IPv4 format] (A: IPv4 形式の IP アドレス) または [AAAA: IP address in IPv6 format] (AAAA: IPv6 形式の IP アドレス) を選択した場合のみ指定できます。

ELB Network Load Balancer

このオプションは、Elastic Load Balancing Network Load Balancer にトラフィックをルーティングする場合に選択します。このオプションは、[DNS type] (DNS タイプ) に [A: IP address in IPv4 format] (A: IPv4 形式の IP アドレス) または [AAAA: IP address in IPv6 format] (AAAA: IPv6 形式の IP アドレス) を選択した場合のみ指定できます。

Elastic Beanstalk 環境

このオプションは、Elastic Beanstalk 環境にトラフィックをルーティングする場合に選択します。このオプションは、[DNS type] (DNS タイプ) に [A: IP address in IPv4 format] (A: IPv4 形式の IP アドレス) を選択した場合のみ指定できます。

S3 ウェブサイトエンドポイント

ウェブサイトエンドポイントとして設定された Amazon S3 バケットにトラフィックをルーティングする場合に、このオプションを選択します。このオプションは、[DNS type] (DNS タイプ) に [A: IP address in IPv4 format] (A: IPv4 形式の IP アドレス) を選択した場合のみ指定できます。

DNS タイプの値の入力

Route 53 が [値] フィールドの値を使って DNS クエリに応答するようにしたい場合に、このオプションを選択します。例えば、このトラフィックポリシーを作成する際に、[DNS type] (DNS タイプ) の値として [A] を選択した場合、[Value type] (値のタイプ) のリストにあるこのオプションは [Type A value] (タイプ A の値) になります。つまり、[Value] (値) フィールドには IPv4 形式で IP アドレスを入力する必要があります。Route 53 は、このエンドポイントにルーティングされた DNS クエリに [値] フィールドに入っている IP アドレスを返します。

値

[Value type (値の型)] で選択したオプションに基づいて値を選択または入力します。

CloudFront 配信

現在の AWS アカウントに関連付けられているディストリビューションのリストから CloudFront ディストリビューションを選択します。

ELB Application load balancer

現在の AWS アカウントに関連付けられているロードバランサーのリストから Elastic Load Balancing Application ロードバランサーを選択します。

ELB Classic load balancer

現在の AWS アカウントに関連付けられているロードバランサーのリストから Elastic Load Balancing Classic ロードバランサーを選択します。

ELB Network Load Balancer

現在の AWS アカウントに関連付けられているロードバランサーのリストから Elastic Load Balancing Network ロードバランサーを選択します。

Elastic Beanstalk 環境

現在の AWS アカウントに関連付けられた環境のリストから Elastic Beanstalk 環境を選択します。

S3 ウェブサイトエンドポイント

ウェブサイトエンドポイントとして設定され、現在の AWS アカウントに関連付けられている Amazon S3 バケットのAmazon S3リストから Amazon S3 バケットを選択します。

> **Important**
>
> このトラフィックポリシーに基づいてポリシーレコードを作成する場合、ここで選択するバケットは、ポリシーレコードの [Policy record DNS name] に指定したドメイン名 (www.example.com など) に一致する必要があります。[Value] (値) と [Policy record DNS name] (ポリシーレコード DNS 名) が一致しない場合、Amazon S3 はそのドメイン名に対する DNS クエリに応答しません。

DNS タイプの値の入力

このトラフィックポリシーを開始したときに [DNS type] で指定した値に対応する値を入力します。たとえば、[DNS type (DNS タイプ)] として [MX] を選択した場合、次の 2 つの値を入力します。メールサーバーに割り当てる優先順位およびメールサーバーのドメイン名 (`10 sydney.mail.example.com` など)。

サポートされる DNS タイプについては、「サポートされる DNS レコードタイプ」を参照してください。

キー (新しいコンソールのみ)

ルーティングルールのフレンドリ名またはキーのエンドポイントを入力します。この値はエディタでノードの名前として表示されます。

地理的近接性の設定の効果を示す地図の表示

地理的近接性ルールを使用すると、 AWS リージョン または Local Zones の両方で、また、緯度と経度を使用して、 以外のAWS リソースの場所を指定できます。地理的近接性ルールを作成すると、デフォルトで Route 53 はユーザーに最も近いリソースにインターネットトラフィックをルーティングするようになります。また、ルーティング元である地理的地域を拡大または縮小するバイアスを指定することでリソースへのトラフィック量を増減させることもできます。地理的近接性ルールの詳細については、「地理的近接性ルーティング」を参照してください。

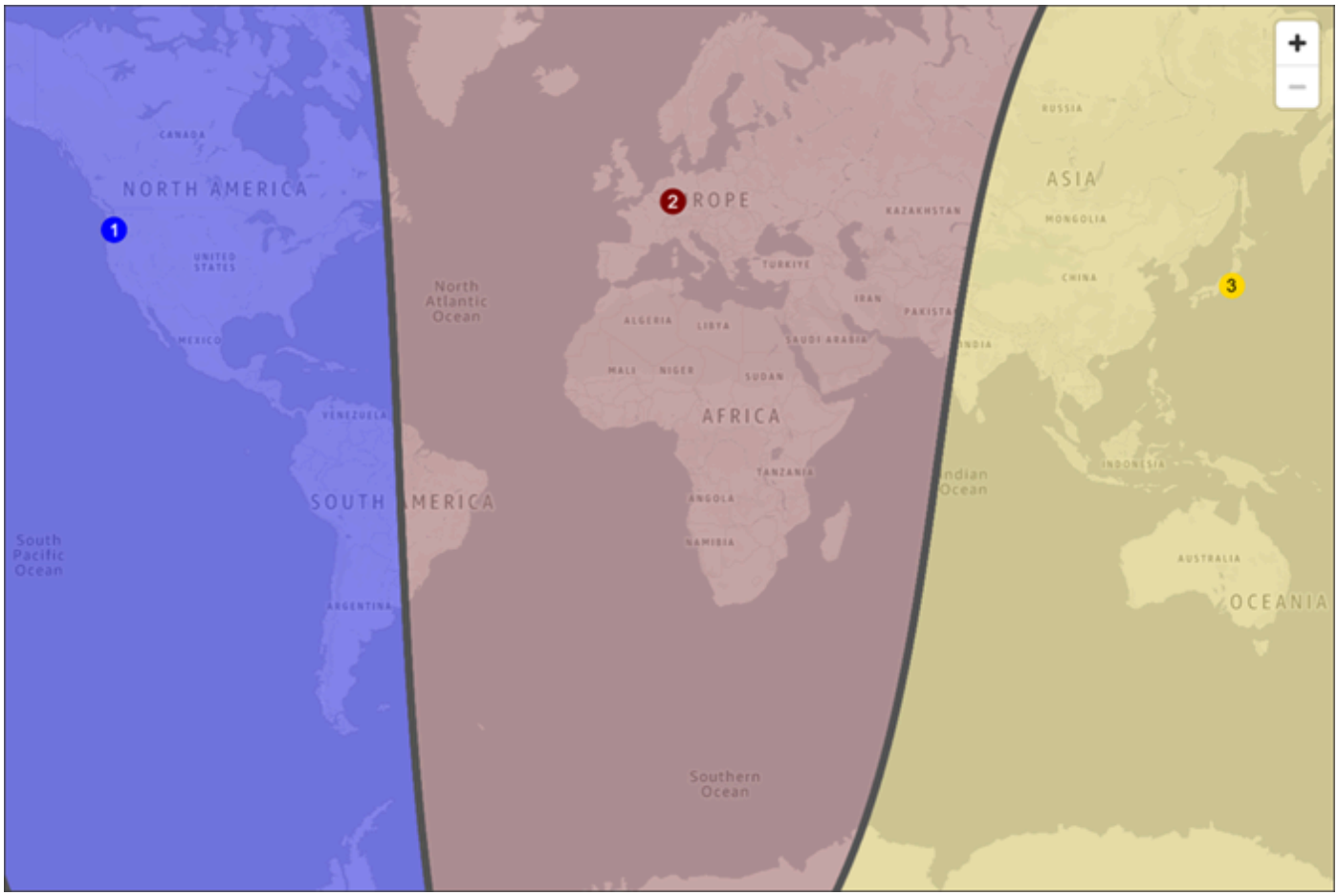
> **Note**
>
> Route 53 は Traffic Flow コンソールを更新しています。旧コンソールは移行期間中も引き続きご使用いただけます。

お使いのコンソールのタブを選択します。

- 新しいコンソール
- 旧コンソール

New console

地理的近接性の現在の設定の効果を示すマップを表示できます。例えば、米国西部 (オレゴン)、欧州 (フランクフルト)、アジアパシフィック (東京) の各リージョンにリソースがあり、バイアスを指定しない場合、次のようなマップになります。



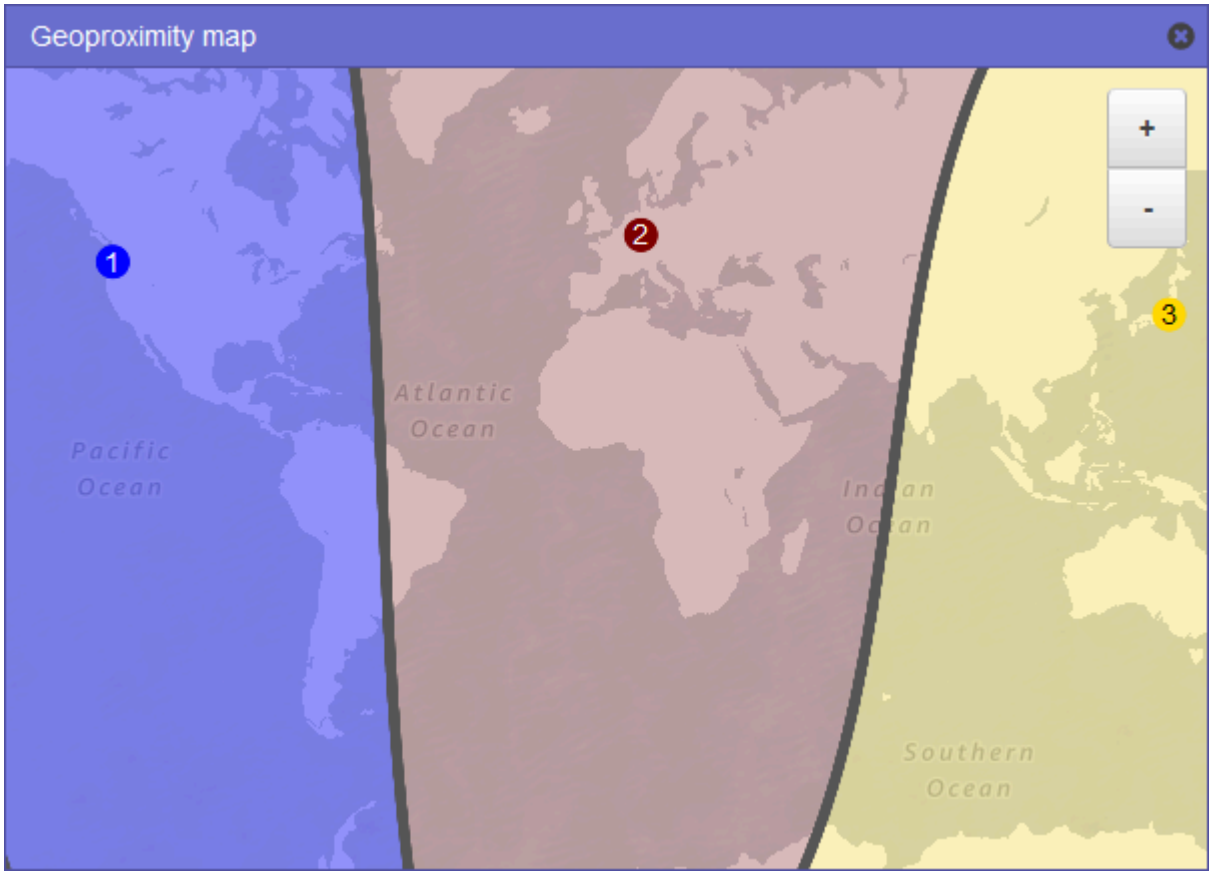
地域を追加または削除すると、地理的近接性ルールのマップが [プロパティ] と更新に自動的に表示されます。

次の点に注意してください。

- マップの精度は約 10 マイル (16 km) です。
- リージョンを追加、編集、削除した場合や、リージョンのバイアス設定を変更した場合、マップが自動的に調整されます。
- 各ルール定義のリージョン番号とカラーは、マップ上の番号とカラーに対応します。
- 拡大および縮小して、表示の詳細度を変更できます。ズームレベルを変更するには、マップ上の [+] および [-] ボタンや、タッチパッド、マウスホイールを使用します。リージョンまたはリージョン番号が表示されない場合は、[プロパティ] ペインを拡大すると表示されます。
- マップウィンドウ内でマップを動かし、特定の領域を表示することができます。タッチパッドを使用するか、マップをドラッグして移動します。ブラウザウィンドウ内でマップウィンドウを移動させることもできます。
- ポリシー内に複数の地理的近接性ルールがある場合、一度に 1 つのルールのマップしか表示できません。

Old console

地理的近接性の現在の設定の効果を示すマップを表示できます。例えば、米国西部 (オレゴン)、欧州 (フランクフルト)、アジアパシフィック (東京) の各リージョンにリソースがあり、バイアスを指定しない場合、次のようなマップになります。



地理的近接性ルールのマップを表示するには、[地理的近接性マップの表示] の横にあるグラフアイコンを選択します。(このアイコンはルールの上部に表示されます。) マップを非表示にするには、アイコンをもう一度選択し、マップの右上角にある [x] を選択します。

次の点に注意してください。

- マップの精度は約 10 マイル (16 km) です。
- リージョンを追加、編集、削除した場合や、リージョンのバイアス設定を変更した場合、マップが自動的に調整されます。
- 各ルール定義のリージョン番号とカラーは、マップ上の番号とカラーに対応します。
- 拡大および縮小して、表示の詳細度を変更できます。ズームレベルを変更するには、マップ上の [+] および [-] ボタンや、タッチパッド、マウスホイールを使用します。
- マップウィンドウ内でマップを動かし、特定の領域を表示することができます。タッチパッドを使用するか、マップをドラッグして移動します。ブラウザウィンドウ内でマップウィンドウを移動させることもできます。
- ポリシー内に複数の地理的近接性ルールがある場合、一度に 1 つのルールのマップしか表示できません。

トラフィックポリシーの追加のバージョンの作成

トラフィックポリシーを編集する場合、Amazon Route 53 はトラフィックポリシーの別のバージョンを自動的に作成し、削除するまで以前のバージョンを保持します。新しいバージョンの名前は編集しているトラフィックポリシーの名前と同じになります。Route 53 が自動的にカウントアップするバージョン番号によってオリジナルバージョンと区別できます。トラフィックポリシーの新しいバージョンは、同じ名前が付けられたトラフィックポリシーの任意の既存のバージョンに基づくことができます。

Route 53 は特定のトラフィックポリシーの新しいバージョンで、バージョン番号を再利用しません。たとえば、3 つのバージョンの [MyTrafficPolicy] を作成した後、最後の 2 つのバージョンを削除して別のバージョンを作成した場合、新しいバージョンはバージョン 4 となります。以前のバージョンを保持することにより、Route 53 は新しい設定で希望どおりにトラフィックをルーティングできない場合にロールバックできることを保証しています。

新しいトラフィックポリシーバージョンを作成するには、以下の手順を実行します。

> **Note**
>
> Route 53 は Traffic Flow コンソールを更新しています。旧コンソールは移行期間中も引き続きご使用いただけます。

お使いのコンソールのタブを選択します。

- 新しいコンソール
- 旧コンソール

New console

トラフィックポリシーの別のバージョンを作成するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで、[Traffic policies] を選択します。
3. 新しいバージョンを作成するトラフィックポリシーの名前を選択します。

4. ページ上部の [Traffic policy versions] の表で、新しいトラフィックポリシーバージョンのベースとして使用するトラフィックポリシーバージョンのチェックボックスをオンにします。
5. [Edit policy as new version] を選択します。
6. [ポリシーを新しいバージョンとして編集] ダイアログボックスで、新しいトラフィックポリシーバージョンの説明を入力します。このバージョンを同じトラフィックポリシーの他のバージョンと区別する説明を指定します。新しいポリシーレコードを作成すると、指定した値はこのトラフィックポリシーで使用可能なバージョンの一覧に表示されます。
7. [次へ] を選択します。
8. 必要に応じて設定を更新します。詳細については、「トラフィックポリシーを作成するときに指定する値」を参照してください。

   トラフィックポリシーのルール、エンドポイント、ブランチは、次の方法で削除できます。

   - ルールまたはエンドポイントを削除するには、エディタでルールを選択し、[プロパティ] ペインで [削除] を選択します。

     > **Important**
     >
     > 子ルールおよび子エンドポイントがあるルールを削除すると、Route 53 はそれらの子もすべて削除します。

   - 2 つのルールが同じ子ルールまたは子エンドポイントに接続されていて、片方の接続を削除する場合、削除する接続を選択し、[プロパティ] ペインの [削除] を選択します。
9. 編集を終えると、[Save as new version] を選択します。
10. オプション: 新しいトラフィックポリシーバージョンを使って、1 つのホストゾーンで 1 つ以上のポリシーレコードを作成するための設定を指定します。詳細については、「ポリシーレコードを作成または更新する場合に指定する値」を参照してください。後で、同じホストゾーンまたは追加のホストゾーンでポリシーレコードを作成することもできます。

    ポリシーレコードを今すぐ作成しない場合は、キャンセルを選択すると、コンソールに現在の AWS アカウントを使用して作成したトラフィックポリシーとポリシーレコードのリストが表示されます。
11. 前述のステップでレコードポリシーの設定を指定した場合、[Create policy record] を選択します。

Old console

トラフィックポリシーの別のバージョンを作成するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで、[Traffic policies] を選択します。
3. 新しいバージョンを作成するトラフィックポリシーの名前を選択します。
4. ページ上部の [Traffic policy versions] の表で、新しいトラフィックポリシーバージョンのベースとして使用するトラフィックポリシーバージョンのチェックボックスをオンにします。
5. [Edit policy as new version] を選択します。
6. [Update description (更新点の説明)] ページで、新しいトラフィックポリシーバージョンの説明を入力します。このバージョンを同じトラフィックポリシーの他のバージョンと区別する説明を指定します。新しいポリシーレコードを作成すると、指定した値はこのトラフィックポリシーで使用可能なバージョンの一覧に表示されます。
7. [次へ] を選択します。
8. 必要に応じて設定を更新します。詳細については、「トラフィックポリシーを作成するときに指定する値」を参照してください。

   トラフィックポリシーのルール、エンドポイント、ブランチは、次の方法で削除できます。

   - ルールまたはエンドポイントを削除するには、ボックスの右上隅にある x を選択します。

     > **Important**
     >
     > 子ルールおよび子エンドポイントがあるルールを削除すると、Route 53 はそれらの子もすべて削除します。

   - 2 つのルールを同じ子ルールまたはエンドポイントに接続し、いずれかの接続を削除する場合は、削除する接続にカーソルを置き、その接続の x を選択します。
9. 編集を終えると、[Save as new version] を選択します。
10. オプション: 新しいトラフィックポリシーバージョンを使って、1 つのホストゾーンで 1 つ以上のポリシーレコードを作成するための設定を指定します。詳細については、「ポリシーレコードを作成または更新する場合に指定する値」を参照してください。後で、同じホストゾーンまたは追加のホストゾーンでポリシーレコードを作成することもできます。

今すぐポリシーレコードを作成しない場合は、このステップをスキップを選択すると、コンソールに現在の AWS アカウントを使用して作成したトラフィックポリシーとポリシーレコードのリストが表示されます。

11. 前述のステップでレコードポリシーの設定を指定した場合、[Create policy record] を選択します。

JSON ドキュメントを使用してトラフィックポリシーを作成する

トラフィックポリシーに含めるすべてのエンドポイントとルールを説明した JSON 形式のドキュメントをインポートすることによって、新しいトラフィックポリシーまたは既存のトラフィックポリシーの新しいバージョンを作成できます。JSON ドキュメントの形式、およびコピーして修正できるいくつかの例については、「Amazon Route 53 API リファレンス」の「Traffic Policy Document Format (トラフィックポリシードキュメントの形式)」を参照してください。

既存のトラフィックポリシーバージョンの JSON 形式のドキュメントを取得する最も簡単な方法は、 CLI AWS で `get-traffic-policy` コマンドを使用することです。詳細については、AWS CLI コマンドリファレンスの「get-traffic-policy」を参照してください。

`get-traffic-policy` コマンドによって作成された JSON ファイルには、エスケープ文字としてバックスラッシュ (\) が含まれます。JSON ファイルをインポートするときは、先に、すべてのバックスラッシュを NULL 文字に置き換えます。

> **Note**
>
> Route 53 は Traffic Flow コンソールを更新しています。旧コンソールは移行期間中も引き続きご使用いただけます。

お使いのコンソールのタブを選択します。

- 新しいコンソール
- 旧コンソール

New console

JSON ドキュメントをインポートしてトラフィックポリシーを作成する

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. JSON ドキュメントをインポートしてトラフィックポリシーを作成するには、以下の手順に従ってください。

   a. ナビゲーションペインで、[Traffic policies] を選択します。

   b. [Create traffic policy] を選択します。

   c. [Name policy] ページで、適切な値を指定します。詳細については、「トラフィックポリシーを作成するときに指定する値」を参照してください。

   d. ステップ 4 に進みます。
3. JSON ドキュメントをインポートして既存のトラフィックポリシーの新しいバージョンを作成するには、以下の手順に従ってください:

   a. ナビゲーションペインで、[Traffic policies] を選択します。

   b. 新しいバージョンのベースにするトラフィックポリシーの名前を選択します。

   c. [Traffic policy versions] の表で、新しいバージョンのベースにするバージョンのチェックボックスをオンにします。

   d. [Edit policy as new version] を選択します。

   e. [Update description (更新点の説明)] ページで、新しいバージョンの説明を入力します。

   f. ステップ 4 に進みます。
4. [次へ] を選択します。
5. エディタページで、エディタの右上隅にある JSON エディタ

   (</>)

   アイコンを選択します。
6. 新しいトラフィックポリシーを入力し、トラフィックポリシーの例を貼り付けるか、既存のトラフィックポリシーを貼り付けます。

   ポリシーの例については、「トラフィックフローポリシー JSON の例」を参照してください。
7. [更新] を選択します。

Old console

JSON ドキュメントをインポートしてトラフィックポリシーを作成する

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. JSON ドキュメントをインポートしてトラフィックポリシーを作成するには、以下の手順に従ってください。

   a. ナビゲーションペインで、[Traffic policies] を選択します。

   b. [Create traffic policy] を選択します。

   c. [Name policy] ページで、適切な値を指定します。詳細については、「トラフィックポリシーを作成するときに指定する値」を参照してください。

   d. ステップ 4 に進みます。
3. JSON ドキュメントをインポートして既存のトラフィックポリシーの新しいバージョンを作成するには、以下の手順に従ってください:

   a. ナビゲーションペインで、[Traffic policies] を選択します。

   b. 新しいバージョンのベースにするトラフィックポリシーの名前を選択します。

   c. [Traffic policy versions] の表で、新しいバージョンのベースにするバージョンのチェックボックスをオンにします。

   d. [Edit policy as new version] を選択します。

   e. [Update description (更新点の説明)] ページで、新しいバージョンの説明を入力します。

   f. ステップ 4 に進みます。
4. [次へ] を選択します。
5. [Import traffic policy] を選択します。
6. 新しいトラフィックポリシーを入力し、トラフィックポリシーの例を貼り付けるか、既存のトラフィックポリシーを貼り付けます。

   ポリシーの例については、「トラフィックフローポリシー JSON の例」を参照してください。
7. [Import traffic policy] を選択します。

トラフィックポリシーバージョンおよび関連するポリシーレコードの表示

トラフィックポリシーで作成したすべてのバージョン、およびトラフィックポリシーの各バージョンを使って作成したすべてのポリシーレコードを表示できます。

> **Note**
>
> Route 53 は Traffic Flow コンソールを更新しています。旧コンソールは移行期間中も引き続きご使用いただけます。

お使いのコンソールのタブを選択します。

- 新しいコンソール
- 旧コンソール

New console

トラフィックポリシーバージョンおよび関連するポリシーレコードを表示するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで、[Traffic policies] を選択します。
3. トラフィックポリシーのリンクされた名前を選択します。
4. 上の表では、トラフィックポリシーで作成したすべてのバージョンが一覧表示されます。表には、次の情報が含まれます。

   バージョン番号

   作成したトラフィックポリシーの各バージョンの数。バージョン番号を選択した場合、コンソールにはそのバージョンの設定が表示されます。

   ポリシーレコードの数

   このポリシーバージョンを使って作成したポリシーレコードの数。

   DNS タイプ

   トラフィックポリシーバージョンを作成したときに指定した DNS タイプ。

バージョンの説明

トラフィックポリシーバージョンを作成したときに指定した説明。

5. 下の表では、上の表にあるトラフィックポリシーバージョンを使って作成したすべてのポリシーレコードの一覧を表示しています。表には、次の情報が含まれます。

[DNS 名]

トラフィックポリシーを関連付けた DNS の名前。

ステータス

以下に示しているのは、可能な値です。

申請済み

Route 53 はポリシーレコードおよび対応するレコードの作成および更新を終了しました。

作成

Route 53 は新しいポリシーレコード用にレコードを作成しています。

更新中

ポリシーレコードを更新し、Route 53 は、指定された DNS 名でレコードの既存のグループを置き換えるレコードの新しいグループを作成中です。

削除

Route 53 はポリシーレコードおよび関連するレコードを削除中です。

失敗

Route 53 はポリシーレコードおよび関連するレコードを作成または更新できませんでした。

DNS タイプ

このポリシーレコード用に Route 53 が作成したすべてのレコードの DNS タイプ。ポリシーレコードを編集する場合、編集するポリシーレコードの DNS タイプと同じ DNS タイプを持つトラフィックポリシーバージョンを指定する必要があります。

バージョン

ポリシーレコードを作成するために使用したトラフィックポリシーのバージョンを示します。

TTL (秒単位)

DNS 再帰リゾルバーがこのレコードに関する情報をキャッシュする秒単位の時間。より大きい値 (172,800 秒 = 2 日など) を指定した場合、再帰的なリゾルバーが Route 53 にリクエストを送信する頻度が低くなるため、Route 53 サービスのコストが低くなります。ただし、再帰的なリゾルバーは、Route 53 に最新の情報を問い合わせる代わりに、長い間キャッシュ内の値を使用するため、レコードに対する変更 (例えば、新しい IP アドレス) が有効になるまでに時間が多くかかります。

Old console

トラフィックポリシーバージョンおよび関連するポリシーレコードを表示するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで、[Traffic policies] を選択します。
3. トラフィックポリシーの名前を選択します。
4. 上の表では、トラフィックポリシーで作成したすべてのバージョンが一覧表示されます。表には、次の情報が含まれます。

   バージョン番号

   作成したトラフィックポリシーの各バージョンの数。バージョン番号を選択した場合、コンソールにはそのバージョンの設定が表示されます。

   ポリシーレコードの数

   このポリシーバージョンを使って作成したポリシーレコードの数。

   DNS タイプ

   トラフィックポリシーバージョンを作成したときに指定した DNS タイプ。

   バージョンの説明

   トラフィックポリシーバージョンを作成したときに指定した説明。

5. 下の表では、上の表にあるトラフィックポリシーバージョンを使って作成したすべてのポリシーレコードの一覧を表示しています。表には、次の情報が含まれます。

   ポリシーレコード DNS 名

   トラフィックポリシーを関連付けた DNS の名前。

   ステータス

   以下に示しているのは、可能な値です。

   申請済み

   Route 53 はポリシーレコードおよび対応するレコードの作成および更新を終了しました。

   作成

   Route 53 は新しいポリシーレコード用にレコードを作成しています。

   更新中

   ポリシーレコードを更新し、Route 53 は、指定された DNS 名でレコードの既存のグループを置き換えるレコードの新しいグループを作成中です。

   削除

   Route 53 はポリシーレコードおよび関連するレコードを削除中です。

   失敗

   Route 53 はポリシーレコードおよび関連するレコードを作成または更新できませんでした。

   使用バージョン

   ポリシーレコードを作成するために使用したトラフィックポリシーのバージョンを示します。

   DNS タイプ

   このポリシーレコード用に Route 53 が作成したすべてのレコードの DNS タイプ。ポリシーレコードを編集する場合、編集するポリシーレコードの DNS タイプと同じ DNS タイプを持つトラフィックポリシーバージョンを指定する必要があります。

TTL (秒単位)

DNS 再帰リゾルバーがこのレコードに関する情報をキャッシュする秒単位の時間。より大きい値 (172,800 秒 = 2 日など) を指定した場合、再帰的なリゾルバーが Route 53 にリクエストを送信する頻度が低くなるため、Route 53 サービスのコストが低くなります。ただし、再帰的なリゾルバーは、Route 53 に最新の情報を問い合わせる代わりに、長い間キャッシュ内の値を使用するため、レコードに対する変更 (例えば、新しい IP アドレス) が有効になるまでに時間が多くかかります。

トラフィックポリシーバージョンとトラフィックポリシーの削除

トラフィックポリシーを削除するには、トラフィックポリシー用に作成したすべてのバージョン (オリジナルを含む) を削除する必要があります。加えて、トラフィックポリシーバージョンを削除するには、トラフィックポリシーバージョンを使用して作成したすべてのポリシーレコードを削除する必要があります。

> **Important**
>
> Amazon Route 53 が DNS クエリへの応答に使用しているポリシーレコードを削除すると、Route 53 は対応する DNS 名のクエリへの応答を停止します。例えば、Route 53 が www.example.com のポリシーレコードを使用して www.example.com の DNS クエリに応答し、ポリシーレコードを削除した場合、ユーザーはドメイン名 www.example.com を使用してウェブサイトまたはウェブアプリケーションにアクセスできません。

トラフィックポリシーバージョンおよび、必要に応じて、トラフィックポリシーを削除するには、以下の手順を実行します。

> **Note**
>
> Route 53 は Traffic Flow コンソールを更新しています。旧コンソールは移行期間中も引き続きご使用いただけます。

お使いのコンソールのタブを選択します。

- 新しいコンソール
- 旧コンソール

New console

トラフィックポリシーバージョンおよびトラフィックポリシーを削除するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで、[Traffic policies] を選択します。
3. トラフィックポリシーバージョン、または必要に応じてトラフィックポリシー全体を削除するトラフィックポリシーのリンクされた名前を選択します。
4. 上のテーブルで削除するトラフィックポリシーバージョンが [Policy records] (ポリシーレコード) テーブルの [Version] (バージョン) 列に表示されている場合、下のテーブルの対応するポリシーレコードのチェックボックスをオンにします。

   例えば、トラフィックポリシーのバージョン 3 を削除する場合、下の表のいずれかのポリシーレコードをバージョン 3 で作成したなら、そのポリシーレコードのチェックボックスをオンにします。
5. [ポリシーレコードの削除] を選択し、[ポリシーレコードの削除] ダイアログボックスで [確認] を選択します。
6. 削除したポリシーレコードがテーブルに表示されなくなるまで、ページを更新します。
7. 上の表で、削除するトラフィックポリシーバージョンのチェックボックスをオンにします。
8. [削除] を選択します。
9. 前述のステップですべてのトラフィックポリシーバージョンを削除し、トラフィックポリシーも削除する場合、テーブルが空になるまでページを更新し、ディスプレイを更新します。
10. ナビゲーションペインで、[Traffic policies] を選択します。
11. トラフィックポリシーのリストで、削除するトラフィックポリシーのチェックボックスをオンにします。
12. [Delete traffic policy] を選択します。

Old console

トラフィックポリシーバージョンおよびトラフィックポリシーを削除するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。

2. ナビゲーションペインで、[Traffic policies] を選択します。
3. トラフィックポリシーバージョン、または必要に応じてトラフィックポリシー全体を削除するトラフィックポリシーの名前を選択します。
4. 上の表で削除するトラフィックポリシーバージョンが下の表の [Version used] に表示されている場合、下の表の対応するポリシーレコードのチェックボックスをオンにします。

   例えば、トラフィックポリシーのバージョン 3 を削除する場合、下の表のいずれかのポリシーレコードをバージョン 3 で作成したなら、そのポリシーレコードのチェックボックスをオンにします。
5. [Delete policy records] を選択します。
6. 削除したポリシーレコードが表に表示されなくなるまで、下の表の [Refresh] ボタンを選択してディスプレイを更新します。
7. 上の表で、削除するトラフィックポリシーバージョンのチェックボックスをオンにします。
8. [Delete version] を選択します。
9. 前述のステップですべてのトラフィックポリシーバージョンを削除し、トラフィックポリシーも削除する場合、表が空になるまで上の表の [Refresh] ボタンを選択してディスプレイを更新します。
10. ナビゲーションペインで、[Traffic policies] を選択します。
11. トラフィックポリシーのリストで、削除するトラフィックポリシーのチェックボックスをオンにします。
12. [Delete traffic policy] を選択します。

ポリシーレコードの作成および管理

トラフィックポリシーを作成したときに指定したリソースにインターネットトラフィックをルーティングするには、1 つ以上のポリシーレコードを作成します。各ポリシーレコードは、ポリシーレコードを作成するホストゾーンと、トラフィックをルーティングするドメインまたはサブドメイン名を識別します。たとえば、www.example.com のトラフィックをルーティングする場合は、example.com がホストされたゾーンのホストゾーン ID を指定し、ポリシーレコード DNS 名にwww.example.com を指定します。

同じトラフィックポリシーを使用して、複数のドメインまたはサブドメイン名のトラフィックをルーティングする場合は、次の 2 つのオプションがあります。

- 各ドメインまたはサブドメイン名のポリシーレコードを作成できます。

- 1 つのポリシーレコードを作成し、そのポリシーレコードを参照する CNAME またはエイリアスレコードを作成します。

例えば、example.com、example.net、example.org に同じトラフィックポリシーを使用する場合、次のいずれかを実行できます。

- それぞれに 1 つのポリシーレコードを作成します。
- いずれか 1 つに対してポリシーレコードを作成し、他の 2 つ用のホストゾーンで CNAME レコードを作成します。2 つの CNAME レコードで、ポリシーレコードを作成したレコードの名前を指定します。

ドメインとそのサブドメイン (example.com と www.example.com など) に同じトラフィックポリシーを使用する場合、1 つの名前に対してポリシーレコードを作成し、他の名前に対してエイリアスレコードを作成できます。例えば、example.com のポリシーレコードを作成し、エイリアスターゲットとして example.com レコードを持つ www.example.com のエイリアスレコードを作成できます。

> **Note**
>
> 作成する各ポリシーレコードについて月額料金が発生します。複数のドメインまたはサブドメイン名に同じトラフィックポリシーを使用する場合は、CNAME またはエイリアスレコードを使用して料金を削減できます。
>
> - 1 つのポリシーレコードを作成し、そのポリシーレコードを参照する 1 つ以上の CNAME レコードを作成する場合、そのポリシーレコードおよび CNAME レコード用の DNS クエリに対してのみ料金が発生します。
> - 1 つのポリシーレコードと、そのポリシーレコードを参照する同じホストゾーンで 1 つ以上のエイリアスレコードを作成する場合、そのポリシーレコードおよびエイリアスレコードの DNS クエリに対してのみ料金が発生します。

トピック

- ポリシーレコードの作成
- ポリシーレコードを作成または更新する場合に指定する値
- ポリシーレコードの更新
- ポリシーレコードの削除

ポリシーレコードの作成

ポリシーレコードを作成するには、以下の手順を実行します。

> **Important**
>
> 作成する各ポリシーレコードについて月額料金が発生します。後にポリシーレコードを削除すると、料金は按分されます。詳細については、Amazon Route 53 の料金表の「トラフィックフロー」セクションを参照してください。

> **Note**
>
> Route 53 は Traffic Flow コンソールを更新しています。旧コンソールは移行期間中も引き続きご使用いただけます。

お使いのコンソールのタブを選択します。

- 新しいコンソール
- 旧コンソール

New console

ポリシーレコードを作成するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで、[Policy records] を選択します。
3. [Policy records] ページで、[Create policy records] を選択します。
4. [Create policy records] ページで、該当する値を指定します。詳細については、「ポリシーレコードを作成または更新する場合に指定する値」を参照してください。
5. 同じホストゾーンにレコードを追加するには、[ポリシーレコードの追加] を選択します。
6. [Create policy records] を選択します。

   作成されたポリシーレコードのステータスが [適用済み] と表示されるまでに数分かかる場合があります。

7. 別のホストゾーンでポリシーレコードを作成する場合、ステップ 3 ~ 5 を繰り返します。

> **Note**
>
> ポリシーレコードのステータスが [失敗] の場合、ステータスの横にある [情報] ボタンを選択し、失敗に関する詳細情報を取得してください。サポートが必要な場合は AWS 、「 からテクニカルサポートを受けるにはどうすればよいですか？」を参照してください AWS。

Old console

ポリシーレコードを作成するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで、[Policy records] を選択します。
3. [Policy records] ページで、[Create policy records] を選択します。
4. [Create policy records] ページで、該当する値を指定します。詳細については、「ポリシーレコードを作成または更新する場合に指定する値」を参照してください。
5. [Create policy records] を選択します。

   作成されたポリシーレコードのステータスが [適用済み] と表示されるまでに数分かかる場合があります。
6. 別のホストゾーンでポリシーレコードを作成する場合、ステップ 3 ~ 5 を繰り返します。

> **Note**
>
> ポリシーレコードのステータスが [失敗] の場合、ステータスの横にある [情報] ボタンを選択し、失敗に関する詳細情報を取得してください。サポートが必要な場合は AWS 、「 からテクニカルサポートを受けるにはどうすればよいですか？」を参照してください AWS。

ポリシーレコードを作成または更新する場合に指定する値

> **Note**
>
> Route 53 は Traffic Flow コンソールを更新しています。旧コンソールは移行期間中も引き続きご使用いただけます。次のリストは、特に明記されていない限り、両方のコンソールに適用されます。

ポリシーレコードを作成または更新する場合、次の値を指定します。

- Traffic policy
- Version
- Hosted zone
- Policy record DNS name
- TTL

トラフィックポリシー

このポリシーレコードで使用する設定のトラフィックポリシーを選択します。

バージョン

このポリシーレコードで使用する設定のトラフィックポリシーのバージョンを選択します。

既存のポリシーレコードを更新する場合、ポリシーレコードの現在の DNS タイプに一致する DNS タイプのバージョンを選択する必要があります。たとえば、ポリシーレコードの DNS タイプが [A] の場合、DNS タイプが [A] のバージョンを選択する必要があります。

ホストゾーン

指定したトラフィックポリシーとバージョンを使用してポリシーレコードを作成するホストゾーンを選択します。ポリシーレコードを作成した後に [Hosted zone] の値を変更することはできません。

DNS 名 (新しいコンソール)、ポリシーレコード DNS 名 (古いコンソール)

ポリシーレコードを作成する場合、指定したトラフィックポリシーとバージョンを使用して Route 53 が DNS クエリに応答するドメイン名またはサブドメイン名を入力します。

指定したホストゾーンで複数のドメイン名またはサブドメイン名で同じ設定を使用するには、[Add policy record] (ポリシーレコードの追加) (新しいコンソール) または [Add another policy record] (別のポリシーレコードの追加) (古いコンソール) を選択して、該当するドメイン名またはサブドメイン名および TTL を入力します。

ポリシーレコードを作成した後に [Policy record DNS name] の値を変更することはできません。

TTL (秒単位)

再帰的な DNS リゾルバーでこのレコードに関する情報をキャッシュしておく時間 (秒単位) を入力します。より大きい値 (172800 秒、つまり 2 日など) を指定した場合、再帰的なリゾルバーが Route 53 にリクエストを送信する頻度が低くなるため、Route 53 サービスのコストが低くなります。ただし、再帰的なリゾルバーは、Route 53 に最新の情報を問い合わせる代わりに、長い間キャッシュ内の値を使用するため、レコードに対する変更 (例えば、新しい IP アドレス) が有効になるまでに時間が多くかかります。

ポリシーレコードの更新

ポリシーレコードの設定を更新するには、以下の手順を実行します。

> **Note**
>
> Route 53 は Traffic Flow コンソールを更新しています。旧コンソールは移行期間中も引き続きご使用いただけます。

お使いのコンソールのタブを選択します。

- 新しいコンソール
- 旧コンソール

New console

ポリシーレコードを更新するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで、[Policy records] を選択します。

3. [Policy records] (ポリシーレコード) ページで、更新するポリシーレコードのチェックボックスをオンにして、[Edit] (編集) を選択します。
4. [Edit policy record] ページで、該当する値を指定します。詳細については、「ポリシーレコードを作成または更新する場合に指定する値」を参照してください。
5. [Edit policy record] を選択します。

   作成されたポリシーレコードのステータスが [適用済み] と表示されるまでに数分かかる場合があります。
6. 別のポリシーレコードを更新するには、ステップ 3 ~ 5 を繰り返します。

> **Note**
>
> ポリシーレコードのステータスが [失敗] の場合、ステータスの横にある [情報] ボタンを選択し、失敗に関する詳細情報を取得してください。サポートが必要な場合は AWS 、「 からテクニカルサポートを受けるにはどうすればよいですか？」を参照してください AWS。

Old console

ポリシーレコードを更新するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで、[Policy records] を選択します。
3. [Policy records] ページで、更新するポリシーレコードのチェックボックスをオンにして、[Edit policy record] を選択します。
4. [Edit policy record] ページで、該当する値を指定します。詳細については、「ポリシーレコードを作成または更新する場合に指定する値」を参照してください。
5. [Edit policy record] を選択します。

   作成されたポリシーレコードのステータスが [適用済み] と表示されるまでに数分かかる場合があります。
6. 別のポリシーレコードを更新するには、ステップ 3 ~ 5 を繰り返します。

> **Note**
>
> ポリシーレコードのステータスが [失敗] の場合、ステータスの横にある [情報] ボタンを選択し、失敗に関する詳細情報を取得してください。サポートが必要な場合は AWS 、「 からテクニカルサポートを受けるにはどうすればよいですか？」を参照してください AWS。

ポリシーレコードの削除

ポリシーレコードを削除するには、以下の手順を実行します。

> **Important**
>
> Amazon Route 53 が DNS クエリへの応答に使用しているポリシーレコードを削除すると、Route 53 は対応する DNS 名のクエリへの応答を停止します。例えば、Route 53 が www.example.com のポリシーレコードを使用して www.example.com の DNS クエリに応答し、ポリシーレコードを削除した場合、ユーザーはドメイン名 www.example.com を使用してウェブサイトまたはウェブアプリケーションにアクセスできません。

> **Note**
>
> Route 53 は Traffic Flow コンソールを更新しています。旧コンソールは移行期間中も引き続きご使用いただけます。

お使いのコンソールのタブを選択します。

- 新しいコンソール
- 旧コンソール

New console

ポリシーレコードを削除するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。

2. ナビゲーションペインで、[Policy records] を選択します。
3. [Policy records] (ポリシーレコード) ページで、削除するポリシーレコードのチェックボックスをオンにして、[Delete] (削除) を選択します。
4. [Delete policy record] (ポリシーレコードの削除) ダイアログボックスで、 [Confirm] (確認) を選択します。

   数分待ってからページを更新し、ポリシーレコードがリストから消えることを確認します。

Old console

ポリシーレコードを削除するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで、[Policy records] を選択します。
3. [Policy records] ページで、削除するポリシーレコードのチェックボックスをオンにして、[Delete policy record] を選択します。

   数分待ってからページを更新し、ポリシーレコードがリストから消えることを確認します。

トラフィックポリシードキュメントの形式

Amazon Route 53 API、 AWS SDKs の 1 つ、、 AWS CLIまたは を使用してプログラムでトラフィックポリシーを作成する場合は AWS Tools for Windows PowerShell、トラフィックポリシーの定義を JSON 形式の `Document`要素で指定します。

トラフィックポリシーの詳細については、Amazon Route 53 デベロッパーガイドの「トラフィックフローを使用して DNS トラフィックをルーティング」を参照してください。

トピック

- 基本構文
- エンドポイント定義の構文
- ルール定義の構文
- 例

基本構文

トラフィックポリシードキュメントの基本的な構文は次のとおりです。

```
{
   "AWSPolicyFormatVersion": "2015-10-01 | 2023-05-09",
   "RecordType": "DNS type for all resource record sets created by this traffic
 policy",
   "StartEndpoint | StartRule": "ID that you assign to an endpoint or rule",
   "Endpoints": {
      "Endpoint ID that you assign": {
         Endpoint definition
      },
      ...
   },
   "Rules": {
      "Rule ID that you assign": {
         Rule definition
      },
      ...
   }
}
```

トラフィックポリシードキュメントの基本的な構文には、次のオブジェクトが含まれています。

AWSPolicyFormatVersion

トラフィックポリシー形式のバージョン、 AWS ローカルゾーンをサポートする最新バージョン、2023-05-09。

以前のバージョン もサポートされています2015-10-01。

RecordType

このトラフィックポリシーに基づいて Amazon Route 53 が作成するすべてのリソースレコードセットの DNS タイプ。トラフィックを次の AWS リソースにルーティングする場合は、該当する値を選択します。

- CloudFront ディストリビューション – [A: IPv4 形式の IP アドレス] または [AAAA: IPv6 形式の IP アドレス] を選択します。
- ELB Application Load Balancer – [A: IPv4 形式の IP アドレス] または [AAAA: IPv6 形式の IP アドレス] を選択します。

- ELB Classic Load Balancer – [A: IPv4 形式の IP アドレス] または [AAAA: IPv6 形式の IP アドレス] を選択します。
- ELB Network Load Balancer – [A: IPv4 形式の IP アドレス] または [AAAA: IPv6 形式の IP アドレス] を選択します。
- Elastic Beanstalk 環境 – A: IPv4 形式の IP アドレスまたは AAAA: IPv6 形式の IP アドレスを選択します。
- ウェブサイトエンドポイントとして設定された Amazon S3 バケット: [A: IP address in IPv4 format] (A: IPv4 形式の IP アドレス) を選択します。

トラフィックを他のリソースにルーティングする場合は、リソースに適したタイプを選択します。たとえば、トラフィックをメールサーバーにルーティングする場合は、 を指定しますMX。Route 53 がサポートする DNS タイプのリストについては、「Amazon Route 53 デベロッパーガイド」の「サポートされている DNS リソースレコードタイプ」を参照してください。

StartEndpoint | StartRule

トラフィックポリシーの開始点をエンドポイントとルールのどちらにするか、およびトラフィックポリシードキュメントの他の場所でエンドポイントまたはルールに割り当てた ID。

エンドポイント

このトラフィックポリシーで使用するエンドポイントの定義。詳細については、「エンドポイント定義の構文」を参照してください。

Rules

このトラフィックポリシーで使用するルールの定義。詳細については、「ルール定義の構文」を参照してください。

エンドポイント定義の構文

トラフィックポリシードキュメントで指定するエンドポイント定義の構文は次のとおりです。

```
{
   "Type": value | cloudfront | application-load-balancer | elastic-load-balancer |
 network-load-balancer | elastic-beanstalk | s3-website,
   "Region": "AWS region that you created your Amazon S3 bucket in"
   "Value": "value applicable to the type of endpoint"
}
```

エンドポイント定義の構文には、次のオブジェクトが含まれます。

タイプ

該当する値を指定します。

値

次のリストのリソース以外のリソースにトラフィックをルーティングするには、 valueに を指定しますType。

cloudfront

CloudFront ディストリビューションにトラフィックをルーティングするには、 cloudfrontに を指定しますType。

application-load-balancer

Application Load Balancer にトラフィックをルーティングするには、 application-load-balancerに を指定しますType。

elastic-load-balancer

ELB Classic ロードバランサーにトラフィックをルーティングするには、 elastic-load-balancerに を指定しますType。

network-load-balancer

ELB Network Load Balancer にトラフィックをルーティングするには、 network-load-balancerに を指定しますType。

elastic-beanstalk

Elastic Beanstalk 環境にトラフィックをルーティングするには、 elastic-beanstalkに を指定しますType。

s3 ウェブサイト

ウェブサイトエンドポイントとして設定された Amazon S3 バケットにトラフィックをルーティングするには、 s3-websiteに を指定しますType。

リージョン

ウェブサイトエンドポイントとして設定された Amazon S3 バケットにトラフィックをルーティングするには、 のバケットを作成したリージョンを指定しますRegion。他のリソースの場合は、 を省略しますRegion。

値

該当する値を指定します。

値

以下に示すリソース以外のリソースにトラフィックをルーティングするには、 に指定した値に対応する値を指定しますRecordType。たとえば、 Aに を指定した場合はRecordType、に IPv4 形式の IP アドレスを指定しますValue。

cloudfront

cloudfront に を指定した場合はType、CloudFront ディストリビューションの作成時に CloudFront が CloudFront ディストリビューションに割り当てたドメイン名を指定します。たとえば、 ですd111111abcdef8.cloudfront.net。

application-load-balancer

application-load-balancer に を指定した場合はType、ロードバランサーの DNS 名を指定します。例えば、exampleAlb-1283637735.us-east-1.elb.amazonaws.com。

elastic-load-balancer

elastic-load-balancer に を指定した場合はType、ロードバランサーの DNS 名を指定します。たとえばdualstack、 で始まる値を使用しますdualstack.my-load-balancer-1234567890.us-west-2.elb.amazonaws.com。

network-load-balancer

network-load-balancer に を指定した場合はType、ロードバランサーの DNS 名を指定します。例えば、exampleNlb-74f87b114e21682a.elb.us-east-1.amazonaws.com。

elastic-beanstalk

elastic-beanstalk に を指定した場合はType、Elastic Beanstalk 環境のドメイン名を指定します。例えば、example-beanstalk-env-1.eba-ns4qrife.us-east-1.elasticbeanstalk.com。

s3 ウェブサイト

s3-website に を指定した場合はType、Amazon S3 バケットの名前を指定します。例: example.com.s3-website-us-east-1.amazonaws.com。

> **Important**
>
> このトラフィックポリシーに基づいてトラフィックポリシーインスタンスを作成する場合、ここで指定するバケットは、CreateTrafficPolicyInstance リクエストNameで に

指定するドメイン名 (www.example.com など) と一致する必要があります。Value とが一致しNameない場合、Amazon S3 はドメイン名の DNS クエリに応答しません。

ルール定義の構文

トラフィックポリシードキュメントで指定するルール定義には、使用するルーティングポリシーのタイプに応じて、フェイルオーバー、位置情報、地理的近接性、レイテンシー、複数値回答、または重み付けなど、さまざまな構文があります。

トピック

- フェイルオーバールール
- 位置情報ルール
- 地理的近接性ルール
- レイテンシールール
- 複数値回答ルール
- 加重ルール

フェイルオーバールール

詳細については、「Amazon Route 53 デベロッパーガイド」の「DNS フェイルオーバーの設定」を参照してください。

```
{
   "RuleType": "failover",
   "Primary": {
      "EndpointReference | RuleReference": "ID that you assigned to the rule or
 endpoint that this rule routes traffic to",
      "EvaluateTargetHealth": "true" | "false",
      "HealthCheck": "optional health check ID"
   },
   "Secondary": {
      "EndpointReference | RuleReference": "ID that you assigned to the rule or
 endpoint that this rule routes traffic to",
      "EvaluateTargetHealth": "true" | "false",
      "HealthCheck": "optional health check ID"
   }
}
```

フェイルオーバールールを定義するときは、次のオブジェクトを指定します。

RuleType

`failover` を指定します。

プライマリ | セカンダリ

`Primary` オブジェクトで、対応するリソースが利用可能な場合にトラフィックをルーティングするルールまたはエンドポイントの設定を指定します。

`Secondary` オブジェクトで、プライマリリソースが利用できないときにトラフィックをルーティングするルールまたはエンドポイントの設定を指定します。

EndpointReference | RuleReference

トラフィックをエンドポイントにルーティングするか、別のルールにルーティングするか、およびトラフィックポリシードキュメントの他の場所でエンドポイントまたはルールに割り当てた ID。

EvaluateTargetHealth

Amazon Route 53 でエンドポイントの状態を評価し、トラフィックを正常なエンドポイントにのみルーティングするかどうかを示すブール値。詳細については、ChangeResourceRecordSets に関するドキュメントの「EvaluateTargetHealth」を参照してください。

HealthCheck

ヘルスチェックをエンドポイントまたはルールに関連付ける場合は、ヘルスチェックの ID を指定します。詳細については、ChangeResourceRecordSets に関するドキュメントの「HealthCheckId」を参照してください。

位置情報ルール

位置情報ルールを追加するときは、ユーザーの地理的位置に基づいてトラフィックをルーティングするようにトラフィックポリシーを設定します。詳細については、「Amazon Route 53 デベロッパーガイド」の「位置情報ルーティング」を参照してください。

```
{
   "RuleType": "geo",
   "Locations": [
      {
         "EndpointReference | RuleReference": "ID that you assigned to the rule or
 endpoint that this rule routes traffic to",
```

```
         "IsDefault": "true" | "false",
         "Continent": "continent name,
         "Country": "country name,
         "Subdivision": "subdivision name,
         "EvaluateTargetHealth": "true" | "false",
         "HealthCheck": "optional health check ID"
      },
      ...
   ]
}
```

位置情報ルールを定義するときは、次のオブジェクトを指定します。

RuleType

geo を指定します。

ロケーション

トラフィックをルーティングする地理的ロケーションHealthCheckごとに 1 つの値セット (EndpointReference | RuleReference、IsDefaultContinentCountrySubdivision、、EvaluateTargetHealth、、を指定します。

EndpointReference | RuleReference

トラフィックをエンドポイントにルーティングするか、別のルールにルーティングするか、およびトラフィックポリシードキュメントの他の場所でエンドポイントまたはルールに割り当てた ID。

IsDefault

この値のセットがデフォルトの場所を表すかどうかを示すブール値。を地理的位置の CountryCode要素の値*として指定すると、この位置の IsDefault要素の値はTrueデフォルトで に設定され、同じ位置情報ルールの他の地理的位置の IsDefault要素の値Trueとして を指定することはできません。CountryCode 要素の値*として を指定する方法の詳細については、の次のエントリを参照してくださいContinent, Country, Subdivision。

Continent、Country、Subdivision

ルールまたはエンドポイントにトラフィックをルーティングするユーザーの地理的位置を示す値。詳細については、ChangeResourceRecordSets に関するドキュメントの以下の要素の説明を参照してください。

- GeoLocation
- ContinentCode
- CountryCode
- SubdivisionCode

詳細については、「Amazon Route 53 デベロッパーガイド」の「ロケーション」を参照してください。

> **Important**
>
> 位置情報は、IP アドレスを場所にマッピングすることで動作します。ただし、一部の IP アドレスは地理的な場所にマッピングされないため、7 つの大陸すべてをカバーする地理的な場所を作成しても、Route 53 は識別できない場所からいくつかの DNS クエリを受け取ります。の値が である地理的な場所を作成することをお勧めしますCountry*。クエリの 2 つのグループは、このレコードで指定したリソースにルーティングされます。地理的場所を作成していない場所からのクエリと、場所にマッピングされていない IP アドレスからのクエリです。* 地理的場所を作成しない場合、Route 53 はマッピングされていない場所からのクエリに対して「応答なし」レスポンスを返します。

EvaluateTargetHealth

Amazon Route 53 でエンドポイントの状態を評価し、トラフィックを正常なエンドポイントにのみルーティングするかどうかを示すブール値。詳細については、ChangeResourceRecordSets に関するドキュメントのEvaluateTargetHealth」を参照してください。

HealthCheck

ヘルスチェックをエンドポイントまたはルールに関連付ける場合は、ヘルスチェックの ID を指定します。詳細については、ChangeResourceRecordSets に関するドキュメントのHealthCheckId」を参照してください。

地理的近接性ルール

地理的近接性ルールを追加するときは、リソースの地理的位置に基づいてトラフィックをリソースにルーティングするように Amazon Route 53 を設定します。オプションで、バイアスを指定して、特定のエンドポイントまたはルールにより多くのトラフィックをルーティングするか、より少ないトラフィックをルーティングするかを選択することもできます。バイアスを使用して、トラフィックが

エンドポイントまたはルールにルーティングされる地理的リージョンのサイズを拡大または縮小します。詳細については、「Amazon Route 53 デベロッパーガイド」の「地理的近接性ルーティング」を参照してください。

次の例は AWSPolicyFormatVersion 2023-05-09専用です。

```
{
   "RuleType": "geoproximity",
   "GeoproximityLocations": [
      {
         "EndpointReference | RuleReference": "ID that you assigned to the endpoint or
 rule that this rule routes traffic to",
         "Location":{
            "Type": "Region | LocalZone",
            "LocationName": "AWS Region | AWS Local Zone"
         },
         "Bias": "optional value to expand or shrink the geographic region for this
 rule, -99 to 99",
         "EvaluateTargetHealth": "true | false",
         "HealthCheck": "optional health check ID"
      },
      {
         "EndpointReference | RuleReference": "ID that you assigned to the endpoint or
 rule that this rule routes traffic to",
         "Location":{
            "Type": "Coordinate",
            "Latitude": "location south (negative) or north (positive) of the equator,
 -90 to 90 degrees",
            "Longitude": "location west (negative) or east (positive) of the prime
 meridian, -180 to 180 degrees"
         },
         "Bias": "optional value to expand or shrink the geographic region for this
 rule, -99 to 99",
         "EvaluateTargetHealth": "true | false",
         "HealthCheck": "optional health check ID"
      }
   ]
}
```

次の例は、 AWSPolicyFormatVersion 2015-10-01専用です。

```
{
   "RuleType": "geoproximity",
```

```
   "GeoproximityLocations": [
      {
         "EndpointReference | RuleReference": "ID that you assigned to the endpoint or
 rule that this rule routes traffic to",
         "Region": "AWS Region",
         "Bias": "optional value to expand or shrink the geographic region for this
 rule, -99 to 99",
         "EvaluateTargetHealth": "true | false",
         "HealthCheck": "optional health check ID"
      },
      {
         "EndpointReference | RuleReference": "ID that you assigned to the endpoint or
 rule that this rule routes traffic to",
         "Latitude": "location south (negative) or north (positive) of the equator, -90
 to 90 degrees",
         "Longitude": "location west (negative) or east (positive) of the prime
 meridian, -180 to 180 degrees",
         "Bias": "optional value to expand or shrink the geographic region for this
 rule, -99 to 99",
         "EvaluateTargetHealth": "true | false",
         "HealthCheck": "optional health check ID"
      }
   ]
}
```

地理的近接性ルールを定義するときは、次のオブジェクトを指定します。

RuleType

`geoproximity` を指定します。

GeoproximityLocations

トラフィックをルーティングするリソースごとに 1 セットの値を指定します。Location フィールドを指定できます。これは、 の AWS リージョン、ローカルゾーン、緯度と経度をサポートしますAWSPolicyFormatVersion 2023-05-09。 AWS リージョン、または の地理的位置の緯度と経度を指定することもできますAWSPolicyFormatVersion 2015-10-01。

EndpointReference | RuleReference

トラフィックをエンドポイントにルーティングするか、別のルールにルーティングするか、およびトラフィックポリシードキュメントの他の場所でエンドポイントまたはルールに割り当てた ID。

Location (**AWSPolicyFormatVersion 2023-05-09** のみ)

Location フィールドは、 AWS リージョン、ローカルゾーン、緯度と経度を次の形式でサポートします。

ローカルゾーンの場合: `"Location": { "Type": "LocalZone", "LocationName": "aws:route53:us-east-1-atl-1a" }`

リージョンの場合: `"Location": { "Type": "Region", "LocationName": "aws:route53:us-east-1" },`

座標の場合: `"Location": { "Type": "Coordinate", "Latitude": "38.9", "Longitude": "-77.01" },`

有効なリージョンコードのリストについては、ChangeResourceRecordSets に関するドキュメントの「リージョン」を参照してください。

使用可能なローカルゾーンについては、「AWS Local Zones ロケーション」を参照してください。

リージョン (**AWSPolicyFormatVersion 2015-10-01** のみ)

エンドポイントが AWS リソースの場合は、リソースを作成した AWS リージョンを指定します。次の形式を使用します。

`aws:route53:`*`region-code`*

有効なリージョンコードのリストについては、ChangeResourceRecordSets に関するドキュメントの「リージョン」を参照してください。

緯度と経度 (**AWSPolicyFormatVersion 2015-10-01** のみ)

エンドポイントが AWS リソースでない場合は、リソースの場所の緯度と経度を入力します。次の点に注意してください。

- 緯度は南緯 (負) または北緯 (正) で表します。有効な値の範囲は -90 度から 90 度です。
- 経度は西経 (負) または東経 (正) で表します。有効な値の範囲は -180 度から 180 度です。
- 緯度と経度は一部のオンラインマップアプリケーションで入手できます。例えば Google マップでは、その場所の URL に緯度と経度が指定されています。

  https://www.google.com/maps/@47.6086111,-122.3409953,20z
- のように、小数点以下 2 桁までの精度を入力できます`47.61`。精度の高い値を指定すると、Route 53 はエラーを返します。緯度と経度は赤道上で、0.01 度が約 0.69 マイルです。

Bias (バイアス)

近くのエンドポイントからエンドポイントにより多くのトラフィックをルーティングする場合 (正の値) 、またはエンドポイントにより少ないトラフィックをルーティングBiasする場合 (負の値) に、 の値を指定します。有効な値の範囲は -99 ~ 99 です。デフォルト値は 0 です。

> **Important**
>
> の値は、距離に基づく絶対値ではなく、他のリソースの場所に基づく相対値Biasです。その結果、変更の効果を予測することは簡単ではありません。例えば、リソースの場所に応じて、バイアスを から 10 に変更15すると、ニューヨーク市大都市圏からの大量のトラフィックを加算または減算する違いがわかります。バイアスを小規模に変更して結果を評価してから、必要に応じてさらに変更を行うことをお勧めします。

EvaluateTargetHealth

Route 53 でエンドポイントの状態を評価し、トラフィックを正常なエンドポイントにのみルーティングするかどうかを示すブール値。詳細については、ChangeResourceRecordSets に関するドキュメントのEvaluateTargetHealth」を参照してください。

HealthCheck

ヘルスチェックをエンドポイントまたはルールに関連付ける場合は、ヘルスチェックの ID を指定します。詳細については、ChangeResourceRecordSets に関するドキュメントのHealthCheckId」を参照してください。

レイテンシールール

レイテンシールールを追加するときは、ユーザーと、ELB ロードバランサーや Amazon S3 バケットなどの AWS リソースを作成した AWS リージョン間のレイテンシー (遅延時間) に基づいてトラフィックをルーティングするようにトラフィックポリシーを設定します。詳細については、「Amazon Route 53 デベロッパーガイド」の「レイテンシールーティング」を参照してください。

```
{
   "RuleType": "latency",
   "Regions": [
      {
```

```
        "EndpointReference | RuleReference": "ID that you assigned to the rule or
 endpoint that this rule routes traffic to",
        "Region": "AWS region that you want to route traffic to",
        "EvaluateTargetHealth": "true" | "false",
        "HealthCheck": "optional health check ID"
      },
      ...
   ]
}
```

レイテンシールールを定義するときは、次のオブジェクトを指定します。

RuleType

`latency` を指定します。

リージョン

トラフィックをルーティングするリージョンHealthCheckごとに Region1 つの値セット (EndpointReference | RuleReference、EvaluateTargetHealth、、) を指定します。

EndpointReference | RuleReference

トラフィックをエンドポイントにルーティングするか、別のルールにルーティングするか、およびトラフィックポリシードキュメントの他の場所でエンドポイントまたはルールに割り当てた ID。

リージョン

リソースを作成したリージョンの AWS リージョンコード。有効なリージョンコードのリストについては、ChangeResourceRecordSets に関するドキュメントの「リージョン」を参照してください。

EvaluateTargetHealth

Amazon Route 53 でエンドポイントの状態を評価し、トラフィックを正常なエンドポイントにのみルーティングするかどうかを示すブール値。詳細については、ChangeResourceRecordSets に関するドキュメントのEvaluateTargetHealth」を参照してください。

HealthCheck

ヘルスチェックをエンドポイントまたはルールに関連付ける場合は、ヘルスチェックの ID を指定します。詳細については、ChangeResourceRecordSets に関するドキュメントのHealthCheckId」を参照してください。

複数値回答ルール

複数値回答ルールを追加するときは、トラフィックポリシーを設定して、トラフィックを正常なリソースにほぼランダムにルーティングします。Amazon Route 53 は最大 8 つの正常なレコードで DNS クエリに応答します。8 つ以下の正常なレコードがある場合、Route 53 はすべての正常なレコードですべての DNS クエリに応答します。詳細については、「MultiValueAnswer」を参照してください。

```
{
   "RuleType": "multivalue",
   "Items": [
      {
         "EndpointReference": "ID that you assigned to the endpoint that this rule
 routes traffic to",
         "HealthCheck": "optional health check ID"
      },
      ...
   ]
}
```

複数値の回答ルールを定義するときは、次のオブジェクトを指定します。

RuleType

`multivalue` を指定します。

項目

トラフィックをルーティングする複数値の回答ルールまたはエンドポイントごとに、値のセット (`EndpointReference` と `HealthCheck`) を 1 つ指定します。

EndpointReference

トラフィックポリシードキュメントの他の場所でエンドポイントに割り当てた ID。

HealthCheck

ヘルスチェックをエンドポイントに関連付ける場合は、ヘルスチェックの ID を指定します。詳細については、「HealthCheckId」を参照してください。

加重ルール

加重ルールを追加するときは、指定した比率に基づいてトラフィックをルーティングするようにトラフィックポリシーを設定します。たとえば、重みとして 4、5、5、6 (合計 = 20) を指定できます。その結果、トラフィックの 4/20 は平均して最初のエンドポイントまたはルールにルーティングされ、5/20 は 2 番目と 3 番目のエンドポイントまたはルールの両方にルーティングされ、6/20 は最後のエンドポイントまたはルールにルーティングされます。詳細については、Amazon Route 53 デベロッパーガイドの加重ルーティングを参照してください。

```
{
   "RuleType": "weighted",
   "Items": [
      {
         "EndpointReference | RuleReference": "ID that you assigned to the rule or
 endpoint that this rule routes traffic to",
         "Weight": "value between 0 and 255",
         "EvaluateTargetHealth": "true" | "false",
         "HealthCheck": "optional health check ID"
      },
      ...
   ]
}
```

加重ルールを定義するときは、次のオブジェクトを指定します。

RuleType

weighted を指定します。

項目

トラフィックをルーティングする加重ルールまたはエンドポイントHealthCheckごとに 1 つの値セット (EndpointReference | RuleReferenceWeight、、EvaluateTargetHealth、) を指定します。

EndpointReference | RuleReference

トラフィックをエンドポイントにルーティングするか、別のルールにルーティングするか、およびトラフィックポリシードキュメントの他の場所でエンドポイントまたはルールに割り当てた ID。

Weight

対応するエンドポイントまたはルールにルーティングされるトラフィックの割合を決定する 0 ~ 255 の値。詳細については、ChangeResourceRecordSets に関するドキュメントの「重み」を参照してください。

EvaluateTargetHealth

Amazon Route 53 でエンドポイントの状態を評価し、トラフィックを正常なエンドポイントにのみルーティングするかどうかを示すブール値。詳細については、ChangeResourceRecordSets に関するドキュメントのEvaluateTargetHealth」を参照してください。

HealthCheck

ヘルスチェックをエンドポイントまたはルールに関連付ける場合は、ヘルスチェックの ID を指定します。詳細については、ChangeResourceRecordSets に関するドキュメントのHealthCheckId」を参照してください。

例

次の例は、フェイルオーバー、位置情報、地理的近接性、レイテンシー、加重ルールを使用する方法と、同じトラフィックポリシーで複数のタイプのルールを使用する方法を示しています。

トピック

- フェイルオーバーの例
- 位置情報の例
- 地理的近接性の例
- レイテンシーの例
- 加重例
- フェイルオーバー、レイテンシー、位置情報ルールの例

フェイルオーバーの例

```
{
   "AWSPolicyFormatVersion":"2015-10-01",
   "RecordType":"A",
   "StartRule":"site_switch",
   "Endpoints":{
      "my_elb":{
```

```
         "Type":"elastic-load-balancer",
         "Value":"elb-111111.us-east-1.elb.amazonaws.com"
      },
      "site_down_banner":{
         "Type":"s3-website",
         "Region":"us-east-1",
         "Value":"www.example.com"
      }
   },
   "Rules":{
      "site_switch":{
         "RuleType":"failover",
         "Primary":{
            "EndpointReference":"my_elb"
         },
         "Secondary":{
            "EndpointReference":"site_down_banner"
         }
      }
   }
}
```

位置情報の例

```
{
  "AWSPolicyFormatVersion":"2015-10-01",
  "RecordType":"A",
  "StartRule":"geo_dest",
  "Endpoints":{
    "english":{
      "Type":"value",
      "Value":"192.0.2.1"
    },
    "french":{
      "Type":"value",
      "Value":"192.0.2.2"
    },
    "german":{
      "Type":"value",
      "Value":"192.0.2.3"
    }
  },
  "Rules":{
```

```
    "geo_dest":{
      "RuleType":"geo",
      "Locations":[
        {
          "EndpointReference":"english",
          "Country":"*",
          "HealthCheck":"11111111-1111-1111-1111-111111111111"
        },
        {
          "EndpointReference":"french",
          "Country":"FR",
          "IsDefault":false,
          "HealthCheck":"22222222-2222-2222-2222-222222222222"
        },
        {
          "EndpointReference":"french",
          "Country":"BE",
          "IsDefault":false,
          "HealthCheck":"22222222-2222-2222-2222-222222222222"
        },
        {
          "EndpointReference":"german",
          "Country":"DE",
          "IsDefault":false,
          "HealthCheck":"33333333-3333-3333-3333-333333333333"
        }
      ]
    }
  }
}
```

地理的近接性の例

```
{
  "AWSPolicyFormatVersion":"2015-10-01",
  "RecordType":"A",
  "StartRule":"geoprox-rule",
  "Endpoints":{
    "aws-us-west-1-region":{
      "Type":"elastic-load-balancer",
      "Value":"elb-123456.us-east-1.elb.amazonaws.com"
    },
    "london-data-center":{
```

```
      "Type":"value",
      "Value":"192.0.2.1"
    }
  },
  "Rules":{
    "geoprox-rule":{
      "RuleType": "geoproximity",
      "GeoproximityLocations": [
        {
          "EndpointReference": "aws-us-west-1-region",
          "Region": "aws:route53:us-west-1",
          "Bias": "10",
          "HealthCheck": "11111111-1111-1111-1111-111111111111"
        },
        {
          "EndpointReference": "london-data-center",
          "Latitude": "51.50",
          "Longitude": "-0.16",
          "Bias": "0",
          "HealthCheck": "22222222-2222-2222-2222-222222222222"
        }
      ]
    }
  }
}
```

```
{
  "AWSPolicyFormatVersion":"2023-05-09",
  "RecordType":"A",
  "StartRule":"geoprox-rule",
  "Endpoints":{
    "aws-us-west-1-region":{
      "Type":"elastic-load-balancer",
      "Value":"elb-123456.us-west-1.elb.amazonaws.com"
    },
    "aws-us-east-1-atl-local-zone":{
      "Type":"elastic-load-balancer",
      "Value":"elb-123456.us-east-1.elb.amazonaws.com"
    },
    "london-data-center":{
      "Type":"value",
      "Value":"192.0.2.1"
    }
```

```
  },
  "Rules":{
    "geoprox-rule":{
      "RuleType": "geoproximity",
      "GeoproximityLocations": [
        {
          "EndpointReference": "aws-us-west-1-region",
          "Location": {
            "Type": "Region",
            "LocationName": "aws:route53:us-west-1"
          },
          "Bias": "-10",
          "HealthCheck": "11111111-1111-1111-1111-111111111111"
        },
        {
          "EndpointReference": "aws-us-east-1-atl-local-zone",
          "Location": {
            "Type": "LocalZone",
            "LocationName": "aws:route53:us-east-1-atl-1a"
          },
          "Bias": "10",
          "HealthCheck": "22222222-2222-2222-2222-222222222222"
        },
        {
          "EndpointReference": "london-data-center",
          "Location": {
            "Type": "Coordinate",
            "Latitude": "51.50",
            "Longitude": "-0.16"
          },
          "Bias": "0",
          "HealthCheck": "33333333-3333-3333-3333-333333333333"
        }
      ]
    }
  }
}
```

レイテンシーの例

```
{
  "AWSPolicyFormatVersion":"2015-10-01",
  "RecordType":"A",
```

```
  "StartRule":"region_selector",
  "Endpoints":{
    "us_lb":{
      "Type":"elastic-load-balancer",
      "Value":"elb-123456.us-east-1.elb.amazonaws.com"
    },
    "europe_lb":{
      "Type":"elastic-load-balancer",
      "Value":"elb-654321.eu-west-1.elb.amazonaws.com"
    }
  },
  "Rules":{
    "region_selector":{
      "RuleType":"latency",
      "Regions":[
        {
          "Region":"us-east-1",
          "EndpointReference":"us_lb"
        },
        {
          "Region":"eu-west-1",
          "EndpointReference":"europe_lb"
        }
      ]
    }
  }
}
```

加重例

```
{
  "AWSPolicyFormatVersion":"2015-10-01",
  "RecordType":"A",
  "StartRule":"round_robin",
  "Endpoints":{
    "srv1":{
      "Type":"value",
      "Value":"192.0.2.1"
    },
    "srv2":{
      "Type":"value",
      "Value":"192.0.2.2"
    },
```

```
    "srv3":{
      "Type":"value",
      "Value":"192.0.2.3"
    }
  },
  "Rules":{
    "round_robin":{
      "RuleType":"weighted",
      "Items":[
        {
          "EndpointReference":"srv1",
          "Weight":"3",
          "HealthCheck":"11111111-1111-1111-1111-111111111111"
        },
        {
          "EndpointReference":"srv2",
          "Weight":"1",
          "HealthCheck":"22222222-2222-2222-2222-222222222222"
        },
        {
          "EndpointReference":"srv3",
          "Weight":"1",
          "HealthCheck":"33333333-3333-3333-3333-333333333333"
        }
      ]
    }
  }
}
```

フェイルオーバー、レイテンシー、位置情報ルールの例

```
{
  "AWSPolicyFormatVersion":"2015-10-01",
  "RecordType":"A",
  "StartRule":"geo_restriction",
  "Endpoints":{
    "east_coast_lb1":{
      "Type":"elastic-load-balancer",
      "Value":"elb-111111.us-east-1.elb.amazonaws.com"
    },
    "east_coast_lb2":{
      "Type":"elastic-load-balancer",
      "Value":"elb-222222.us-east-1.elb.amazonaws.com"
```

```
    },
    "west_coast_lb1":{
      "Type":"elastic-load-balancer",
      "Value":"elb-111111.us-west-1.elb.amazonaws.com"
    },
    "west_coast_lb2":{
      "Type":"elastic-load-balancer",
      "Value":"elb-222222.us-west-1.elb.amazonaws.com"
    },
    "denied_message":{
      "Type":"s3-website",
      "Region":"us-east-1",
      "Value":"video.example.com"
    }
  },
  "Rules":{
    "geo_restriction":{
      "RuleType":"geo",
      "Locations":[
        {
          "EndpointReference":"denied_message",
          "IsDefault":true
        },
        {
          "RuleReference":"region_selector",
          "Country":"US"
        }
      ]
    },
    "region_selector":{
      "RuleType":"latency",
      "Regions":[
        {
          "Region":"us-east-1",
          "RuleReference":"east_coast_region"
        },
        {
          "Region":"us-west-1",
          "RuleReference":"west_coast_region"
        }
      ]
    },
    "east_coast_region":{
      "RuleType":"failover",
```

```
      "Primary":{
        "EndpointReference":"east_coast_lb1"
      },
      "Secondary":{
        "EndpointReference":"east_coast_lb2"
      }
    },
    "west_coast_region":{
      "RuleType":"failover",
      "Primary":{
        "EndpointReference":"west_coast_lb1"
      },
      "Secondary":{
        "EndpointReference":"west_coast_lb2"
      }
    }
  }
}
```

Route 53 VPC Resolver とは

Route 53 VPC Resolver は、パブリックレコード、Amazon VPC 固有の DNS 名、Amazon Route 53 プライベートホストゾーンの AWS リソースからの DNS クエリに再帰的に応答し、デフォルトですべての VPCs で使用できます。

> **Note**
>
> Route 53 VPC Resolver は以前は Route 53 Resolver と呼ばれていましたが、Route 53 Global Resolver の導入時に名前が変更されました。

Amazon VPC は、VPC+2 IP アドレスで VPC リゾルバーに接続します。この VPC+2 アドレスは、アベイラビリティーゾーン内の VPC リゾルバーに接続します。

VPC リゾルバーは、次の DNS クエリに自動的に応答します。

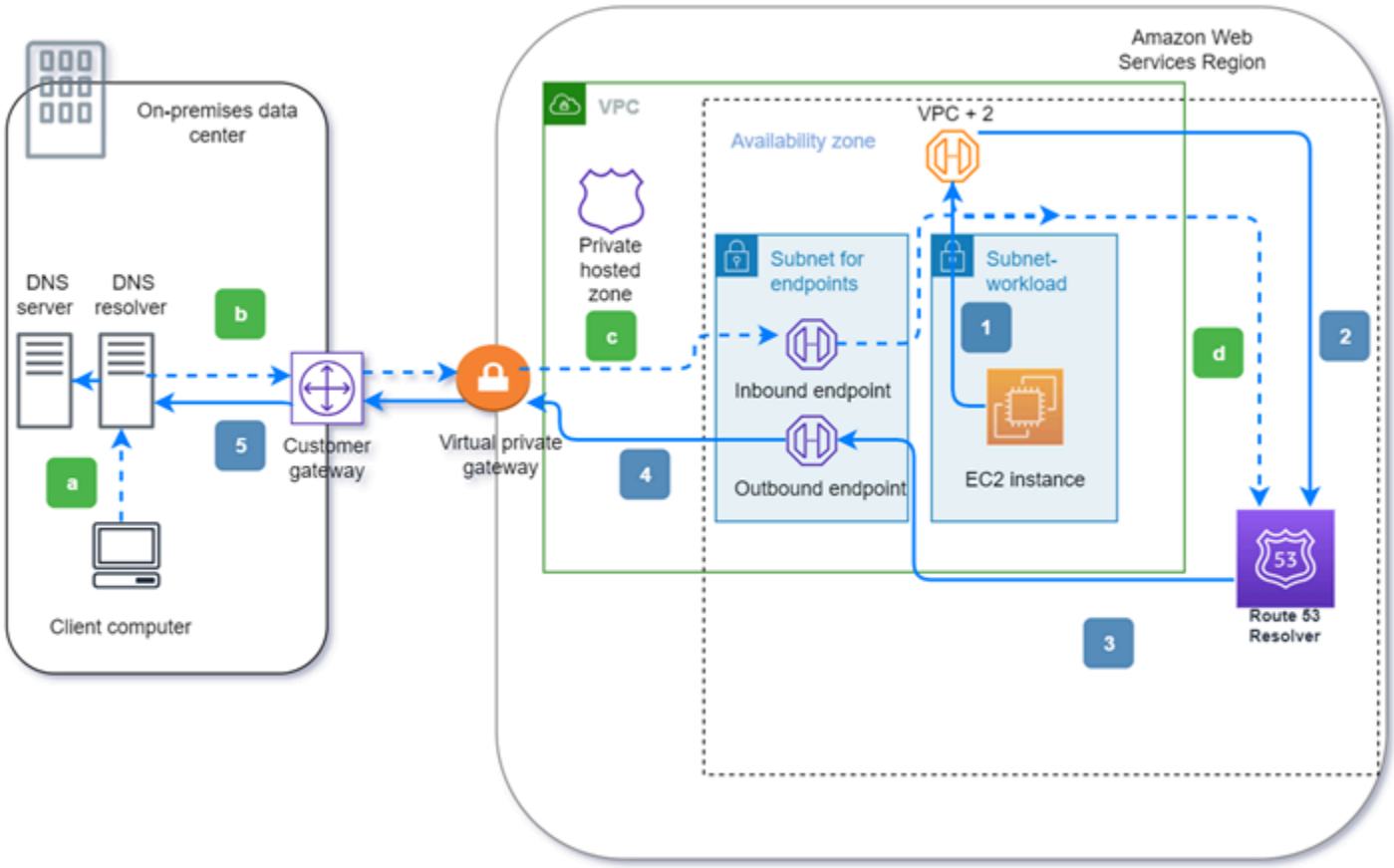
- EC2 インスタンスのローカル VPC ドメイン名 (例えば、ec2-192-0-2-44.compute-1.amazonaws.com)
- プライベートホストゾーンのレコード (例えば、acme.example.com)。
- パブリックドメイン名の場合、VPC Resolver はインターネット上のパブリックネームサーバーに対して再帰的なルックアップを実行します。

VPC とオンプレミスリソースの両方を利用するワークロードがある場合は、オンプレミスでホストされている DNS レコードを解決する必要もあります。同様に、これらのオンプレミスリソースは、ホストされている名前を解決する必要がある場合があります AWS。Resolver エンドポイントと条件付き転送ルールにより、オンプレミスリソースと VPC 間の DNS クエリを解決して、VPN または Direct Connect (DX) 経由でハイブリッドクラウド環境を構築できます。具体的には次のとおりです。

- インバウンド Resolver エンドポイントを使用すると、VPC に、オンプレミスネットワークまたは別の VPC から DNS クエリが可能になります。
- アウトバウンド Resolver エンドポイントを使用すると、VPC から、オンプレミスネットワークまたは別の VPC に DNS クエリが可能になります。

- Resolver ルールを使用すると、ドメイン名ごとに転送ルールを 1 つ作成し、VPC からオンプレミスの DNS リゾルバーへの DNS クエリ、およびオンプレミスから VPC への DNS クエリを転送するドメイン名を指定できます。ルールは VPC に直接適用され、複数のアカウントで共有できます。

次の図は、Resolver エンドポイントを使用したハイブリッド DNS 解決を示しています。この図は、アベイラビリティーゾーンを 1 つだけ表示するように簡略化されていることに注意してください。



この図は、以下のステップを示しています。

アウトバウンド (実線矢印 1 ~ 5):

1. Amazon EC2 インスタンスは internal.example.com というドメインへの DNS クエリを解決する必要があります。権限のある DNS サーバーは、オンプレミスデータセンターで管理されています。この DNS クエリは、VPC Resolver に接続する VPC の VPC+2 に送信されます。
2. VPC リゾルバー転送ルールは、オンプレミスデータセンターの internal.example.com にクエリを転送するように設定されています。
3. クエリはアウトバウンドエンドポイントに転送されます。

4. アウトバウンドエンドポイントは、 AWS とデータセンター間のプライベート接続を介してクエリをオンプレミス DNS リゾルバーに転送します。接続は、仮想プライベートゲートウェイとして表される AWS Site-to-Site VPN Direct Connect または のいずれかになります。
5. オンプレミス DNS リゾルバーは internal.example.com の DNS クエリを解決し、同じパスを逆にして Amazon EC2 インスタンスに回答を返します。

インバウンド (破線矢印 a ~ d):

a. オンプレミスデータセンターのクライアントは、ドメイン dev.example.com の AWS リソースに DNS クエリを解決する必要があります。クエリをオンプレミスの DNS リゾルバーに送信します。
b. オンプレミスの DNS リゾルバーには、dev.example.com へのクエリをインバウンドエンドポイントに向ける転送ルールがあります。
c. クエリは、仮想ゲートウェイとして AWS Site-to-Site VPN示される Direct Connect や などのプライベート接続を介してインバウンドエンドポイントに到着します。
d. インバウンドエンドポイントはクエリを VPC Resolver に送信し、VPC Resolver は dev.example.com の DNS クエリを解決し、同じパスを逆にしてクライアントに回答を返します。

トピック

- VPC とネットワークの間における DNS クエリの解決
- Route 53 VPC Resolver の可用性とスケーリング
- Route 53 VPC Resolver の開始方法
- VPC へのインバウンド DNS クエリの転送
- ネットワークへのアウトバウンド DNS クエリの転送
- リゾルバーの委任ルールのチュートリアル
- Amazon Route 53 での DNSSEC 検証の有効化

VPC とネットワークの間における DNS クエリの解決

VPC リゾルバーには、オンプレミス環境との間で送受信される DNS クエリに応答するように設定したエンドポイントが含まれています。

> **Note**
>
> プライベート DNS クエリでは、オンプレミスまたは他の VPC DNS サーバーから任意の VPC CIDR + 2 アドレスへの転送はサポートされていないため、結果が不安定になる可能性があります。代わりに、Resolver のインバウンドエンドポイントの使用をお勧めします。

転送ルールを設定することで、ネットワーク上の VPC リゾルバーと DNS リゾルバー間で DNS 解決を統合することもできます。ネットワークには、VPC から到達可能なすべてのネットワークを含めることができます。その例を次に示します。

- VPC 自体
- 別のピア接続 VPC
- 、VPN Direct Connect、またはネットワークアドレス変換 (NAT) ゲートウェイ AWS で接続されているオンプレミスネットワーク

クエリの転送を開始する前に、Route 53 Resolver のインバウンドおよび (または) アウトバウンドエンドポイントを、接続された VPC 内に作成します。これらのエンドポイントは、インバウンドまたはアウトバウンドクエリのパスを提供します。

インバウンドエンドポイント: ネットワーク上の DNS リゾルバーは、このエンドポイントを介して DNS クエリを Route 53 VPC Resolver に転送できます

インバウンドエンドポイントには、IP アドレスに転送するデフォルトのインバウンドエンドポイントと、Route 53 プライベートホストゾーンでホストされているサブドメインの権限を Route 53 VPC リゾルバーに委任する委任インバウンドエンドポイントの 2 種類があります。インバウンドエンドポイントを使用すると、DNS リゾルバーは、Route 53 プライベートホストゾーンの EC2 インスタンスやレコードなどの AWS リソースのドメイン名を簡単に解決できます。詳細については、「ネットワーク上の DNS リゾルバーが DNS クエリを Resolver エンドポイントに転送する方法」を参照してください。

アウトバウンドエンドポイント: VPC Resolver は、このエンドポイントを介してネットワーク上のリゾルバーにクエリを条件付きで転送します

クエリを選択して転送するには、Route 53 Resolver ルールを作成して、転送するDNS クエリのドメイン名 (example.com など)、および (クエリの転送先である) ネットワーク上の DNS リゾルバーの IP アドレスを指定します。クエリが (example.com と acme.example.com など) 複数のルールと一致する場合、VPC Resolver では最も具体的なルール (acme.example.com) が選択さ

れ、そのルールで指定している IP アドレスに対しクエリが転送されます。ルールには、転送、システム、委任の 3 種類があります。詳細については、「Resolver エンドポイントが VPCs からネットワークに DNS クエリを転送する方法」を参照してください。

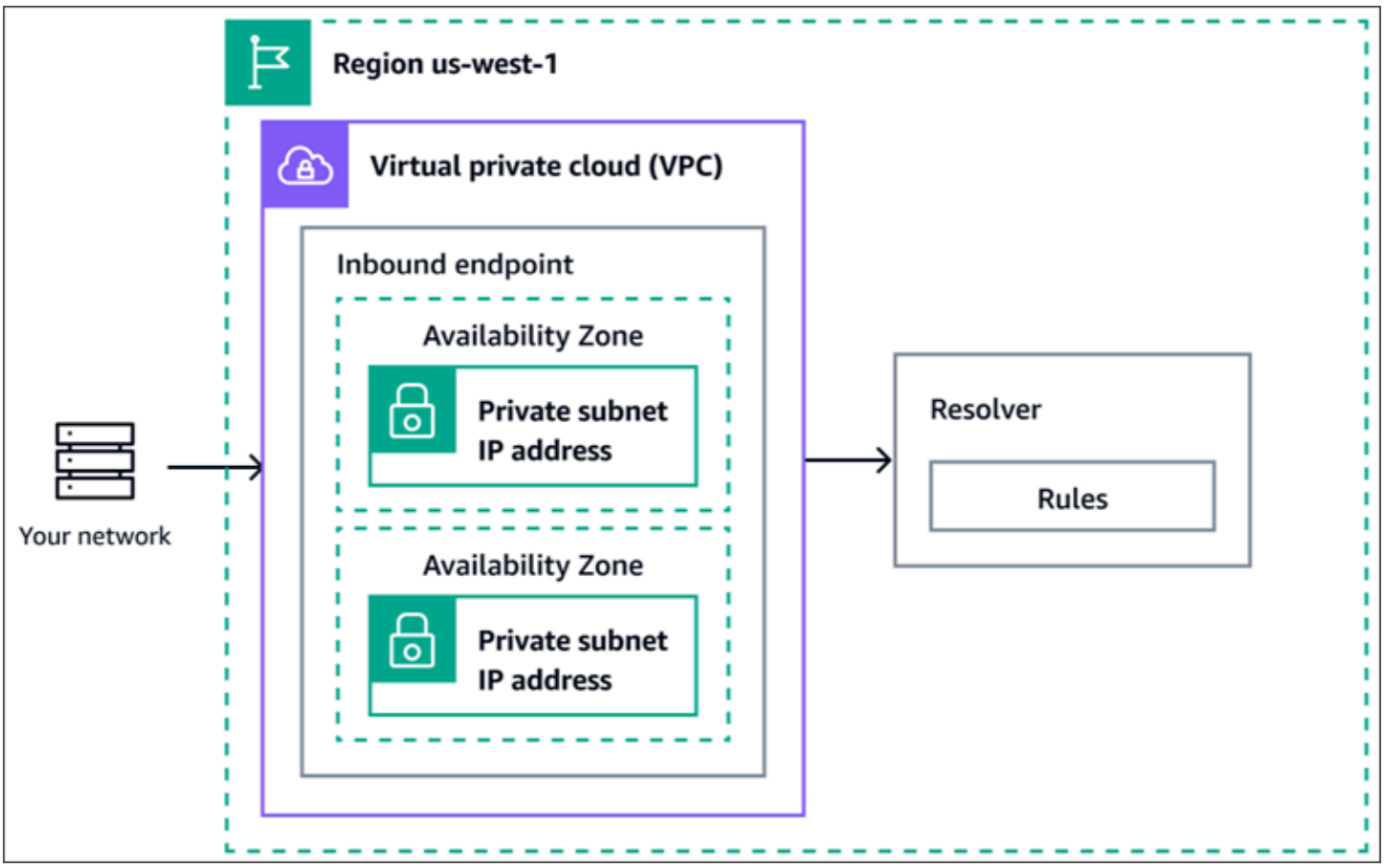
Amazon VPC と同様に、VPC Resolver はリージョン別です。VPCs がある各リージョンでは、VPCs からネットワークにクエリを転送するか (アウトバウンドクエリ) 、ネットワークから VPCs (インバウンドクエリ) 、またはその両方を転送するかを選択できます。

所有していない VPC で Resolver エンドポイントを作成することはできません。VPC 所有者だけが、インバウンドエンドポイントなどの VPC レベルのリソースを作成できます。

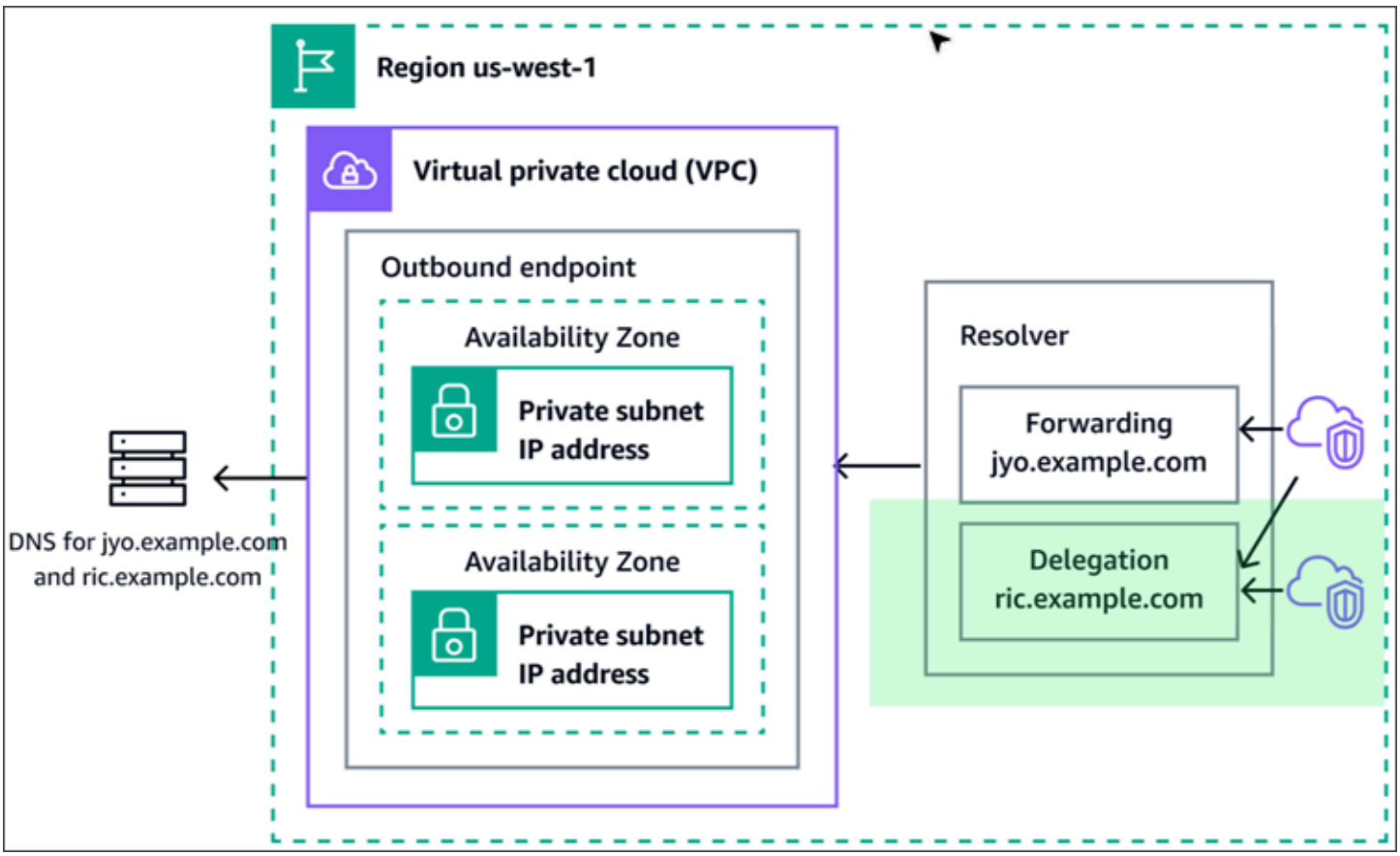
> **Note**
>
> Resolver エンドポイントを作成する際、インスタンスのテナンシー属性が `dedicated` に設定されている VPC を指定することはできません。詳細については、「」を参照してください

インバウンド転送またはアウトバウンド転送を使用するには、VPC に Resolver のエンドポイントを作成します。エンドポイントの定義の一環として、インバウンド DNS クエリを転送する IP アドレス、または DNS 委任、あるいはアウトバウンドクエリの発信元となる IP アドレスを指定します。指定した IP アドレスと委任ごとに、VPC Resolver は VPC Elastic Network Interface を自動的に作成します。

次の図は、ネットワーク上の DNS リゾルバーから Route 53 Resolver エンドポイントへの DNS クエリのパスを示しています。



次の図は、いずれかの VPC の EC2 インスタンスからネットワーク上の DNS リゾルバーへの DNS クエリのパスを示しています。jyo.example.com ドメインは転送ルールを使用しますが、ric.example.com サブドメインは転送権限を VPC Resolver に委任しています。



VPC ネットワークインターフェイスの概要については、Amazon VPC ユーザーガイドの「Elastic Network Interface」を参照してください。

トピック

- ネットワーク上の DNS リゾルバーが DNS クエリを Resolver エンドポイントに転送する方法
- Resolver エンドポイントが VPCs からネットワークに DNS クエリを転送する方法
- インバウンドエンドポイントとアウトバウンドエンドポイントを作成する際の考慮事項

ネットワーク上の DNS リゾルバーが DNS クエリを Resolver エンドポイントに転送する方法

ネットワークから Route 53 VPC Resolver に DNS クエリを転送するには、 AWS リージョンにインバウンドエンドポイントを作成します。インバウンドエンドポイントには、デフォルトと委任の 2 つのカテゴリがあります。

デフォルトのインバウンドエンドポイントを作成するステップ

1. VPC にデフォルトの Resolver インバウンドエンドポイントを作成し、ネットワーク上のリゾルバーが DNS クエリを転送する IP アドレスと、ポート 53 での TCP および UDP アクセスを許可するインバウンドルールを含む VPC セキュリティグループを指定します。手順については、「インバウンド転送の設定」を参照してください。

   インバウンドエンドポイントに指定した IP アドレスごとに、VPC Resolver はインバウンドエンドポイントを作成した VPC に VPC Elastic Network Interface を作成します。
2. 該当するドメイン名の DNS クエリを、インバウンドエンドポイントで指定した IP アドレスに転送するように、ネットワークのリゾルバーを設定します。詳細については、「インバウンドエンドポイントとアウトバウンドエンドポイントを作成する際の考慮事項」を参照してください。

VPC Resolver がデフォルトのインバウンドエンドポイントを介してネットワークで発生する DNS クエリを解決する方法は次のとおりです。

1. ウェブブラウザまたはネットワーク上の別のアプリケーションは、VPC Resolver に転送したドメイン名の DNS クエリを送信します。
2. ネットワークのリゾルバーは、このクエリをインバウンドエンドポイントの IP アドレスに転送します。
3. インバウンドエンドポイントは、クエリを VPC Resolver に転送します。
4. VPC Resolver は、内部的に、またはパブリックネームサーバーに対して再帰的な検索を実行して、DNS クエリ内のドメイン名に該当する値を取得します。
5. VPC Resolver は、インバウンドエンドポイントに値を返します。
6. インバウンドエンドポイントは、この値をお客様環境上のリゾルバーに返します。
7. お客様環境上のリゾルバーは、この値をアプリケーションに返します。
8. VPC Resolver によって返された値を使用して、アプリケーションは Amazon S3 バケット内のオブジェクトのリクエストなど、リクエストを送信します。

委任インバウンドエンドポイントを作成するステップ

1. VPC に委任リゾルバーのインバウンドエンドポイントを作成します。手順については、「インバウンド転送の設定」を参照してください。

   インバウンドエンドポイントに指定した IP アドレスごとに、VPC Resolver はインバウンドエンドポイントを作成した VPC に VPC Elastic Network Interface を作成します。

2. 該当するドメイン名の DNS クエリを VPC Resolver に委任するようにネットワーク上のリゾルバーを設定します。グルーレコードには、インバウンドエンドポイントの IP アドレスを入力する必要があります。詳細については、「インバウンドエンドポイントとアウトバウンドエンドポイントを作成する際の考慮事項」を参照してください。

VPC Resolver が委任インバウンドエンドポイントを介してネットワークで発生する DNS クエリを解決する方法は次のとおりです。

1. 前提条件として、プライベートホストゾーンでホストされているサブドメインをオンプレミスから委任する必要があります。インバウンド委任エンドポイントを介してサブドメインを委任するため、委任されるサブドメインのグルーレコードとしてインバウンドエンドポイント IP アドレスを使用します。

> **Note**
>
> DNS クエリが解決可能であることを確認するために、グルーレコードを含める必要がある場合もあります。親ドメインと同じゾーンにあるネームサーバーにサブドメインを委任する場合は、グルーレコードが必要です。

2. ウェブブラウザまたはネットワーク上の別のアプリケーションは、VPC リゾルバーに委任したドメイン名の DNS クエリを送信します。
3. ネットワークのリゾルバーは、このクエリをインバウンドエンドポイントの IP アドレスに転送します。
4. インバウンドエンドポイントは、クエリを VPC Resolver に委任します。
5. VPC Resolver は、プライベートホストゾーンからインバウンドエンドポイントにアドレスを AWS リソースに返します。
6. インバウンドエンドポイントは、この値をお客様環境上のリゾルバーに返します。
7. お客様環境上のリゾルバーは、この値をアプリケーションに返します。
8. VPC Resolver によって返された値を使用して、アプリケーションは Amazon S3 バケット内のオブジェクトのリクエストなど、リクエストを送信します。

インバウンドエンドポイントを作成しても VPC Resolver の動作は変わりません。 AWS ネットワーク外の場所から VPC Resolver へのパスを提供するだけです。

Resolver エンドポイントが VPCs からネットワークに DNS クエリを転送する方法

AWS リージョンの 1 つ以上の VPCs の EC2 インスタンスからネットワークに DNS クエリを転送する場合は、次の手順を実行します。

1. VPC に Resolver アウトバウンドエンドポイントを作成し、いくつかの値を指定します。
   - お客様環境上のリゾルバーに向かう途中で DNS クエリが通過する VPC。
   - ポート 53 (またはネットワーク上の DNS クエリに使用しているポート) で TCP および UDP アクセスを許可するアウトバウンドルールを含む VPC セキュリティグループ

   アウトバウンドエンドポイントに指定した IP アドレスごとに、VPC Resolver は指定した VPC に Amazon VPC Elastic Network Interface を作成します。詳細については、「インバウンドエンドポイントとアウトバウンドエンドポイントを作成する際の考慮事項」を参照してください。
2. VPC Resolver に転送する DNS クエリのドメイン名を指定するルール、または VPC Resolver がネットワーク上のリゾルバーに転送するルールを 1 つ以上作成します。また、転送ルールでリゾルバーの IP アドレスも指定します。詳細については、「ネットワークに転送するクエリをルールでコントロールする」を参照してください。
3. 各ルールを、ネットワークに DNS クエリを転送する VPC に関連付けます。

ネットワークに転送するクエリをルールでコントロールする

ルールは、Resolver エンドポイントがネットワーク上の DNS リゾルバーに転送する DNS クエリと、VPC Resolver が応答するクエリを制御します。

ルールは 2 通りの方法で分類できます。1 つの方法では、ルールの作成元で分類します。

- 自動定義ルール – VPC Resolver は自動定義ルールを自動的に作成し、ルールを VPCs。これらのルールのほとんどは、VPC Resolver がクエリに応答する AWS特定のドメイン名に適用されます。詳細については、「VPC Resolver が自動定義されたシステムルールを作成するドメイン名」を参照してください。
- カスタムルール – カスタムルールは、ユーザーが作成して VPC に関連付けます。現在、条件付き転送ルール (転送ルールとも呼ばれます) と委任ルールという 2 種類のカスタムルールを作成できます。転送ルールにより、VPC リゾルバーVPCs からネットワーク上の DNS リゾルバーの IP アドレスに DNS クエリを転送します。

自動定義ルールと同じドメインの転送ルールを作成すると、VPC Resolver は転送ルールの設定に基づいて、そのドメイン名のクエリをネットワーク上の DNS リゾルバーに転送します。

委任ルールは、ネットワーク上のリゾルバーに応答して NS レコードに一致する委任ルール内の委任レコードを使用して DNS クエリを転送します。

ルールを分類するもう 1 つの方法は、以下の機能に基づきます。

- 条件付き転送ルール – 指定されたドメイン名の DNS クエリをネットワーク上の DNS リゾルバーに転送する場合は、条件付き転送ルール (転送ルール) を作成します。
- システムルール – システムルールにより、VPC Resolver は転送ルールで定義されている動作を選択的に上書きします。システムルールを作成すると、VPC リゾルバーは、ネットワーク上の DNS リゾルバーによって解決される、指定されたサブドメインの DNS クエリを解決します。

  デフォルトでは、転送ルールはドメイン名とそのすべてのサブドメインに適用されます。ドメインのクエリをネットワークのリゾルバーに転送する際に、一部のサブドメインのクエリを除外する場合は、これらのサブドメインに対してシステムルールを作成します。例えば、example.com の転送ルールを作成する際に acme.example.com のクエリを転送しない場合は、システムルールを作成し、ドメイン名として acme.example.com を指定します。
- 再帰ルール – VPC Resolver は、Internet Resolver という名前の再帰ルールを自動的に作成します。このルールにより、Route 53 VPC Resolver は、カスタムルールを作成せず、VPC Resolver が自動定義ルールを作成しなかったドメイン名の再帰的なリゾルバーとして機能します。この動作を上書きする方法については、このトピックで後ほど説明する「すべてのクエリをネットワークに転送する」を参照してください。

特定のドメイン名 (お客様またはほとんどの AWS ドメイン名) 、パブリック AWS ドメイン名、またはすべてのドメイン名に適用されるカスタムルールを作成できます。

特定のドメイン名のクエリをネットワークに転送する

特定のドメイン名 (example.com など) のクエリをネットワークに転送するには、ルールを作成してそのドメイン名を指定します。転送ルールでは、クエリを転送するネットワーク上の DNS リゾルバーの IP アドレスを指定するか、委任ルールでは、権限をオンプレミスリゾルバーに委任する委任レコードを作成します。次に、各ルールを、ネットワークに DNS クエリを転送する VPC に関連付けます。例えば、example.com、example.org、example.net に個別のルールを作成できます。その後、任意の組み合わせで AWS リージョンの VPCs にルールを関連付けることができます。

amazonaws.com のクエリをネットワークに転送する

ドメイン名 amazonaws.com は、EC2 インスタンスや S3 バケットなどの AWS リソースのパブリックドメイン名です。amazonaws.com のクエリをネットワークに転送する場合は、ルールを作成し、ドメイン名として amazonaws.com を指定し、使用する方法に応じて、ルールタイプとして転送または委任を指定します。

> **Note**
>
> VPC Resolver は、amazonaws.com の転送ルールを作成しても、一部の amazonaws.com サブドメインの DNS クエリを自動的に転送しません。詳細については、「VPC Resolver が自動定義されたシステムルールを作成するドメイン名」を参照してください。この動作を上書きする方法については、次の「すべてのクエリをネットワークに転送する」を参照してください。

すべてのクエリをネットワークに転送する

すべてのクエリが自分のネットワークに転送されるようにするには、ドメイン名に「.」(ドット) を指定しながらルールを作成し、このルールを、ネットワークへのすべての DNS クエリの転送先となる VPC に関連付けます。の外部で DNS リゾルバーを使用すると一部の機能が破損するため、VPC リゾルバー AWS は引き続きすべての DNS クエリをネットワークに転送しません。たとえば、一部の内部 AWS ドメイン名には、外部からアクセスできない内部 IP アドレス範囲があります AWS。「.」のクエリを作成したときに、ネットワークに転送されないクエリのドメイン名のリストについては、「VPC Resolver が自動定義されたシステムルールを作成するドメイン名」を参照してください。

ただし、逆引き DNS の自動定義されたシステムルールを無効にして、「.」ルールを許可し、すべての逆引き DNS クエリをネットワークに転送できます。自動定義されたルールをオフにする方法の詳細については、VPC Resolver でのリバース DNS クエリの転送ルール を参照してください。

デフォルトで転送から除外されるドメイン名も含めて、すべてのドメイン名の DNS クエリをネットワークに転送することを試す場合は、「.」ルールを作成して次のいずれかの操作を実行します。

- VPC の `enableDnsHostnames` フラグを `false` に設定します。
- 「VPC Resolver が自動定義されたシステムルールを作成するドメイン名」に示されているドメイン名に対してルールを作成します。

> **Important**
>
> 「.」ルールの作成時に VPC Resolver が除外するドメイン名を含め、すべてのドメイン名をネットワークに転送すると、一部の機能が動作しなくなる場合があります。

VPC Resolver がクエリ内のドメイン名がルールと一致するかどうかを判断する方法

Route 53 VPC Resolver は、DNS クエリのドメイン名を、クエリの送信元の VPC に関連付けられたルールのドメイン名と比較します。VPC Resolver は、次の場合にドメイン名が一致すると見なします。

- 両方のドメイン名が完全に一致する
- クエリ内のドメイン名は、ルール内のドメイン名のサブドメインである

たとえば、ルールのドメイン名が acme.example.com の場合、VPC Resolver は DNS クエリ内の次のドメイン名を一致と見なします。

- acme.example.com
- zenith.acme.example.com

以下のドメイン名は一致しません。

- example.com
- nadir.example.com

クエリのドメイン名が複数のルール (example.com や www.example.com など) のドメイン名と一致する場合、VPC Resolver は最も具体的なドメイン名 (www.example.com) を含むルールを使用してアウトバウンド DNS クエリをルーティングします。

VPC Resolver が DNS クエリを転送する場所を決定する方法

VPC の EC2 インスタンスで実行されるアプリケーションが DNS クエリを送信すると、Route 53 VPC Resolver は次の手順を実行します。

1. Resolver がルール内のドメイン名を確認します。

クエリのドメイン名がデフォルトの転送ルールのドメイン名と一致する場合、VPC Resolver はアウトバウンドエンドポイントの作成時に指定した IP アドレスにクエリを転送します。アウトバウンドエンドポイントは、このクエリを、ルールの作成時に指定したネットワークのリゾルバーの IP アドレスに転送します。

レスポンスの委任レコードが委任ルールと一致する場合、Resolver は委任ルールに関連付けられたアウトバウンドエンドポイントを介してオンプレミスリゾルバーに権限を委任します。

詳細については、「VPC Resolver がクエリ内のドメイン名がルールと一致するかどうかを判断する方法」を参照してください。

2. Resolver エンドポイントは、「.」ルールの設定に基づいて DNS クエリを転送します。

   クエリのドメイン名が他のルールのドメイン名と一致しない場合、VPC Resolver は自動定義された「.」(ドット) ルールの設定に基づいてクエリを転送します。ドットルールは、一部の AWS 内部ドメイン名とプライベートホストゾーンのレコード名を除くすべてのドメイン名に適用されます。このルールにより、クエリのドメイン名がカスタム転送ルールの名前と一致しない場合、VPC Resolver は DNS クエリをパブリックネームサーバーに転送します。すべてのクエリをネットワークの DNS リゾルバーに転送する場合は、カスタム転送ルールを作成し、ドメイン名として「.」を指定し、[タイプ] として [転送] を指定します。さらに、これらのリゾルバーの IP アドレスを指定します。

3. VPC Resolver は、クエリを送信したアプリケーションにレスポンスを返します。

複数のリージョンにおけるルールの使用

Route 53 VPC Resolver はリージョンサービスであるため、1 つの AWS リージョンで作成するオブジェクトは、そのリージョンでのみ使用できます。同じルールを複数のリージョンで使用するには、リージョンごとにルールを作成する必要があります。

ルールを作成した AWS アカウントは、ルールを他の AWS アカウントと共有できます。詳細については、「Resolver ルールを他の AWS アカウントと共有し、共有ルールを使用する」を参照してください。

VPC Resolver が自動定義されたシステムルールを作成するドメイン名

Resolver は、選択したドメインのクエリを解決する方法を定義する自動定義システムルールを自動的に作成します。

- プライベートホストゾーンの場合、および Amazon EC2 固有のドメイン名 (compute.amazonaws.com や compute.internal など) の場合、「.」(ドット) や「com」など、より具体的なドメイン名に対して条件付き転送ルールを作成した場合、自動定義ルールにより、プライベートホストゾーンと EC2 インスタンスが解決し続けます。
- パブリックに予約されたドメイン名 (localhost や 10.in-addr.arpa など) については、DNS のベストプラクティスに従って、クエリを公開ネームサーバーに転送しないで、ローカルで応答するようお勧めします。「RFC 6303, Locally Served DNS Zones」を参照してください。

> **Note**
>
> 「.」(ドット) または「com」の条件付き転送ルールを作成する場合は、amazonaws.com のシステムルールも作成することをお勧めします。(システムルールにより、VPC Resolver は特定のドメインとサブドメインの DNS クエリをローカルで解決します。) このシステムルールを作成すると、パフォーマンスが向上し、ネットワークに転送されるクエリの数が減少し、VPC リゾルバーの料金が削減されます。

自動定義ルールを上書きする場合は、同じドメイン名に対して条件付き転送ルールを作成できます。

一部の自動定義ルールを無効にすることもできます。詳細については、「VPC Resolver でのリバース DNS クエリの転送ルール」を参照してください。

VPC Resolver は、次の自動定義ルールを作成します。

プライベートホストゾーンのルール

VPC に関連付けるプライベートホストゾーンごとに、VPC Resolver はルールを作成し、VPC に関連付けます。プライベートホストゾーンを複数の VPCs、VPC Resolver はルールを同じ VPCs。

ルールのタイプは [転送] です。

さまざまな AWS 内部ドメイン名のルール

このセクションに示す内部ドメイン名では、すべてのルールタイプが [転送] となっています。VPC Resolver は、これらのドメイン名の DNS クエリを VPC の権威ネームサーバーに転送します。

> **Note**
>
> VPC Resolver は、VPC の enableDnsHostnamesフラグを に設定すると、これらのルールのほとんどを作成しますtrue。VPC Resolver は、Resolver エンドポイントを使用していない場合でもルールを作成します。

VPC Resolver は、VPC の enableDnsHostnamesフラグを に設定すると、次の自動定義ルールを作成し、VPC に関連付けますtrue。

- *Region-name*.compute.internal (例: eu-west-1.compute.internal)。us-east-1 リージョンでは、このドメイン名を使用しません。
- *Region-name*.compute.*amazon-domain-name* (例: eu-west-1.compute.amazonaws.com または cn-north-1.compute.amazonaws.com.cn)。us-east-1 リージョンでは、このドメイン名を使用しません。
- ec2.internal。us-east-1 リージョンでのみ、このドメイン名を使用します。
- compute-1.internal。us-east-1 リージョンでのみ、このドメイン名を使用します。
- compute-1.amazonaws.com。us-east-1 リージョンでのみ、このドメイン名を使用します。

次の自動定義ルールは、VPC の enableDnsHostnamesフラグを に設定したときに VPC Resolver が作成するルールの逆引き DNS ルックアップ用ですtrue。

- 10.in-addr.arpa
- 16.172.in-addr.arpa から 31.172.in-addr.arpa
- 168.192.in-addr.arpa
- 254.169.254.169.in-addr.arpa
- VPC の各 CIDR 範囲のルール。たとえば、CIDR 範囲が 10.0.0.0/23 の VPC の場合、VPC Resolver は次のルールを作成します。
  - 0.0.10.in-addr.arpa
  - 1.0.10.in-addr.arpa

以下の自動定義ルールは、localhost に関連するドメイン用であり、VPC の enableDnsHostnames フラグを true に設定したときに作成されて VPC に関連付けられます。

- 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

VPC Resolver は、トランジットゲートウェイまたは VPC ピアリングを介して VPC を別の VPC に接続し、DNS サポートを有効にすると、次の自動定義ルールを作成し、VPC に関連付けます。

- ピア VPC の IP アドレス範囲の逆引き DNS ルックアップ (例: 0.192.in-addr.arpa)。

  VPC に IPv4 CIDR ブロックを追加すると、VPC Resolver は新しい IP アドレス範囲の自動定義ルールを追加します。
- 他の VPC が別のリージョンにある場合、以下のドメイン名になります。
  - *Region-name*.compute.internal。us-east-1 リージョンでは、このドメイン名を使用しません。
  - *Region-name*.compute.*amazon-domain-name*。us-east-1 リージョンでは、このドメイン名を使用しません。
  - ec2.internal。us-east-1 リージョンでのみ、このドメイン名を使用します。
  - compute-1.amazonaws.com。us-east-1 リージョンでのみ、このドメイン名を使用します。

他のすべてのドメイン用のルール

VPC Resolver は、このトピックの前半で指定されていないすべてのドメイン名に適用される「.」(ドット) ルールを作成します。「.」ルールには 再帰型があります。つまり、このルールにより VPC リゾルバーが再帰リゾルバーとして機能します。

インバウンドエンドポイントとアウトバウンドエンドポイントを作成する際の考慮事項

AWS リージョンでインバウンドおよびアウトバウンドの Resolver エンドポイントを作成する前に、次の問題を考慮してください。

トピック

- 各リージョンのインバウンドエンドポイントおよびアウトバウンドエンドポイントの数
- インバウンドエンドポイントとアウトバウンドエンドポイントに同じ VPC を使用する
- インバウンドエンドポイントとプライベートホストゾーン
- VPC ピアリング接続

- 共有サブネット内の IP アドレス
- ネットワークとエンドポイントを作成する VPC との間の接続
- ルールを共有すると、アウトバウンドエンドポイントも共有されます。
- エンドポイントのプロトコルの選択
- 専用インスタンステナンシー用に設定された VPC での VPCs リゾルバーの使用

各リージョンのインバウンドエンドポイントおよびアウトバウンドエンドポイントの数

AWS リージョン内の VPCs の DNS をネットワークの DNS と統合する場合は、通常、1 つのリゾルバーインバウンドエンドポイント (VPCs に転送する DNS クエリの場合) と 1 つのアウトバウンドエンドポイント (VPCs からネットワークに転送するクエリの場合) が必要です。複数のインバウンドエンドポイントとアウトバウンドエンドポイントを作成できますが、それぞれの方向のDNS クエリを処理するために1つのインバウンドまたはアウトバウンドエンドポイントで十分です。次の点に注意してください。

- 各 Resolver エンドポイントのために、それぞれ異なるアベイラビリティーゾーンで 2 つ以上の IP アドレスを指定します。エンドポイント内の各 IP アドレスは、1 秒間に多数の DNS クエリを処理できます。(エンドポイントの IP アドレスあたりの 1 秒あたりのクエリの現在の最大数については、「Route 53 VPC リゾルバーのクォータ」を参照してください) VPC Resolver でより多くのクエリを処理する必要がある場合は、別のエンドポイントを追加する代わりに、既存のエンドポイントに IP アドレスを追加できます。
- VPC Resolver の料金は、エンドポイント内の IP アドレスの数と、エンドポイントが処理する DNS クエリの数に基づきます。各エンドポイントに最低 2 つの IP アドレスが含まれています。VPC Resolver の料金の詳細については、「Amazon Route 53 の料金」を参照してください。
- 各ルールは、DNS クエリの転送元の発信エンドポイントを指定します。 AWS リージョンに複数のアウトバウンドエンドポイントを作成し、一部またはすべての Resolver ルールをすべての VPC に関連付ける場合は、それらのルールのコピーを複数作成する必要があります。

インバウンドエンドポイントとアウトバウンドエンドポイントに同じ VPC を使用する

インバウンドエンドポイントとアウトバウンドエンドポイントは、同じ VPC 内に作成することも、同じリージョン内の異なる VPC 内に作成することもできます。

詳細については、「Amazon Route 53 のベストプラクティス」を参照してください

インバウンドエンドポイントとプライベートホストゾーン

VPC Resolver でプライベートホストゾーンのレコードを使用してインバウンド DNS クエリを解決する場合は、プライベートホストゾーンをインバウンドエンドポイントを作成した VPC に関連付けます。プライベートホストゾーンと VPC の関連付けについては、「プライベートホストゾーンの使用」を参照してください。

VPC ピアリング接続

選択した VPC が他の VPC とピアリングされているかどうかにかかわらず、インバウンドエンドポイントまたはアウトバウンドエンドポイントに AWS リージョン内の任意の VPCsを使用できます。詳細については、「Amazon Virtual Private Cloud VPC Peering」を参照してください。

共有サブネット内の IP アドレス

インバウンドまたはアウトバウンドエンドポイントを作成する場合、現在のアカウントで VPC を作成した場合のみ、共有サブネットに IP アドレスを指定できます。別のアカウントで VPC を作成し、VPC のサブネットをアカウントと共有している場合、そのサブネットで IP アドレスを指定することはできません。共有サブネットの詳細については、Amazon VPC ユーザーガイドの「共有 VPC の使用」を参照してください。

ネットワークとエンドポイントを作成する VPC との間の接続

ネットワークとエンドポイントを作成する VPC との間には、次のいずれかの接続が必要です。

- インバウンドエンドポイント - ネットワークと、インバウンドエンドポイントの作成先の各 VPC との間に Direct Connect 接続または VPN 接続を設定する必要があります。
- アウトバウンドエンドポイント - ネットワークとアウトバウンドエンドポイントを作成する各 VPC の間に Direct Connect 接続、VPN 接続、またはネットワークアドレス変換 (NAT) ゲートウェイを設定する必要があります。

ルールを共有すると、アウトバウンドエンドポイントも共有されます。

ルールを作成するときは、VPC Resolver が DNS クエリをネットワークに転送するために使用するアウトバウンドエンドポイントを指定します。ルールを別の AWS アカウントと共有する場合、ルールで指定したアウトバウンドエンドポイントも間接的に共有します。複数の AWS アカウントを使用して AWS リージョンに VPCs を作成した場合は、次の操作を実行できます。

- リージョンにアウトバウンドエンドポイントを 1 つ作成します。

- 1 つの AWS アカウントを使用してルールを作成します。
- リージョンで VPCs を作成したすべての AWS アカウントとルールを共有します。

これにより、リージョン内の 1 つのアウトバウンドエンドポイントを使用して、VPC が異なる AWS アカウントを使用して作成された場合でも、DNS クエリを複数の VPCsからネットワークに転送できます。

エンドポイントのプロトコルの選択

エンドポイントプロトコルは、データをインバウンドエンドポイントに送信する方法とアウトバウンドエンドポイントから送信する方法を決定します。ネットワーク上のすべてのパケットフローは、送信と配信の前に正しい送信元と送信先を検証するルールに基づいて個別に承認されるため、VPC トラフィックの DNS クエリを暗号化する必要はありません。送信側と受信側の両方から特別な許可されていない限り、情報がエンティティ間で勝手にやり取りされることはほとんどありません。パケットが、一致するルールのない送信先にルーティングされる場合、そのパケットはドロップされます。詳細については、「Amazon VPC の特徴」を参照してください。

使用可能なプロトコルは次のとおりです。

- Do53: ポート 53 経由の DNS。データは、追加の暗号化なしで VPC リゾルバーを使用して中継されます。データは外部関係者が読み取ることはできませんが、 AWS ネットワーク内で表示できます。UDP または TCP を使用してパケットを送信します。Do53 は主に Amazon VPC 内および Amazon VPC 間のトラフィックに使用されます。現在、これは委任インバウンドエンドポイントで使用できる唯一のプロトコルです。
- DoH: データは暗号化された HTTPS セッションを介して送信されます。DoH は、権限のないユーザーがデータを復号化できず、意図した受信者以外はデータを読み取れないというセキュリティレベルを追加します。委任インバウンドエンドポイントでは使用できません。
- DoH-FIPS: データは FIPS 140-2 暗号規格に準拠した暗号化された HTTPS セッションを介して送信されます。インバウンドエンドポイントのみでサポートされます。詳細については、「FIPS PUB 140-2」を参照してください。委任インバウンドエンドポイントでは使用できません。

転送タイプのインバウンドエンドポイントには、以下のようにプロトコルを適用できます。

- Do53 と DoH の組み合わせ。
- Do53 と DoH-FIPS の組み合わせ。
- Do53 のみ。

- DoH のみ。
- DoH-FIPS のみ。
- なし。Do53 として扱われます。

アウトバウンドエンドポイントには、以下のようにプロトコルを適用できます。

- Do53 と DoH　の組み合わせ。
- Do53 のみ。
- DoH のみ。
- なし。これは Do53 として扱われます。

「インバウンドエンドポイントを作成または編集するときに指定する値」および「アウトバウンドエンドポイントを作成または編集するときに指定する値」も参照してください。

専用インスタンステナンシー用に設定された VPC での VPCs リゾルバーの使用

Resolver エンドポイントを作成する際、インスタンスのテナンシー属性が `dedicated` に設定されている VPC を指定することはできません。VPC Resolver はシングルテナントハードウェアでは実行されません。

VPC Resolver を使用して、VPC で発生する DNS クエリを解決できます。テナンシーが `default` に設定された VPC を少なくとも 1 つ作成し、インバウンドエンドポイントとアウトバウンドエンドポイントを作成するときに、その VPC を指定します。

移管ルールを作成するときは、インスタンステナンシーの設定に関わらず、任意の VPC に関連付けることができます。

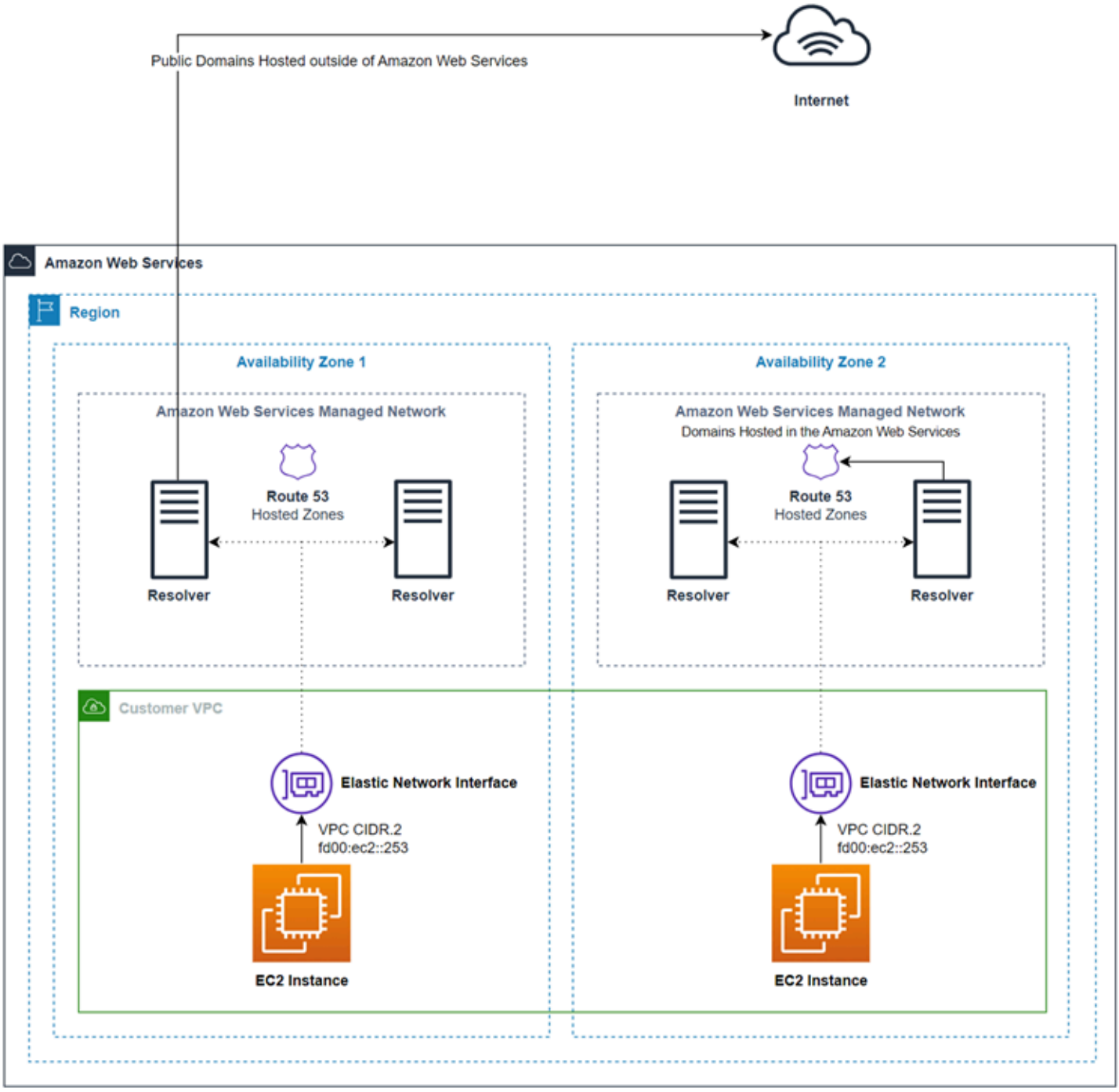
Route 53 VPC Resolver の可用性とスケーリング

Amazon VPC CIDR + 2 アドレスおよび fd00:ec2::253 で実行されている Route 53 VPC Resolver は、デフォルトですべての VPCs、パブリックレコード、Amazon VPC 固有の DNS 名、Route 53 プライベートホストゾーンの DNS クエリに再帰的に応答します。Route 53 VPC Resolver を構成する高可用性コンポーネントには、Nitro Resolver サービスとゾーンリゾルバーフリートの 2 つがあります。Nitro Resolver Service は、Nitro インスタンスの Nitro カードおよび旧世代のインスタンスの Dom0 で実行され、ホストサーバー上のローカルで Route 53 VPC Resolver 宛てのパケットを消費するサービスです。詳細については、「The Security Design of the AWS Nitro System」を参照してください。

Nitro Resolver サービスにはローカルキャッシュが格納されており、インスタンスによって短時間にわたって繰り返されるクエリに応答することでレイテンシーを短縮できます。Nitro Resolver サービスは、キャッシュされた回答がないクエリを受信すると、クエリを Zonal Resolver フリートに転送します。Zonal Resolver フリートは、通常、インスタンスと同じアベイラビリティーゾーンにある高可用性リゾルバーフリートです。アップストリームのネームサーバーやパスのその他のコンポーネントによるクエリの処理に障害が発生した場合、Nitro Resolver サービスは、インスタンスで実行されているワークロードに影響を与えることなく、これらの障害を透過的に処理することがよくあります。さらに、Resolver がドメインのネームサーバーからクエリタイムアウト、拒否された接続、または SERVFAILS が発生した場合、可用性を向上させるために Time-To-Live (TTL) 値を超えるキャッシュされた応答で応答することがあります。Nitro Resolver サービスと Zonal Resolver フリート間のクエリは、顧客 VPC の外部で厳密に制御されたネットワークに制限されます。このネットワークは顧客にアクセスできず、厳格なセキュリティコントロールの対象となります。Nitro Resolver サービスと VPC 外の Zonal Resolver フリート間のクエリを処理することで、顧客は VPC 内の DNS クエリを傍受できなくなります。の外部にあるネームサーバー宛てのクエリ AWS は、ゾーンリゾルバーフリートに属するパブリック IP アドレスから発信されるパブリックインターネットを経由します。VPC Resolver は EDNS0-Client Subnet 属性をサポートしていません。つまり、パブリック DNS ネームサーバー宛てのすべてのクエリには、発信元顧客の IP アドレスに関する情報が含まれません。

Nitro Resolver サービスは、インスタンス上の Link-Local サービスの一部です。リンクローカルサービスには、Route 53 VPC Resolver、Amazon Time Service (NTP)、Instance Metadata Service (IMDS)、Windows Licensing Service (Windows インスタンス用) などがあります。これらのサービスは、VPC で作成する各 Elastic Network Interface に合わせてスケーリングされ、各ネットワークインターフェイスでは、Link-Local サービス宛ての 1024 パケット/秒 (PPS) が許可されます。この制限を超えるパケットは拒否されます。ethtool によって返される `linklocal_allowance_exceeded` 値から、この制限を超えたかどうかを判断できます。ethtool の詳細については、「Amazon EC2 ユーザーガイド」の「Amazon EC2 インスタンスのネットワークパフォーマンスのモニタリング」を参照してください。このメトリクスは、CloudWatch エージェントによって CloudWatch メトリクスに報告することもできます。Route 53 VPC Resolver はネットワークインターフェイスごとに実装されるため、より多くのアベイラビリティーゾーンにインスタンスを追加すると、スケーリングと信頼性が向上します。クエリの数には VPC ごとの集計制限がないため、Route 53 VPC Resolver は、本質的にネットワークアドレス使用量 (NAU) に基づく VPC の境界内でスケールできます。詳細については、「Amazon Virtual Private Cloud ユーザーガイド」の「VPC のネットワークアドレスの使用状況」を参照してください。

次の図は、Route 53 VPC Resolver がアベイラビリティーゾーン内の DNS クエリを解決する方法の概要を示しています。



Route 53 VPC Resolver の開始方法

Route 53 VPC Resolver コンソールには、VPC Resolver の使用を開始するための次のステップをガイドするウィザードが含まれています。

- エンドポイントを作成する: インバウンド、アウトバウンド、またはその両方。

- アウトバウンドエンドポイントの場合は、1 つ以上の転送ルールを作成します。このルールにより、ネットワークにルーティングする DNS クエリのドメイン名を指定します。
- アウトバウンドエンドポイントを作成した場合は、ルールを関連付ける VPC を選択します。

ウィザードを使用して Route 53 VPC Resolver を設定するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53resolver/ で VPC Resolver コンソールを開きます。
2. Route 53 VPC リゾルバーへようこそページで、エンドポイントの設定を選択します。
3. ナビゲーションバーで、Resolver エンドポイントを作成するリージョンを選択します。
4. [Basic configuration (基本的な設定)] で、DNS クエリを転送する方向を選択します。
   - インバウンドとアウトバウンド: ウィザードは、ネットワーク上のリゾルバーから VPC 内の VPC リゾルバーに DNS クエリを転送し、指定されたクエリ (example.com や example.net など) を VPC からネットワーク上のリゾルバーに転送する設定をガイドします。
   - インバウンドのみ: ウィザードは、ネットワーク上のリゾルバーから VPC 内の VPC リゾルバーに DNS クエリを転送する設定をガイドします。
   - Outbound only (アウトバウンドのみ): ウィザードの設定手順に従って、指定したクエリを VPC からネットワークのリゾルバーに転送できます。
5. [Next (次へ)] を選択します。
6. [Inbound and outbound (インバウンドおよびアウトバウンド)] または [Inbound only (インバウンドのみ)] を選択した場合は、インバウンドエンドポイントを設定するための適切な値を入力します。次に、ステップ 7 に進みます。詳細については、「インバウンドエンドポイントを作成または編集するときに指定する値」を参照してください

   [Outbound only (アウトバウンドのみ)] を選択した場合は、ステップ 7 に進みます。
7. アウトバウンドエンドポイントを設定するための適切な値を入力します。詳細については、「アウトバウンドエンドポイントを作成または編集するときに指定する値」を参照してください
8. [Inbound and outbound (インバウンドおよびアウトバウンド)] または [Outbound only (アウトバウンドのみ)] を選択した場合は、ルールを作成するための適切な値を入力します。詳細については、「ルールを作成または編集するときに指定する値」を参照してください
9. [Review and create (確認および作成)] ページで、前のページで指定した設定を確認します。必要に応じて、該当するセクションの [Edit (編集)] を選択し、設定を更新します。設定が適切であることを確認したら、[Submit (送信)] を選択します。

> **Note**
>
> アウトバウンドエンドポイントを作成するには、1～2 分かかります。最初のアウトバウンドエンドポイントの作成が完了するまでは、別のエンドポイントを作成できません。

10. 追加のルールを作成する場合は、「転送ルールの管理」を参照してください。
11. インバウンドエンドポイントを作成した場合は、該当する DNS クエリをインバウンドエンドポイントの IP アドレスに転送するように、ネットワークの DNS リゾルバーを設定します。詳細については、DNS アプリケーションのドキュメントを参照してください。

VPC へのインバウンド DNS クエリの転送

ネットワークから VPC Resolver に DNS クエリを転送するには、インバウンドエンドポイントを作成します。インバウンドエンドポイントは、ネットワーク上の DNS リゾルバーが DNS クエリを転送する IP アドレスを (VPC で使用できる IP アドレスの範囲から) 指定します。これらの IP アドレスはパブリック IP アドレスではないため、インバウンドエンドポイントごとに、 Direct Connect 接続または VPN 接続を使用して VPC をネットワークに接続する必要があります。

インバウンド委任を実装する場合、サブドメインの DNS 権限をオンプレミスの DNS インフラストラクチャから VPC Resolver に委任します。この委任を適切に設定するには、インバウンドエンドポイントの IP アドレスを、委任されるサブドメインのオンプレミスネームサーバーのグルーレコード (NS レコード) として使用する必要があります。例えば、IP アドレスが 10.0.1.100 および 10.0.1.101 のインバウンド委任エンドポイントを介してサブドメイン「aws.example.com」を VPC Resolver に委任する場合、オンプレミス DNS サーバーでこれらの IP アドレスを「aws.example.com」とする NS レコードを作成します。これにより、委任サブドメインの DNS クエリがインバウンドエンドポイントを介して VPC リゾルバーに適切にルーティングされ、VPC リゾルバーが関連するプライベートホストゾーンからのレコードで応答できるようになります。

インバウンド転送の設定

インバウンドエンドポイントを作成するには、次の手順を実行します。

インバウンドエンドポイントを作成するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで、[Inbound endpoints (インバウンドエンドポイント)] を選択します。

3. ナビゲーションバーで、インバウンドエンドポイントを作成するリージョンを選択します。
4. [Create inbound endpoint (インバウンドエンドポイントの作成)] を選択します。
5. 適切な値を入力します。詳細については、「インバウンドエンドポイントを作成または編集するときに指定する値」を参照してください
6. [Create (作成)] を選択します。
7. 該当する DNS クエリをインバウンドエンドポイントの IP アドレスに転送するように、ネットワークの DNS リゾルバーを設定します。詳細については、DNS アプリケーションのドキュメントを参照してください。

インバウンドエンドポイントを作成または編集するときに指定する値

インバウンドエンドポイントを作成または編集する場合、以下の値を指定します。

Outpost ID

AWS Outposts VPC で VPC リゾルバーのエンドポイントを作成する場合、これは AWS Outposts ID です。

エンドポイント名

わかりやすい名前にすると、ダッシュボードでインバウンドエンドポイントを見つけやすくなります。

エンドポイントカテゴリ

デフォルトまたは委任を選択します。カテゴリがデフォルトの場合、ネットワークのリゾルバーは DNS リクエストをインバウンドエンドポイントの IP アドレスに転送します。カテゴリが委任の場合、ドメインの権限は VPC リゾルバーに委任されます。

region-name リージョンの VPC

ネットワークからのすべてのインバウンド DNS クエリは、VPC リゾルバーへの途中でこの VPC を通過します。

このエンドポイントのセキュリティグループ

この VPC へのアクセスを制御するために使用する 1 つ以上のセキュリティグループの ID です。指定したセキュリティグループには、1 つ以上のインバウンドルールを含める必要があります。インバウンドルールでは、ポート 53 での TCP および UDP アクセスを許可する必要があります。DoH プロトコルを使用している場合は、セキュリティグループのポート 443 も許可する必要があります。エンドポイントの作成後にこの値を変更することはできません。

セキュリティグループルールによっては、接続が追跡され、インバウンドエンドポイントの IP アドレスごとの 1 秒あたりの全体的な最大クエリ数は 1,500 に抑えられます。セキュリティグループによる接続の追跡を回避するには、「追跡されていない接続」を参照してください。

> **Note**
>
> 複数のセキュリティグループを追加するには、 AWS CLI コマンド を使用しますcreate-resolver-endpoint。詳細については、「create-resolver-endpoint」を参照してください

詳細については、Amazon VPC ユーザーガイドの「VPC のセキュリティグループ」を参照してください。

エンドポイントタイプ

エンドポイントのタイプは、IPv4、IPv6、デュアルスタック IP アドレスのいずれかです。デュアルスタックエンドポイントの場合、エンドポイントには、ネットワーク上の DNS リゾルバーが DNS クエリを転送できる IPv4 アドレスと IPv6 アドレスの両方があります。

> **Note**
>
> セキュリティ上の理由から、VPC Resolver は、すべてのデュアルスタック IP アドレスと IPv6 IP アドレスに対するパブリックインターネットからの直接 IPv6 トラフィックアクセスを拒否します。

IP アドレス

ネットワークの DNS リゾルバーから DNS クエリを転送する先の IP アドレスです。冗長性を確保するためには、少なくとも 2 つの IP アドレスを指定する必要があります。委任インバウンドエンドポイントを作成した場合は、これらの IP アドレスを、権限を VPC Resolver に委任するサブドメインのグルー NS レコードとして使用します。次の点に注意してください。

複数アベイラビリティーゾーン

少なくとも 2 つのアベイラビリティーゾーンで IP アドレスを指定することをお勧めします。必要に応じて、それらのアベイラビリティーゾーンまたは他のアベイラビリティーゾーンに追加の IP アドレスを指定できます。

IP アドレスと Amazon VPC Elastic Network Interface

指定したアベイラビリティーゾーン、サブネット、および IP アドレスの組み合わせごとに、VPC Resolver は Amazon VPC Elastic Network Interface を作成します。エンドポイントの IP アドレスあたりの 1 秒あたりの DNS クエリの現在の最大数については、「Route 53 VPC リゾルバーのクォータ」を参照してください。各 Elastic Network Interface の料金については、Amazon Route 53 料金ページの「Amazon Route 53」を参照してください。

> **Note**
>
> Resolver エンドポイントはプライベート IP アドレスを持ちます。これらの IP アドレスは、エンドポイントの存続期間中に変更されることはありません。

IP アドレスごとに、以下の値を指定します。各 IP アドレスは、[VPC in the region-name Region (region-name リージョンの VPC)] で指定した VPC のアベイラビリティーゾーンに存在する必要があります。

アベイラビリティーゾーン

VPC に向かう途中で DNS クエリを通過させるアベイラビリティーゾーンです。指定したアベイラビリティーゾーンには、サブネットが設定されている必要があります。

サブネット

Resolver エンドポイント ENI に割り当てる IP アドレスを含むサブネット。これらは DNS クエリを送信するアドレスです。サブネットには使用可能な IP アドレスが必要です。

サブネット IP アドレスはエンドポイントタイプと一致する必要があります。

Outposts ラックでエンドポイントを作成するには、 AWS Outposts で VPC Resolver AWS を使用することをお勧めします。

> **Important**
>
> ローカルネットワークインターフェイス (LNI) が有効になっている Outposts サブネットは、VPC Resolver エンドポイントと互換性がありません。VPC Resolver エンドポイントの Elastic Network Interface (ENIs) を含むサブネットで LNI を有効にすると、それらの ENIsは機能しなくなります。詳細については、「Resolver エンドポイントのサブネット互換性」を参照してください。

IP アドレス

インバウンドエンドポイントに割り当てる IP アドレス。

VPC Resolver で、指定したサブネットで使用可能な IP アドレスの中から IP アドレスを選択するか、自分で IP アドレスを指定するかを選択します。

IP アドレスを自分で指定することを選択した場合は、IPv4 か IPv6 のいずれか、または両方のアドレスを入力します。

プロトコル

エンドポイントプロトコルが、受信エンドポイントへのデータ送信方法を決定します。必要なセキュリティのレベルに応じて 1 つまたは複数のプロトコルを選択します。

- Do53: (デフォルト) データは、追加の暗号化なしで Route 53 VPC リゾルバーを使用してリレーされます。データは外部関係者が読み取ることはできませんが、 AWS ネットワーク内で表示できます。これは、委任インバウンドエンドポイントカテゴリで現在利用できる唯一のプロトコルです。
- DoH: データは暗号化された HTTPS セッションを介して送信されます。DoH は、権限のないユーザーがデータを復号化したり、目的の受信者以外がデータを読み取ったりできないようにするセキュリティレベルを高めます。
- DoH-FIPS: データは FIPS 140-2 暗号規格に準拠した暗号化された HTTPS セッションを介して送信されます。インバウンドエンドポイントのみでサポートされます。詳細については、「FIPS PUB 140-2」を参照してください。

> **Note**
>
> DoH/DoH-FIPS インバウンドエンドポイントの場合、VPC Resolver クエリログに誤ったソース IP が発行されるという既知の問題があります。

インバウンドエンドポイントの場合、プロトコルを次のように適用できます。

- Do53 と DoH　の組み合わせ。
- Do53 と DoH-FIPS の組み合わせ。
- Do53 のみ。
- DoH のみ。
- DoH-FIPS のみ。
- なし。これは Do53 として扱われます。

> **Important**
>
> 受信エンドポイントのプロトコルを Do53 のみから DoH または DoH-FIPS のみに直接変更できません。これは、Do53 に依存する受信トラフィックが突然中断されるのを防止するためです。プロトコルを Do53 から DoH または DoH-FIPS に変更するには、まず Do53 と DoH、または Do53 と DoH-FIPS の両方を有効にして、すべての着信トラフィックが DoH プロトコル (DoH-FIP) を使用するように転送されたことを確認してから、Do53 を削除する必要があります。

DNS64

DNS64 を有効にして、VPC Resolver が IPv4-only4 専用サービスの AAAA (IPv6) レコードを合成できるようにします。IPv6-onlyクライアントが IPv6 アドレスを持たないサービスに対してクエリを実行すると、VPC Resolver は IPv6 アドレスによく知られている`64:ff9b::/96`プレフィックスを付加して IPv46 アドレスを合成します。これにより、インバウンドエンドポイントを介してクエリを送信する IPv6 専用クライアントが IPv4 専用サービスに到達できるようになります。DNS64 は NAT64 と連携して、IPv6 から IPv4 への完全な変換を提供します。

詳細については、Amazon VPC ユーザーガイドの DNS64 および NAT64 を参照してください。

タグ

1 つ以上のキーと対応する値を指定します。例えば、[Key (キー)] に Cost center を、[Value (値)] には 456 を指定します。

インバウンドエンドポイントの管理

インバウンドエンドポイントを管理するには、該当する手順を実行します。

トピック

- インバウンドエンドポイントの表示と編集
- インバウンドエンドポイントのステータスの表示
- インバウンドエンドポイントの削除

インバウンドエンドポイントの表示と編集

インバウンドエンドポイントの設定を表示および編集するには、次の手順を実行します。

インバウンドエンドポイントの設定を表示および編集するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで、[Inbound endpoints (インバウンドエンドポイント)] を選択します。
3. ナビゲーションバーで、インバウンドエンドポイントを作成したリージョンを選択します。
4. 設定を表示または編集するエンドポイントのオプションを選択します。
5. [View details (詳細の表示)] または [Edit (編集)] を選択します。

   インバウンドエンドポイントの値の詳細については、「インバウンドエンドポイントを作成または編集するときに指定する値」を参照してください。
6. [Edit (編集)] を選択した場合は、該当する値を入力し、[Save (保存)] を選択します。

インバウンドエンドポイントのステータスの表示

インバウンドエンドポイントのステータスを表示するには、次の手順を実行します。

インバウンドエンドポイントのステータスを表示するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで、[Inbound endpoints (インバウンドエンドポイント)] を選択します。
3. ナビゲーションバーで、インバウンドエンドポイントを作成したリージョンを選択します。[Status] 列には、次のいずれかの値が表示されます。

   作成

   VPC Resolver は、このエンドポイントの 1 つ以上の Amazon VPC ネットワークインターフェイスを作成および設定しています。

   運用中

   このエンドポイントの Amazon VPC ネットワークインターフェイスが正しく設定されており、ネットワークと VPC Resolver 間でインバウンドまたはアウトバウンドの DNS クエリを渡すことができます。

[更新中]

VPC Resolver は、1 つ以上のネットワークインターフェイスをこのエンドポイントと関連付けまたは関連付け解除しています。

自動復旧中

VPC Resolver は、このエンドポイントに関連付けられている 1 つ以上のネットワークインターフェイスを復旧しようとしています。復旧プロセス中は、IP アドレスごと (ネットワークインターフェイスごと) の DNS クエリの数の制限により、エンドポイントは容量が制限された状態で機能します。現在の制限については、「Route 53 VPC リゾルバーのクォータ」を参照してください。

Action needed (アクションが必要)

このエンドポイントは異常であり、VPC Resolver は自動的に復旧できません。この問題を解決するには、エンドポイントに関連付けした各 IP アドレスを確認することをお勧めします。使用できない IP アドレスごとに別の IP アドレスを追加して、使用できない IP アドレスを削除します。(エンドポイントには常に少なくとも 2 つの IP アドレスが含まれている必要があります。) [必要なアクション] のステータスにはさまざまな原因が考えられます。一般的な 2 つの原因を以下に示します。

- エンドポイントに関連付けられている、1 つまたは複数のネットワークインターフェイスが、Amazon VPC を使用して削除されました。
- VPC Resolver のコントロール外にある何らかの理由により、ネットワークインターフェイスを作成できませんでした。

削除

VPC Resolver はこのエンドポイントと関連するネットワークインターフェイスを削除しています。

インバウンドエンドポイントの削除

インバウンドエンドポイントを削除するには、次の手順を実行します。

> **Important**
>
> インバウンドエンドポイントを削除すると、ネットワークからの DNS クエリは、エンドポイントで指定した VPC の VPC リゾルバーに転送されなくなります。

インバウンドエンドポイントを削除するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで、[Inbound endpoints (インバウンドエンドポイント)] を選択します。
3. ナビゲーションバーで、インバウンドエンドポイントを作成したリージョンを選択します。
4. 削除するエンドポイントのオプションを選択します。
5. [Delete (削除)] を選択します。
6. エンドポイントの削除を確定するには、エンドポイントの名前を入力し、[Submit (送信)] を選択します。

ネットワークへのアウトバウンド DNS クエリの転送

複数の VPC にある Amazon EC2 インスタンスから発信された DNS クエリを、自分のネットワークに転送するには、アウトバウンドエンドポイントと 1 つ以上のルールを作成します。

アウトバウンドエンドポイント

DNS クエリを VPC からネットワークに転送するには、アウトバウンドエンドポイントを作成します。アウトバウンドエンドポイントは、クエリの送信元の IP アドレスを指定します。VPC で使用できる IP アドレスの範囲から選択するこれらの IP アドレスは、パブリック IP アドレスではありません。つまり、アウトバウンドエンドポイントごとに、 Direct Connect 接続、VPN 接続、またはネットワークアドレス変換 (NAT) ゲートウェイを使用して VPC をネットワークに接続する必要があります。同じリージョン内の複数の VPC で、同一のアウトバウンドエンドポイントを使用することも、複数のアウトバウンドエンドポイントを作成することもできます。アウトバウンドエンドポイントで DNS64 を使用する場合は、Amazon Virtual Private Cloud を使用して DNS64 を有効にできます。詳細については、Amazon VPC ユーザーガイドの DNS64 および NAT64 を参照してください。

VPC Resolver ルールのターゲット IP は VPC Resolver によってランダムに選択され、他のターゲット IP よりも特定のターゲット IP を選択する好みはありません。転送された DNS リクエストにターゲット IP が応答しない場合、VPC リゾルバーはターゲット IP 間でランダム IP アドレスに再試行IPs。

すべてのターゲット IP アドレスが Resolver エンドポイントから到達可能であることを確認します。VPC Resolver がアウトバウンド DNS クエリをターゲット IPs に転送できない場合、DNS 解決時間が長くなる可能性があります。

Rules

ネットワークの DNS リゾルバーに転送するクエリのドメイン名を指定するには、1 つまたは複数のルールを作成します。各転送ルールは 1 つのドメイン名を指定します。次に、ネットワークにクエリを転送する VPCs にルールを関連付けます。

アウトバウンド委任ルールは、標準の転送ルールとは異なる特定の委任原則に従います。委任ルールを作成すると、VPC Resolver はルールの委任レコードを DNS レスポンスの NS レコードと照らし合わせて評価し、委任が必要かどうかを判断します。VPC リゾルバーは、委任ルール設定と DNS レスポンスで返された実際の NS レコードが一致している場合にのみ、オンプレミスリゾルバーに権限を委任します。ドメイン名の一致に基づいてクエリをリダイレクトする転送ルールとは異なり、委任ルールは DNS 委任チェーンを尊重し、レスポンス内の信頼できるネームサーバーが委任設定と一致する場合にのみアクティブ化します。

詳細については、以下の各トピックを参照してください。

- Private hosted zones that have overlapping namespaces
- Private hosted zones and Route 53 VPC Resolver rules

アウトバウンド転送の設定

VPC で発生した DNS クエリをネットワークに転送するように VPC Resolver を設定するには、次の手順を実行します。

> **Important**
>
> アウトバウンドエンドポイントを作成したら、1 つ以上のルールを作成し、1 つ以上の VPCs に関連付ける必要があります。ルールは、ネットワークに転送する DNS クエリのドメイン名を指定します。

アウトバウンドエンドポイントを作成するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで、[Outbound endpoints (アウトバウンドエンドポイント)] を選択します。
3. ナビゲーションバーで、アウトバウンドエンドポイントを作成するリージョンを選択します。

4. [Create outbound endpoint (アウトバウンドエンドポイントの作成)] を選択します。
5. 適切な値を入力します。詳細については、「アウトバウンドエンドポイントを作成または編集するときに指定する値」を参照してください
6. [Create (作成)] を選択します。

> **Note**
>
> アウトバウンドエンドポイントを作成するには、1～2 分かかります。最初のアウトバウンドエンドポイントの作成が完了するまでは、別のエンドポイントを作成できません。

7. ネットワークに転送する DNS クエリのドメイン名を指定するには、1 つまたは複数のルールを作成します。詳細については、次の手順を参照してください。

1 つまたは複数の転送ルールを作成するには、次の手順を実行します。

転送ルールを作成して 1 つ以上の VPC に関連付けるには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [ルール] を選択します。
3. ナビゲーションバーで、転送ルールを作成するリージョンを選択します。
4. [Create rule] を選択します。
5. 適切な値を入力します。詳細については、「ルールを作成または編集するときに指定する値」を参照してください
6. [Save] を選択します。
7. さらにルールを追加するには、ステップ 4～6 を繰り返します。

アウトバウンドエンドポイントを作成または編集するときに指定する値

アウトバウンドエンドポイントを作成または編集する場合、以下の値を指定します。

Outpost ID

AWS Outposts VPC で VPC リゾルバーのエンドポイントを作成する場合、これは AWS Outposts ID です。

エンドポイント名

わかりやすい名前にすると、ダッシュボードでアウトバウンドエンドポイントを見つけやすくなります。

region-name リージョンの VPC

すべてのアウトバウンド DNS クエリは、ネットワークへの途中でこの VPC を経由します。

このエンドポイントのセキュリティグループ

この VPC へのアクセスを制御するために使用する 1 つ以上のセキュリティグループの ID です。指定したセキュリティグループには、1 つ以上のアウトバウンドルールを含める必要があります。アウトバウンドルールでは、ネットワークで DNS クエリに使用するポートで TCP および UDP アクセスを許可する必要があります。エンドポイントの作成が完了した後は、この値を変更できません。

セキュリティグループルールによっては、接続が追跡され、アウトバウンドエンドポイントからターゲットネームサーバーへの 1 秒あたりの最大クエリ数に影響する可能性があります。セキュリティグループによる接続の追跡を回避するには、「追跡されていない接続」を参照してください。

詳細については、Amazon VPC ユーザーガイドの「VPC のセキュリティグループ」を参照してください。

エンドポイントタイプ

エンドポイントのタイプは、IPv4、IPv6、デュアルスタック IP アドレスのいずれかです。デュアルスタックエンドポイントの場合、エンドポイントには、ネットワーク上の DNS リゾルバーが DNS クエリを転送できる IPv4 アドレスと IPv6 アドレスの両方があります。

> **Note**
>
> セキュリティ上の理由から、VPC Resolver はデフォルトですべてのデュアルスタック IP アドレスと IPv6 IP アドレスのパブリックインターネットへの IPv6 トラフィックの直接アクセスを拒否します。このアクセスを有効にするには、エンドポイントを作成または編集するときに IPv6 インターネットアクセスをオンにします。

IP アドレス

VPC Resolver がネットワーク上のリゾルバーに向かう途中で DNS クエリを に転送する VPC 内の IP アドレス。これらは、ネットワークの DNS リゾルバーの IP アドレスではありません。リ

ゾルバーの IP アドレスは、1 つ以上の VPC に関連付けるルールを作成するときに指定します。冗長性を確保するためには、少なくとも 2 つの IP アドレスを指定する必要があります。

> **Note**
>
> Resolver エンドポイントはプライベート IP アドレスを持ちます。これらの IP アドレスは、エンドポイントの存続期間中に変更されることはありません。

次の点に注意してください。

複数アベイラビリティーゾーン

少なくとも 2 つのアベイラビリティーゾーンで IP アドレスを指定することをお勧めします。必要に応じて、それらのアベイラビリティーゾーンまたは他のアベイラビリティーゾーンに追加の IP アドレスを指定できます。

IP アドレスと Amazon VPC Elastic Network Interface

指定したアベイラビリティーゾーン、サブネット、および IP アドレスの組み合わせごとに、VPC Resolver は Amazon VPC Elastic Network Interface を作成します。エンドポイントの IP アドレスあたりの 1 秒あたりの DNS クエリの現在の最大数については、「Route 53 VPC リゾルバーのクォータ」を参照してください。各 Elastic Network Interface の料金については、Amazon Route 53 料金ページの「Amazon Route 53」を参照してください。

IP アドレスの順序

IP アドレスは任意の順序で指定できます。DNS クエリを転送する場合、VPC Resolver は IP アドレスがリストされている順序に基づいて IP アドレスを選択しません。

IP アドレスごとに、以下の値を指定します。各 IP アドレスは、[VPC in the region-name Region (region-name リージョンの VPC)] で指定した VPC のアベイラビリティーゾーンに存在する必要があります。

アベイラビリティーゾーン

ネットワークに向かう途中で DNS クエリを通過させるアベイラビリティーゾーンです。指定したアベイラビリティーゾーンには、サブネットが設定されている必要があります。

サブネット

ネットワークに向かう途中で DNS クエリを通過させる IP アドレスが含まれているサブネットです。サブネットには使用可能な IP アドレスが必要です。

サブネット IP アドレスはエンドポイントタイプと一致する必要があります。

Outposts ラックでエンドポイントを作成するには、 AWS Outposts で VPC Resolver AWS を使用することをお勧めします。

> **Important**
>
> ローカルネットワークインターフェイス (LNI) が有効になっている Outposts サブネットは、VPC Resolver エンドポイントと互換性がありません。VPC Resolver エンドポイントの Elastic Network Interface (ENIs) を含むサブネットで LNI を有効にすると、それらの ENIs は機能しなくなります。詳細については、「Resolver エンドポイントのサブネット互換性」を参照してください。

IP アドレス

ネットワークに向かう途中で DNS クエリを通過させる IP アドレスです。

VPC Resolver で、指定したサブネットで使用可能な IP アドレスの中から IP アドレスを選択するか、自分で IP アドレスを指定するかを選択します。

IP アドレスを自分で指定することを選択した場合は、IPv4 か IPv6 のいずれか、または両方のアドレスを入力します。

プロトコル

エンドポイントプロトコルは、送信エンドポイントからのデータの送信方法を決定します。必要なセキュリティのレベルに応じて 1 つまたは複数のプロトコルを選択します。

- Do53: (デフォルト) データは、追加の暗号化なしで Route 53 VPC リゾルバーを使用してリレーされます。データは外部から読み取ることはできませんが、 AWS ネットワーク内では表示できます。
- DoH: データは暗号化された HTTPS セッションを介して送信されます。DoH は、権限のないユーザーがデータを復号化したり、目的の受信者以外がデータを読み取ったりできないようにするセキュリティレベルを高めます。

アウトバウンドエンドポイントには、以下のようにプロトコルを適用できます。

- Do53 と DoH　の組み合わせ。
- Do53 のみ。

- DoH のみ。
- なし。これは Do53 として扱われます。

IPv6 インターネットアクセス

IPv6 インターネットアクセスを有効にして、アウトバウンドエンドポイントがインターネットゲートウェイを介して DNS クエリをパブリック IPv6 ターゲットに転送できるようにします。有効にすると、エンドポイントの Elastic Network Interface (ENI) は DNS クエリをパブリック IPv6 リゾルバーに送信できます。

> **Important**
>
> IPv6 インターネットアクセスを有効にする場合は、セキュリティグループ、NACL、Egress-Only インターネットゲートウェイなどのネットワークコントロールを使用して、未承諾の入力トラフィックからエンドポイント ENI を保護します。一部のネットワークコントロールは、接続追跡により DNS クエリのスループットに影響する可能性があることに注意してください。詳細については、Amazon EC2 セキュリティグループ接続の追跡」と「リゾルバーエンドポイントのスケーリング」を参照してください。

タグ

1 つ以上のキーと対応する値を指定します。例えば、[Key (キー)] に Cost center を、[Value (値)] には 456 を指定します。

ルールを作成または編集するときに指定する値

転送ルールを作成または編集する場合、以下の転送値を指定します。

ルール名

わかりやすい名前にすると、ダッシュボードでルールを見つけやすくなります。

ルールタイプ

適用可能な値を選択します。

- Forward – 特定のドメイン名での DNS クエリをネットワークのリゾルバーに転送する場合は、このオプションを選択します。

- 委任 – プライベートホストゾーンでホストされているサブドメインの権限をオンプレミスのリゾルバー (または別の VPC の VPC リゾルバー) に委任する場合は、このオプションを選択します。
- システム – VPC Resolver で転送ルールで定義されている動作を選択的に上書きする場合は、このオプションを選択します。システムルールを作成すると、VPC リゾルバーは、ネットワーク上の DNS リゾルバーによって解決される、指定されたサブドメインの DNS クエリを解決します。

デフォルトでは、転送ルールはドメイン名とそのすべてのサブドメインに適用されます。ドメインのクエリをネットワークのリゾルバーに転送する際に、一部のサブドメインのクエリを除外する場合は、これらのサブドメインに対してシステムルールを作成します。例えば、example.com の転送ルールを作成する際に acme.example.com のクエリを転送しない場合は、システムルールを作成し、ドメイン名として acme.example.com を指定します。

委任レコード – 委任ルールのみ

このドメインに一致する DNS クエリは、ネットワーク上のリゾルバーに転送されます。

> **Note**
>
> 委任ルールの前提条件として、プライベートホストゾーンを使用してアウトバウンド委任を行う場合、プライベートホストゾーンに NS レコードを作成する必要があります。レコードは NS - 委任ルールを使用してリゾルバーアウトバウンドエンドポイントを介して委任するネームサーバーです。詳細については、「NS レコードタイプ」を参照してください。

このルールを使用する VPCs

このルールを使用して、指定したドメイン名の DNS クエリを転送する VPC です。ルールは、必要な数の VPCsに適用できます。

ドメイン名 – 転送ルールのみ

このドメイン名の DNS クエリは、[Target IP addresses (ターゲット IP アドレス)] で指定した IP アドレスに転送されます。例えば、特定のドメイン (example.com)、最上位ドメイン (com)、ドット (.) を指定して、すべての DNS クエリを転送できます。詳細については、「VPC Resolver がクエリ内のドメイン名がルールと一致するかどうかを判断する方法」を参照してください。

アウトバウンドエンドポイント

VPC Resolver は、ここで指定したアウトバウンドエンドポイントを介して、ターゲット IP アドレスで指定した IP アドレスに DNS クエリを転送します。

ターゲット IP アドレス

DNS クエリが [Domain name (ドメイン名)] で指定した名前と一致すると、アウトバウンドエンドポイントはここで指定した IP アドレスにクエリを転送します。これらは、通常、お客様環境上の DNS リゾルバーの IP アドレスです。

[Target IP addresses (ターゲット IP アドレス)] は、[Rule type (ルールタイプ)] の値が [Forward (転送)] である場合にのみ利用できます。

IPv4 または IPv6 アドレス、プロトコル、およびエンドポイントに使用する ServerNameIndication を指定します。ServerNameIndication は、選択したプロトコルが DoH の場合にのみ適用されます。

アウトバウンドエンドポイントを介したネットワーク上では DoH リゾルバーの FQDN のターゲット IP アドレスの解決はサポートされていません。アウトバウンドエンドポイントには、DoH クエリを転送するために、ネットワーク上の DoH リゾルバーのターゲット IP アドレスが必要です。ネットワーク上の DoH リゾルバーが TLS SNI および HTTP ホストヘッダーに FQDN を必要とする場合、ServerNameIndication を指定する必要があります。

ServerNameIndication

クエリを転送する DoH サーバーのサーバー名の表示。これは、プロトコルが DoH の場合にのみ使用されます。

タグ

1 つ以上のキーと対応する値を指定します。例えば、[Key (キー)] に Cost center を、[Value (値)] には 456 を指定します。

これらは、 が AWS 請求書を整理するために AWS Billing and Cost Management 提供するタグです。タグを使ったコスト配分の詳細については、AWS Billing ユーザーガイドのコスト配分タグの使用を参照してください。

アウトバウンドエンドポイントの管理

アウトバウンドエンドポイントを管理するには、該当する手順を実行します。

トピック

- アウトバウンドエンドポイントの表示と編集
- アウトバウンドエンドポイントのステータスの表示
- アウトバウンドエンドポイントの削除

アウトバウンドエンドポイントの表示と編集

アウトバウンドエンドポイントの設定を表示および編集するには、次の手順を実行します。

アウトバウンドエンドポイントの設定を表示および編集するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで、[Outbound endpoints (アウトバウンドエンドポイント)] を選択します。
3. ナビゲーションバーで、アウトバウンドエンドポイントを作成したリージョンを選択します。
4. 設定を表示または編集するエンドポイントのオプションを選択します。
5. [View details (詳細の表示)] または [Edit (編集)] を選択します。

   アウトバウンドエンドポイントの値の詳細については、「アウトバウンドエンドポイントを作成または編集するときに指定する値」を参照してください。
6. [Edit (編集)] を選択した場合は、該当する値を入力し、[Save (保存)] を選択します。

アウトバウンドエンドポイントのステータスの表示

アウトバウンドエンドポイントのステータスを表示するには、次の手順を実行します。

アウトバウンドエンドポイントのステータスを表示するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで、[Outbound endpoints (アウトバウンドエンドポイント)] を選択します。
3. ナビゲーションバーで、アウトバウンドエンドポイントを作成したリージョンを選択します。[Status] 列には、次のいずれかの値が表示されます。

作成

VPC Resolver は、このエンドポイントの 1 つ以上の Amazon VPC ネットワークインターフェイスを作成および設定しています。

運用中

このエンドポイントの Amazon VPC ネットワークインターフェイスが正しく設定されており、ネットワークと VPC Resolver 間でインバウンドまたはアウトバウンドの DNS クエリを渡すことができます。

[更新中]

VPC Resolver は、1 つ以上のネットワークインターフェイスをこのエンドポイントに関連付けまたは関連付け解除しています。

自動復旧中

VPC Resolver は、このエンドポイントに関連付けられている 1 つ以上のネットワークインターフェイスを復旧しようとしています。復旧プロセス中は、IP アドレスごと (ネットワークインターフェイスごと) の DNS クエリの数の制限により、エンドポイントは容量が制限された状態で機能します。現在の制限については、「Route 53 VPC リゾルバーのクォータ」を参照してください。

Action needed (アクションが必要)

このエンドポイントは異常であり、VPC Resolver は自動的に復旧できません。この問題を解決するには、エンドポイントに関連付けした各 IP アドレスを確認することをお勧めします。使用できない IP アドレスごとに別の IP アドレスを追加して、使用できない IP アドレスを削除します。(エンドポイントには常に少なくとも 2 つの IP アドレスが含まれている必要があります。) [必要なアクション] のステータスにはさまざまな原因が考えられます。一般的な 2 つの原因を以下に示します。

- エンドポイントに関連付けられている、1 つまたは複数のネットワークインターフェイスが、Amazon VPC を使用して削除されました。
- VPC Resolver のコントロール外にある何らかの理由により、ネットワークインターフェイスを作成できませんでした。

削除

VPC Resolver はこのエンドポイントと関連するネットワークインターフェイスを削除しています。

アウトバウンドエンドポイントの削除

エンドポイントを削除する前に、VPC に関連付けられているルールをすべて削除する必要があります。

アウトバウンドエンドポイントを削除するには、次の手順を実行します。

> **Important**
>
> アウトバウンドエンドポイントを削除すると、VPC Resolver は、削除されたアウトバウンドエンドポイントを指定するルールについて、VPC からネットワークへの DNS クエリの転送を停止します。

アウトバウンドエンドポイントを削除するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで、[Outbound endpoints (アウトバウンドエンドポイント)] を選択します。
3. ナビゲーションバーで、アウトバウンドエンドポイントを作成したリージョンを選択します。
4. 削除するエンドポイントのオプションを選択します。
5. [Delete (削除)] を選択します。
6. エンドポイントの削除を確定するには、エンドポイントの名前を入力し、[Submit (送信)] を選択します。

転送ルールの管理

VPC Resolver で指定されたドメイン名のクエリをネットワークに転送する場合は、ドメイン名ごとに 1 つの転送ルールを作成し、クエリを転送するドメインの名前を指定します。

トピック

- 転送ルールの表示と編集
- 転送ルールの作成
- 逆引き参照のルールの追加
- 転送ルールと VPC の関連付け

- 転送ルールと VPC の関連付けの解除
- Resolver ルールを他の AWS アカウントと共有し、共有ルールを使用する
- 転送ルールの削除
- VPC Resolver でのリバース DNS クエリの転送ルール

転送ルールの表示と編集

転送ルールの設定を表示および編集するには、次の手順を実行します。

転送ルールの設定を表示および編集するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [ルール] を選択します。
3. ナビゲーションバーで、転送ルールを作成したリージョンを選択します。
4. 設定を表示または編集する転送ルールのオプションを選択します。
5. [View details (詳細の表示)] または [Edit (編集)] を選択します。

   転送ルールの値の詳細については、「ルールを作成または編集するときに指定する値」を参照してください。
6. [Edit (編集)] を選択した場合は、該当する値を入力し、[Save (保存)] を選択します。

転送ルールの作成

1 つまたは複数の転送ルールを作成するには、次の手順を実行します。

転送ルールを作成して 1 つ以上の VPC に関連付けるには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [ルール] を選択します。
3. ナビゲーションバーで、転送ルールを作成するリージョンを選択します。
4. [Create rule] を選択します。
5. 適切な値を入力します。詳細については、「ルールを作成または編集するときに指定する値」を参照してください

6. [Save] を選択します。
7. さらにルールを追加するには、ステップ 4 ~ 6 を繰り返します。

逆引き参照のルールの追加

VPC での逆引き参照を制御する必要がある場合は、アウトバウンドリゾルバーのエンドポイントにルールを追加します。

逆引き参照のルールを作成するには

1. 前出の手順で、ステップ 5 までを完了します。
2. ルールを定義する際に、IP アドレスの PTR レコード、もしくは逆引き参照の転送ルールを適用するアドレスを入力します。

   例えば、10.0.0.0/23 の範囲内のアドレスに対する参照を転送したい場合は、以下の 2 つのルールを入力します。

   - 0.0.10.in-addr.arpa
   - 1.0.10.in-addr.arpa

   これらのサブネット内のすべての IP アドレスは、これらの PTR レコードのサブドメインとして参照されます。例えば、10.0.1.161 は逆引き参照アドレスとして 161.1.0.10.in-addr.apra を持ちます。このアドレスは 1.0.10.in-addra.arpa のサブドメインです。
3. これらの参照を転送するサーバーを指定します。
4. アウトバウンドリゾルバーのエンドポイントに、作成したルールを追加します。

VPC の enableDNSHostNames をオンにすると、PTR レコードが自動的に追加されることに注意してください。「Route 53 VPC Resolver とは」を参照してください。前述の手順は、特定の IP 範囲に対してリゾルバーを明示的に指定する (例えばアクティブディレクトリサーバーにクエリを転送する) 場合にのみ必要です。

転送ルールと VPC の関連付け

転送ルールを作成したら、それを 1 つ以上の VPC に関連付ける必要があります。ルールは、VPC に関連付けられた後にのみ機能します。ルールを VPC に関連付けると、VPC リゾルバーは、ルールで指定されたドメイン名の DNS クエリを、ルールで指定された DNS リゾルバーに転送し始めます。クエリは、ルールの作成時に指定したアウトバウンドエンドポイントを通過します。

転送ルールを 1 つ以上の VPC に関連付けるには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [ルール] を選択します。
3. ナビゲーションバーで、転送ルールを作成したリージョンを選択します。
4. 1 つまたは複数の VPC に関連付けるルールの名前を選択します。
5. [Associate VPC] を選択します。
6. [このルールを使用する VPC] で、ルールを関連付ける VPC を選択します。
7. [Add] を選択します。

転送ルールと VPC の関連付けの解除

以下の場合は、転送ルールと VPC の関連付けを解除します。

- この VPC から送信される DNS クエリの場合、VPC Resolver でルールで指定されたドメイン名のクエリのネットワークへの転送を停止する必要があります。
- 転送ルールを削除する場合。ルールが現在 1 つ以上の VPC に関連付けられている場合は、ルールを削除する前に、すべての VPC からルールの関連付けを解除する必要があります。

1 つ以上の VPC からルールの関連付けを解除する場合は、次の手順を実行します。

転送ルールと VPC の関連付けを解除するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [ルール] を選択します。
3. ナビゲーションバーで、転送ルールを作成したリージョンを選択します。
4. 1 つ以上の VPC から関連付けを解除するルールの名前を選択します。
5. ルールの関連付けを解除する VPC のオプションを選択します。
6. [関連付け解除] を選択します。
7. 「disassociate」と入力して確定します。
8. [Submit] を選択します。

Resolver ルールを他の AWS アカウントと共有し、共有ルールを使用する

1 つの AWS アカウントを使用して作成した Resolver ルールを他の AWS アカウントと共有できます。ルールを共有するには、Route 53 VPC Resolver コンソールを AWS Resource Access Manager と統合します。Resource Access Manager の詳細については、Resource Access Manager ユーザーガイドを参照してください。

次の点に注意してください。

共有ルールと VPC の関連付け

別の AWS アカウントが 1 つ以上のルールをアカウントと共有している場合、作成したルールを VPCs に関連付けるのと同じ方法で、ルールを VPCsに関連付けることができます。詳細については、「転送ルールと VPC の関連付け」を参照してください。

ルールの削除または共有解除

ルールを他のアカウントと共有してからルールを削除するか、共有を停止し、そのルールが 1 つ以上の VPCs に関連付けられている場合、Route 53 VPC Resolver は残りのルールに基づいてそれらの VPCsの DNS クエリの処理を開始します。この動作は、ルールと VPC の関連付けを解除する場合と同じです。

ルールが組織単位 (OU) と共有され、その OU 内のアカウントが別の OU に移動された場合、そのアカウント内の VPC に対する共有ルールとの関連付けはすべて削除されます。ただし、VPC リゾルバールールが送信先 OU とすでに共有されている場合、VPC の関連付けは変更されず、関連付けが解除されません。

ルールと関連付けの最大数

アカウントがルールを作成し、他の 1 つ以上のアカウントと共有する場合、 AWS リージョンあたりのルールの最大数は、ルールを作成したアカウントに適用されます。

ルールを共有しているアカウントが、このルールを 1 つ以上の VPC に関連付ける場合は、リージョンあたりのルールと VPC の関連付けの最大数が、ルールを共有しているアカウントに適用されます。

現在の VPC リゾルバーのクォータについては、「」を参照してくださいRoute 53 VPC リゾルバーのクォータ。

アクセス許可

ルールを別の AWS アカウントと共有するには、PutResolverRulePolicy アクションを使用するアクセス許可が必要です。

ルールが共有されている AWS アカウントの制限

ルールを共有するアカウントは、ルールを変更または削除できません。

タグ付け

ルールを作成したアカウントのみが、ルールのタグを追加、削除、または表示できます。

ルールの現在の共有ステータス (ルールを共有したアカウントやルールの共有先であるアカウントなど) を確認し、別のアカウントとルールを共有するには、以下の手順を実行します。

共有ステータスを表示し、別の AWS アカウントとルールを共有するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [ルール] を選択します。
3. ナビゲーションバーで、転送ルールを作成したリージョンを選択します。

   [Sharing status (共有ステータス)] 列に、現在のアカウントで作成されたルールまたは現在のアカウントと共有されているルールの現在の共有ステータスが表示されます。

   - Not shared: 現在の AWS アカウントがルールを作成し、そのルールは他のアカウントと共有されません。
   - Shared by me (自分が共有): 現在のアカウントがルールを作成し、1 つ以上の他のアカウントと共有しています。
   - Shared with me (自分と共有): 別のアカウントがルールを作成し、現在のアカウントと共有しています。
4. 共有情報を表示するルールまたは別のアカウントと共有するルールの名前を選択します。

   [Rule: ***rule name*** (ルール: rule name)] ページで、[Owner (所有者)] の値として、ルールを作成したアカウントの ID が表示されます。これは現在のアカウントです。ただし、[Sharing status (共有ステータス)] の値が [Shared with me (自分と共有)] である場合を除きます。その場合の [Owner (所有者)] は、ルールを作成して現在のアカウントと共有しているアカウントです。
5. [Share (共有)] を選択し、追加情報を表示するか、別のアカウントとルールを共有します。[Sharing status (共有ステータス)] の値に応じたページが Resource Access Manager コンソールに表示されます。

- Not shared (未共有): [Create resource share (リソース共有の作成)] ページが表示されます。別のアカウント、OU、または組織とルールを共有する方法については、ステップ 6 に進んでください。
- Shared by me (自分が共有): [Shared resources (共有リソース)] ページに、現在のアカウントが所有し、他のアカウントと共有しているルールと他のリソースが表示されます。
- Shared with me (自分と共有): [Shared resources (共有リソース)] ページに、他のアカウントが所有し、現在のアカウントと共有しているルールと他のリソースが表示されます。

6. ルールを別の AWS アカウント、OU、または組織と共有するには、次の値を指定します。

> **Note**
>
> 共有設定を更新することはできません。以下のいずれかの設定を変更する場合は、新しい設定を使用してルールを共有し直し、古い共有設定を削除する必要があります。

説明

ルールを共有した理由を示す短い説明を入力します。

リソース

共有するルールのチェックボックスをオンにします。

プリンシパル

AWS アカウント番号、OU 名、または組織名を入力します。

タグ

1 つ以上のキーと対応する値を指定します。例えば、[Key (キー)] に Cost center を、[Value (値)] には 456 を指定します。

これらは、 が AWS 請求書を整理するために AWS Billing and Cost Management 提供するタグです。他の目的でタグを使用することもできます。タグを使ったコスト配分の詳細については、AWS Billing ユーザーガイドのコスト配分タグの使用を参照してください。

転送ルールの削除

転送ルールを削除するには、次の手順を実行します。

次の点に注意してください。

- 次のルールと関連付けられている VPC がある場合は、ルールを削除する前に、VPC からルールの関連付けを解除する必要があります。詳細については、「転送ルールと VPC の関連付けの解除」を参照してください
- [Internet Resolver (インターネットリゾルバ)] では、デフォルトの ([Type (タイプ)] 値が [Recursive (再帰的)] となっている) ルールは削除できません。このルールにより、Route 53 VPC Resolver は、カスタムルールを作成せず、VPC Resolver が自動定義ルールを作成しなかったドメイン名の再帰的なリゾルバーとして機能します。ルールが分類される方法の詳細については、「ネットワークに転送するクエリをルールでコントロールする」を参照してください。

転送ルールを削除するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [ルール] を選択します。
3. ナビゲーションバーで、転送ルールを作成したリージョンを選択します。
4. 削除するルールのオプションを選択します。
5. [Delete (削除)] を選択します。
6. ルールの削除を確定するには、ルールの名前を入力し、[Submit (送信)] を選択します。

VPC Resolver でのリバース DNS クエリの転送ルール

Amazon VPC の Virtual Private Cloud (VPC) `true`に対して `enableDnsHostnames`と が に設定されている場合、VPC Resolver `enableDnsSupport`はリバース DNS クエリの自動定義システムルールを自動的に作成します。これらの設定の詳細については、Amazon VPC デベロッパーガイドの VPC の DNS 属性を参照してください。

逆引き DNS クエリの転送ルールは、SSH やActive Directory などのサービスで特に役立ちます。これらのサービスでは、お客様がリソースに接続しようとしている IP アドレスについて逆引き DNS ルックアップを実行してユーザーを認証するオプションが用意されています。自動定義されたシステムルールの詳細については、VPC Resolver が自動定義されたシステムルールを作成するドメイン名を参照してください。

これらのルールをオフにし、すべての逆引き DNS クエリを変更して、例えば、解決のためにオンプレミスのネームサーバーにこれらが転送されるようにすることができます。

自動ルールをオフにした後、必要に応じてオンプレミスリソースにクエリを転送するルールを作成します。転送ルールの管理方法の詳細については、「転送ルールの管理」を参照してください。

自動定義ルールをオフにするには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインの VPC Resolver で VPCs、VPC ID を選択します。
3. [Autodefined rules for reverse DNS resolution] (逆引き DNS 解決の自動定義ルール) で、チェックボックスの選択を解除します。チェックボックスの選択が既に解除されている場合は、チェックボックスを選択して、自動定義された逆引き DNS 解決をオンにすることができます。

関連する APIs「VPC リゾルバー設定 APIs」を参照してください。

リゾルバーの委任ルールのチュートリアル

委任ルールにより、VPC Resolver は指定されたアウトバウンドエンドポイントを介して委任ゾーンをホストするネームサーバーに到達できます。転送ルールは、DNS クエリをアウトバウンドエンドポイントを介して指定されたドメインに一致するネームサーバーに転送するように VPC リゾルバーに通知しますが、委任ルールは、委任 NS レコードが返されたときに指定されたアウトバウンドエンドポイントを介して委任ネームサーバーに到達するように VPC リゾルバーに通知します。VPC Resolver は、DNS レスポンスの NS レコードが委任レコードで指定されたドメイン名と一致すると、委任ネームサーバーにクエリを送信します。

Resolver エンドポイントのアウトバウンド委任を使用するステップ

1. DNS クエリの送信元の VPC に、ネットワーク上のリゾルバーへのリゾルバーアウトバウンドエンドポイントを作成します。

   次の API または CLI コマンドを使用できます。

   - `CreateResolverEndpoint API`
   - `create-resolver-endpoint CLI`
2. 指定されたアウトバウンドエンドポイントを介してクエリをネットワークに委任するドメイン名を指定する 1 つ以上の委任ルールを作成します。

   CLI を使用した委任ルールの作成例:

```
aws route53resolver create-resolver-rule \
--region REGION \
--creator-request-id delegateruletest \
--delegation-record example.com \
--name delegateruletest \
--rule-type DELEGATE \
--resolver-endpoint-id outbound endpoint ID
```

3. クエリを委任する VPC に委任ルールを関連付けます。

   次の API または CLI コマンドを使用できます。

   - AssociateResolverRule API。
   - associate-resolver-rules CLI コマンド。

Resolver アウトバウンドエンドポイントでサポートされている委任のタイプ

VPC Resolver は、次の 2 種類のアウトバウンド委任をサポートしています。

- Route 53 プライベートホストゾーンから VPC Resolver へのアウトバウンド委任:

  アウトバウンド委任を使用して、プライベートホストゾーンからインターネット上のオンプレミス DNS サーバーまたはパブリックホストゾーンにサブドメインを委任します。このアウトバウンド委任により、プライベートホストゾーンと委任ゾーン間で DNS レコードの管理を分割できます。委任は、DNS 設定に基づいてプライベートホストゾーンのグルーレコードの有無にかかわらず行うことができます。詳細については「プライベートホストゾーンからアウトバウンドへ」を参照してください。

- VPC リゾルバーのアウトバウンドからアウトバウンドへの委任:

  アウトバウンドからアウトバウンドへの委任を使用して、オンプレミス DNS サーバーから同じ場所または異なる場所にある別のオンプレミスサーバーにサブドメインを委任します。これは、プライベートホストゾーンからアウトバウンドエンドポイントに委任する場合に似ており、オンプレミスのネームサーバーでホストされているゾーンに委任できます。詳細については、「アウトバウンドからアウトバウンドへ」を参照してください。

Route 53 プライベートホストゾーンから VPC Resolver へのアウトバウンド委任の設定例

親ホストゾーンが Amazon VPC の Route 53 プライベートホストゾーンでホストされ、サブドメインが欧州、アジア、北米でホストされているネームサーバーに委任されている DNS 設定を考えてみます。すべての DNS クエリは VPC リゾルバーを介して渡されます。

手順に従って、プライベートホストゾーンと VPC リゾルバーを設定します。

アウトバウンド委任のプライベートホストゾーンを設定する

1. プライベートホストゾーンのセットアップの場合:

   親ホストゾーン: `hr.example.com`

   ```
   $TTL    86400 ; 24 hours
   $ORIGIN hr.example.com
   @  1D  IN     SOA @    root (20200322001 3H 15 1w 3h)
   @  1D  IN  NS @
   eu.hr.example.com IN NS ns1.eu.hr.example.com.
   apac.hr.example.com IN NS ns2.apac.hr.example.com.
   na.hr.example.com IN NS ns3.na.hr.example.net. # Out of Zone Delegation

   ns1.eu.hr.example.com IN A 10.0.0.30 # Glue Record
   ns2.apac.hr.example.com IN A 10.0.0.40 # Glue Record
   ```

2. 欧州のオンプレミスリージョンのオンプレミスネームサーバーの場合:

   - ホストゾーン: `eu.hr.example.com` NS IP: `10.0.0.30`

   ```
   $TTL    86400 ; 24 hours
   $ORIGIN eu.hr.example.com
   @  1D  IN     SOA @    root (20200322001 3H 15 1w 3h)
   @  1D  IN  NS @

   test.eu.hr.example.com IN A 1.2.3.4
   ```

3. アジアのオンプレミスリージョンのオンプレミスネームサーバーの場合:

   ホストゾーン: `apac.hr.example.com`、`10.0.0.40`

   apac ネームサーバーは、サブドメインを他のネームサーバーに委任できます。

```
$TTL    86400 ; 24 hours
$ORIGIN apac.hr.example.com
@  1D  IN     SOA @    root (20200322001 3H 15 1w 3h)
@  1D  IN  NS @

test.apac.hr.example.com IN A 5.6.7.8
engineering.apac.hr.example.com IN NS ns1.engineering.apac.hr.example.com
sales.apac.hr.example.com IN NS ns2.sales.apac.hr.example.com
ns1.engineering.apac.hr.example.com IN A 10.0.0.80
ns2.sales.apac.hr.example.com IN A 10.0.0.90
```

ホストゾーン: engineering.apac.hr.example.com、10.0.0.80

```
$TTL 86400 ; 24 hours
$ORIGIN engineering.apac.hr.example.com
@ 1D IN SOA @ root (20200322001 3H 15 1w 3h)
@ 1D IN NS @
test.engineering.apac.hr.example.com IN A 1.1.1.1
```

4. 北米のオンプレミスリージョンのオンプレミスネームサーバーの場合:

   ホストゾーン: na.hr.example.net NS IP: 10.0.0.50

```
$TTL    86400 ; 24 hours
$ORIGIN na.hr.example.net
@  1D  IN     SOA @    root (20200322001 3H 15 1w 3h)
@  1D  IN  NS @
ns3.na.hr.example.net. IN A 10.0.0.50
test.na.hr.example.com  IN A 9.10.11.12
```

VPC リゾルバーのセットアップ

- VPC リゾルバーでは、1 つのフォワードルールと 2 つの委任ルールを設定する必要があります。

  転送ルール

  1. ゾーンout-of-zone委任レコードを転送する場合、Route 53 VPC Resolver は最初のリクエストを転送する委任 NS の IP を認識します。

domain-name: hr.example.net target-ips: 10.0.0.50

委任ルール

1. ゾーン内の委任の委任ルール:

   委任レコード: hr.example.com
2. ゾーン外の委任の委任ルール:

   委任レコード: hr.example.net

アウトバウンドからアウトバウンドへの委任の設定例

親ホストゾーンを Amazon VPC に配置する代わりに、親ホストゾーンが中央のオンプレミスロケーションにあり、サブドメインが欧州、アジア、北米でホストされているネームサーバーに委任されている DNS 設定を考えてみます。すべての DNS クエリは VPC リゾルバーを介して渡されます。

手順に従って、オンプレミス DNS と VPC リゾルバーを設定します。

オンプレミス DNS を設定する

1. 中央のオンプレミスリージョンのオンプレミスネームサーバーの場合:

   - 親ホストゾーン: hr.example.com

     ホストゾーン hr.example.com、NS IP: 10.0.0.20

```
$TTL    86400 ; 24 hours
$ORIGIN hr.example.com
@  1D  IN     SOA @    root (20200322001 3H 15 1w 3h)
@  1D  IN  NS @
eu.hr.example.com IN NS ns1.eu.hr.example.com.
apac.hr.example.com IN NS ns2.apac.hr.example.com.
na.hr.example.com IN NS ns3.na.hr.example.net. # Out of zone delegation

ns1.eu.hr.example.com IN A 10.0.0.30 # Glue record
ns2.apac.hr.example.com IN A 10.0.0.40 # Glue record
```

2. 欧州のオンプレミスリージョンのオンプレミスネームサーバーの場合 (欧州、アジア、北米のネームサーバーの設定は、プライベートホストゾーンからアウトバウンドへの委任の場合と同じ)。

   - ホストゾーン: eu.hr.example.com NS IP: 10.0.0.30

```
$TTL    86400 ; 24 hours
$ORIGIN eu.hr.example.com
@  1D  IN     SOA @    root (20200322001 3H 15 1w 3h)
@  1D  IN  NS @

test.eu.hr.example.com IN A 1.2.3.4
```

3. アジアのオンプレミスリージョンのオンプレミスネームサーバーの場合:

   ホストゾーン: apac.hr.example.com、10.0.0.40

   apac ネームサーバーは、サブドメインを他のネームサーバーに委任できます。

```
$TTL    86400 ; 24 hours
$ORIGIN apac.hr.example.com
@  1D  IN     SOA @    root (20200322001 3H 15 1w 3h)
@  1D  IN  NS @

test.apac.hr.example.com IN A 5.6.7.8
engineering.apac.hr.example.com IN NS ns1.engineering.apac.hr.example.com
sales.apac.hr.example.com IN NS ns2.sales.apac.hr.example.com
ns1.engineering.apac.hr.example.com IN A 10.0.0.80
ns2.sales.apac.hr.example.com IN A 10.0.0.90
```

   ホストゾーン: engineering.apac.hr.example.com、10.0.0.80

```
$TTL 86400 ; 24 hours
$ORIGIN engineering.apac.hr.example.com
@ 1D IN SOA @ root (20200322001 3H 15 1w 3h)
@ 1D IN NS @
test.engineering.apac.hr.example.com IN A 1.1.1.1
```

4. 北米のオンプレミスリージョンのオンプレミスネームサーバーの場合:

   ホストゾーン: na.hr.example.net NS IP: 10.0.0.50

```
$TTL    86400 ; 24 hours
$ORIGIN na.hr.example.net
@  1D  IN     SOA @    root (20200322001 3H 15 1w 3h)
@  1D  IN  NS @
ns3.na.hr.example.net. IN A 10.0.0.50
test.na.hr.example.com  IN A 9.10.11.12
```

VPC リゾルバーのセットアップ

- VPC リゾルバーでは、フォワードルールと委任ルールを設定する必要があります。

  転送ルール

  1. クエリが中央ロケーションの親ホストゾーン hr.example.com に転送されるように最初のリクエストを転送するには:

     domain-name: hr.example.com target-ips: 10.0.0.20
  2. ゾーンout-of-zone委任レコードを転送する場合、VPC リゾルバーは、最初のリクエストを転送する委任ネームサーバーの IP アドレスを認識します。

     domain-name: hr.example.net target-ips: 10.0.0.50

  委任ルール

  1. ゾーン内の委任の委任ルール:

     委任レコード: hr.example.com
  2. ゾーン外の委任の委任ルール:

     委任レコード: hr.example.net

Amazon Route 53 での DNSSEC 検証の有効化

Amazon Route 53 で Virtual Private Cloud (VPC) の DNSSEC 検証を有効にすると、DNSSEC 署名が暗号的にチェックされ、レスポンスが改ざんされていないことを確認します。DNSSEC 検証の有効化は、VPC の詳細ページから行います。

DNSSEC 検証は、再帰的な DNS 解決を実行するときに、VPC Resolver によってパブリック署名名に適用されます。

ただし、VPC リゾルバーが別の DNS リゾルバーに転送されている場合、そのリゾルバーは再帰的な DNS 解決を実行しているため、DNSSEC 検証も適用する必要があります。

> **Important**
>
> DNSSEC 検証を有効にすると、VPC 内の AWS リソースから送られるパブリック DNS レコードの DNS 解決が影響を受け、この機能が停止する可能性があります。DNSSEC 検証の有効化および無効化には、数分かかる場合があります。

> **Note**
>
> 現時点では、VPC の Route 53 VPC Resolver (別名 AmazonProvidedDNS) は、DNS クエリの DO (DNSSEC OK) EDNS ヘッダービットと CD (Checking Disabled) ビットを無視します。DNSSEC を設定している場合、VPC リゾルバーは DNSSEC 検証を実行している間、DNSSEC レコードを返したり、レスポンスに AD ビットを設定したりしません。したがって、独自の DNSSEC 検証の実行は現在、VPC リゾルバーではサポートされていません。これを行う必要がある場合は、独自の再帰的な DNS 解決を実行する必要があります。

VPC のために DNSSEC 検証を有効にするには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインの VPC Resolver で、VPCsを選択します。
3. [DNSSEC 検証] でチェックボックスをオンにします。チェックボックスが既にオンになっている場合は、オフにすると、DNSSEC 検証を無効にすることができます。

   DNSSEC 検証の有効化および無効化には、数分かかる場合があります。

AWS リソースへのインターネットトラフィックのルーティング

Amazon Route 53 を使用して、さまざまな AWS リソースにトラフィックをルーティングできます。

- ドメイン名を使用してトラフィックを Amazon API Gateway の API にルーティングする
- ドメイン名を使用したトラフィックの Amazon CloudFront ディストリビューションへのルーティング
- Amazon EC2 インスタンスへのトラフィックのルーティング
- AWS App Runner サービスへのトラフィックのルーティング
- へのトラフィックのルーティング AWS Global Accelerator
- AWS Elastic Beanstalk 環境へのトラフィックのルーティング
- ELB ロードバランサーへのトラフィックのルーティング
- Amazon S3 バケットでホストされているウェブサイトへのトラフィックのルーティング
- ドメイン名を使用してトラフィックを Amazon Virtual Private Cloud インターフェイスエンドポイントにルーティングする
- Amazon WorkMail へのトラフィックのルーティング
- Amazon OpenSearch Service ドメインエンドポイントへのトラフィックのルーティング
- Amazon VPC Lattice サービスドメインエンドポイントへのトラフィックのルーティング
- 他の AWS リソースへのトラフィックのルーティング
- を使用した Amazon Route 53 および Route 53 VPC Resolver リソースの作成 AWS CloudFormation

ドメイン名を使用してトラフィックを Amazon API Gateway の API にルーティングする

API を作成、発行、管理、モニタリング、保護するために、Amazon API Gateway を使用できます。AWS クラウドに保存されているデータに加えて、 AWS サービスまたは他のウェブサービスにアクセスする APIs を作成できます。

ドメイントラフィックを API Gateway API にルーティングするために使用する方法は、リージョン API Gateway エンドポイントとエッジ最適化 API Gateway エンドポイントのどちらを作成したかに関係なく同じです。プライベート API Gateway エンドポイントを作成する場合、プロセスは若干異なります。

- リージョン API エンドポイント: リージョン API エンドポイントにトラフィックをルーティングする Route 53 エイリアスレコードを作成します。
- エッジ最適化 API エンドポイント: エッジ最適化 API にトラフィックをルーティングする Route 53 エイリアスレコードを作成します。これにより、エッジ最適化 API に関連付けられた CloudFront ディストリビューションにトラフィックがルーティングされます。
- プライベート API エンドポイント: プライベートホストゾーンの API Gateway のインターフェイス VPC エンドポイントを使用して、プライベート API エンドポイントにトラフィックをルーティングする Route 53 エイリアスレコードを作成します。

エイリアスレコードは、CNAME レコードに似た DNS の Route 53 拡張機能です。エイリアスレコードと CNAME レコードの比較については、「エイリアスレコードと非エイリアスレコードの選択」を参照してください。

> **Note**
>
> Route 53 では、API Gateway APIs やその他の AWS リソースへのエイリアスクエリには課金されません。

トピック

- 前提条件
- トラフィックを API Gateway エンドポイントにルーティングするための Route 53 の設定

前提条件

使用開始には、以下が必要です。

- 作成する Route 53 レコードの名前と一致するカスタムドメイン名 (api.example.com など) を含む API Gateway API。

  詳細については、以下の各トピックを参照してください。

  - Amazon API Gateway デベロッパーガイドの HTTP API のカスタムドメイン名の設定。
  - Amazon API Gateway デベロッパーガイドの REST API のカスタムドメイン名の設定。
  - Amazon API Gateway デベロッパーガイドの WebSocket API のカスタムドメイン名の設定。
  - Amazon API Gateway デベロッパーガイドのAPI Gateway でのプライベート API 用のカスタムドメイン名。
- 登録済みドメイン名 ドメインレジストラとして、Amazon Route 53 を使用することも、あるいは別のレジストラを使用することもできます。
- ドメインの DNS サービスとしての Route 53。Route 53 を使用してドメイン名を登録した場合、Route 53 をドメインの DNS サービスとして自動的に設定します。

  Route 53 をドメインの DNS サービスプロバイダとして使用する方法の詳細については、「Amazon Route 53 を既存ドメインの DNS サービスとして使用する」を参照してください。

トラフィックを API Gateway エンドポイントにルーティングするための Route 53 の設定

トラフィックを API Gateway エンドポイントにルーティングするように Route 53 を設定するには、以下の手順を実行します。

Custom domain names for public APIs

次の手順では、パブリック API のカスタムドメイン名の APIs Gateway エンドポイントにトラフィックをルーティングする方法について説明します。

API Gateway エンドポイントにトラフィックをルーティングするには

1. 同じアカウントを使用して Route 53 ホストゾーンとエンドポイントを作成した場合は、ステップ 2 に進みます。

   異なるアカウントを使用してホストゾーンとエンドポイントを作成した場合は、使用するカスタムドメイン名のターゲットドメイン名を取得します。

   a. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/apigateway/ で API Gateway コンソールを開きます。
   b. ナビゲーションペインで、[Custom domain names] を選択します。
   c. 使用するカスタムドメイン名について、[API Gateway ドメイン名] の値を取得します。
2. Route 53 コンソール (https://console.aws.amazon.com/route53/) を開きます。

3. ナビゲーションペインで [Hosted zones] を選択します。
4. API へのトラフィックのルーティングに使用するドメイン名があるホストゾーンの名前を選択します。
5. [Create record (レコードを作成)] を選択します。
6. 次の値を指定します。

> **Important**
>
> エイリアスを有効にすることをお勧めします。Route 53 エイリアスレコードを使用しないドメイン名では、プライベート DNS が有効になっている VPC を使用してプライベート API を呼び出した場合、問題が発生する可能性があります。プライベート DNS は、VPC 内のデフォルトの DNS 解決動作をオーバーライドします。それによって、外部 DNS レコードとの競合が発生する可能性があります。

ルーティングポリシー

該当するルーティングポリシーを選択します。詳細については、「ルーティングポリシーの選択」を参照してください

レコード名

API へのトラフィックのルーティングに使用するドメイン名を入力します。

トラフィックのルーティング先の API では、Route 53 レコードの名前と一致するカスタムドメイン名 (api.example.com など) を指定する必要があります。

エイリアス

クイック作成レコード作成方法を使用している場合、[エイリアス] をオンにします。

値/トラフィックのルーティング先

[API Gateway API へのエイリアス]を選択し、さらにエンドポイントの元のリージョンを選択します。

Endpoint の値を指定する方法は、同じ AWS アカウントまたは異なるアカウントを使用してホストゾーンと API を作成したかどうかによって異なります。

- 同じアカウント – ターゲットドメイン名のリストには、[レコード名] に指定した値と一致するカスタムドメイン名を含む API のみが示されます。該当する値を選択します。

- 異なるアカウント – この手順のステップ 1 で取得した値を入力します。

レコードタイプ

[A – IPv4 address (A – IPv4 address)] を選択します。

ターゲットの正常性の評価

DNS フェイルオーバーを制御するには、カスタムヘルスチェックを設定します。例については、「API Gateway ユーザーガイド」の「Configure custom health checks for DNS failover」(DNS フェイルオーバーのカスタムヘルスチェックの設定) を参照してください。

7. [レコードを作成] を選択します。

通常、変更は 60 秒以内にすべての Route 53 サーバーに伝播されます。伝達が完了すると、この手順で作成したエイリアスレコードの名前を使用して、トラフィックを API にルーティングできるようになります。

Custom domain names for private APIs

次の手順では、プライベート API のカスタムドメイン名の API Gateway エンドポイントにトラフィックをルーティングする方法について説明します。

API Gateway エンドポイントにトラフィックをルーティングするには

1. Route 53 コンソール (https://console.aws.amazon.com/route53/) を開きます。
2. ナビゲーションペインで [Hosted zones] を選択します。
3. API へのトラフィックのルーティングに使用するドメイン名があるプライベートホストゾーンの名前を選択します。
4. [Create record (レコードを作成)] を選択します。
5. 次の値を指定します。

ルーティングポリシー

該当するルーティングポリシーを選択します。詳細については、「ルーティングポリシーの選択」を参照してください

レコード名

API へのトラフィックのルーティングに使用するドメイン名を入力します。

トラフィックのルーティング先の API では、Route 53 レコードの名前と一致するカスタムドメイン名 (api.example.com など) を指定する必要があります。

エイリアス

エイリアスをオンにします。

値/トラフィックのルーティング先

[Alias to VPC Endpoint] (VPC エンドポイントへのエイリアス) を選択します。エンドポイントの送信元のリージョンを選択し、VPC エンドポイントを選択します。

レコードタイプ

VPC エンドポイントに IPv6 を使用している場合は、AAAA レコードタイプを作成します。VPC エンドポイントにデュアルスタックを使用している場合は、AAAA レコードタイプと A レコードタイプの両方を作成します。

ターゲットの正常性の評価

DNS フェイルオーバーを制御するには、カスタムヘルスチェックを設定します。例については、「API Gateway ユーザーガイド」の「Configure custom health checks for DNS failover」(DNS フェイルオーバーのカスタムヘルスチェックの設定) を参照してください。

6. [レコードを作成] を選択します。

通常、変更は 60 秒以内にすべての Route 53 サーバーに伝播されます。伝達が完了すると、この手順で作成したエイリアスレコードの名前を使用して、トラフィックを API にルーティングできるようになります。

ドメイン名を使用したトラフィックの Amazon CloudFront ディストリビューションへのルーティング

このトピックでは、DNS トラフィックを任意の Amazon CloudFront ディストリビューションにルーティングするための包括的な手順について説明します。Amazon CloudFront と Amazon Simple Storage Service で静的ウェブサイトを設定する場合の完全なチュートリアルについては、「Amazon CloudFront ディストリビューションを使用して静的なウェブサイトを提供する」を参照してください。

ウェブ AWS コンテンツの配信を高速化する 1 つの方法として、コンテンツ配信ネットワーク (CDN) である Amazon CloudFront を使用できます。CloudFront は、エッジロケーションのグローバルネットワークを使用して、動的、静的、ストリーミング、インタラクティブなコンテンツを含む、ウェブサイト全体を配信できます。コンテンツをリクエストしたユーザーは、レイテンシーが最も低いエッジロケーションに自動的にルーティングされます。

> **Note**
>
> CloudFront ディストリビューションにトラフィックをルーティングできるのは、パブリックホストゾーンの場合のみです。

CloudFront を使用してウェブサイトのコンテンツを配信するには、ディストリビューションを作成してその設定を指定します。例えば、CloudFront がコンテンツを取得する Amazon S3 バケットまたは HTTP サーバー、選択したユーザーのみがコンテンツにアクセスできるようにするかどうか、ユーザーに HTTPS を使用させるかどうかを指定します。

ディストリビューションを作成すると、CloudFront が、d111111abcdef8.cloudfront.net などのドメイン名をディストリビューションに割り当てます。このドメイン名は、コンテンツの URL で使用できます。次に例を示します。

```
http://d111111abcdef8.cloudfront.net/logo.jpg
```

または、次の例のように、URL で独自のドメイン名を使用することもできます。

```
http://example.com/logo.jpg
```

CloudFront がディストリビューションに割り当てるドメイン名の代わりに、CloudFront ディストリビューション内のファイルの URL で独自のドメイン名を使用するには、Amazon CloudFront デベロッパーガイドの手順に従ってください。独自のドメイン名を、CloudFront ディストリビューションで使用する方法については、「代替ドメイン名 (CNAME) を追加してカスタム URL を使用する」を参照してください。

CloudFront ディストリビューションで Route 53 ドメイン名を使用する場合は、Amazon Route 53 を使用して、CloudFront ディストリビューションを指すエイリアスレコードを作成します。エイリアスレコードは、DNS への Route 53 拡張です。CNAME レコードに似ていますが、ルートドメイン (example.com など) とサブドメイン (www.example.com など) の両方にエイリアスレコードを作成できます (サブドメインのみに対して CNAME レコードを作成できます)。エイリアスレコードの名前とタイプに一致する DNS クエリを Route 53 が受け取ると、Route 53 はディストリビューションに関連付けられたドメイン名で応答します。

> **Note**
>
> Route 53 では、CloudFront ディストリビューションまたは他の AWS リソースへのエイリアスクエリには料金が発生しません。

前提条件

使用開始には、以下が必要です。

1. 登録済みドメイン名 ドメインレジストラとして、Amazon Route 53 を使用することも、あるいは別のレジストラを使用することもできます。
2. ドメインの DNS サービスとしての Route 53。Route 53 を使用してドメイン名を登録した場合、Route 53 をドメインの DNS サービスとして自動的に設定します。

   Route 53 をドメインの DNS サービスプロバイダとして使用する方法の詳細については、「Amazon Route 53 を既存ドメインの DNS サービスとして使用する」を参照してください。
3. CloudFront ディストリビューションまたは CloudFront ディストリビューションテナント。ディストリビューションには、CloudFront がディストリビューションに割り当てたドメイン名の代わりに URL に使用するドメイン名に一致する代替ドメイン名を含める必要があります。CloudFront ディストリビューションテナントの場合、URL に使用するドメイン名が含まれている必要があります。

   たとえば、コンテンツの URL にドメイン名 example.com を含める場合、ディストリビューションの [Alternate Domain Name] フィールドには example.com を含める必要があります。

   詳細については、Amazon CloudFront デベロッパーガイドの中の次のドキュメントを参照してください：

   - ディストリビューションを作成するためのタスクリスト
   - CloudFront コンソールを使用したディストリビューションの作成または更新

   > **Note**
   >
   > 静的ウェブサイトを作成する場合の完全なセットアップ手順については、「Amazon CloudFront デベロッパーガイド」の「安全な静的ウェブサイトの開始方法」を参照してください。

4. (オプション) Amazon CloudFront ディストリビューションで HTTPS が必要となるように、パブリック証明書をリクエストします。詳細については、「AWS Certificate Manager ユーザーガイド」の「AWS Certificate Managerにおける DNS 検証」を参照してください。

Amazon Route 53 を設定して、CloudFront ディストリビューションにトラフィックをルーティング

トラフィックが CloudFront ディストリビューションにルーティングされるように Amazon Route 53 を設定するには。独自のドメイン名を、CloudFront ディストリビューションで使用する方法については、Amazon CloudFront デベロッパーガイドの「代替ドメイン名 (CNAME) を追加してカスタム URL を使用する」を参照してください。

> **Note**
>
> 通常、変更は 60 秒以内にすべての Route 53 サーバーに伝播されます。変更内容が伝播すると、この手順で作成したエイリアスレコードの名前を使用して、CloudFront ディストリビューションに対しトラフィックをルーティングできるようになります。

CloudFront ディストリビューションにトラフィックをルーティングするには

1. CloudFront によりディストリビューションに割り当てられたドメイン名を取得し、IPv6 が有効かどうかを確認します。

   a. にサインイン AWS マネジメントコンソール し、 で CloudFront コンソールを開きますhttps://console.aws.amazon.com/cloudfront/v4/home。

   b. ID 列で、トラフィックのルーティング先のディストリビューションのリンクされた名前を選択します。

   c. [General] (一般) タブで、[Distribution domain name] (ディストリビューションドメイン名) の値を取得します。

   d. [General] (一般) タブの [Settings] (設定) セクションで、[Edit] (編集) を選択し、スクロールして [IPv6] フィールドでディストリビューションに対し IPv6 が有効になっていることを確認します。IPv6 が有効になっている場合は、ディストリビューションに対して 2 つのエイリアスレコードを作成する必要があります。1 つでは IPv4 のトラフィックをディストリビューションにルーティングし、別の 1 つでは IPv6 のトラフィックをルーティングします。[キャンセル] を選択します。

詳細については、Amazon CloudFront デベロッパーガイドのトピック「ディストリビューションを作成または更新する場合に指定する値」で「IPv6 を有効にする」を参照してください。

2. CloudFront ディストリビューションテナントの場合、

   a. 左側のナビゲーションで [SaaS] を選択し、次に [Distribution tenants] (ディストリビューションテナント) を選択し、トラフィックをルーティングするドメイン名を持つディストリビューションテナントを選択します。

   b. [General details] (一般詳細) セクションで、エンドポイントの値をコピーします。

3. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。

4. ナビゲーションペインで [Hosted zones] を選択します。

5. CloudFront ディストリビューションへのトラフィックのルーティングに使用するドメインのホストゾーンのリンクされた名前を選択します。

6. [Create record (レコードを作成)] を選択します。

7. 次の値を指定します。

   レコード名

   CloudFront ディストリビューションへのトラフィックのルーティングに使用するドメイン名を入力します。デフォルト値はホストゾーンの名前です。

   たとえば、ホストゾーンの名前が example.com で、[acme.example.com] を使用してトラフィックをディストリビューションにルーティングする場合、「acme」と入力します。

   レコードタイプ

   [A – IPv4 address (A – IPv4 address)] を選択します。

   ディストリビューションに対して IPv6 が有効になっていて、2 番目のレコードを作成する場合は、[AAAA – IPv6 アドレス] を選択します。

   エイリアス

   エイリアスをオンにします。

> **Important**
>
> CloudFront ディストリビューションを機能させるには、エイリアスレコードを作成する必要があります。

トラフィックのルーティング先

[Alias to CloudFront distribution] (CloudFront ディストリビューションへのエイリアス) を選択します。ディストリビューションの作成時に、CloudFront がそのディストリビューションに割り当てた名前を選択します。これはステップ 1 で取得した値です。

CloudFront ディストリビューションテナントの場合は、ステップ 2 からエンドポイントを選択します。

ターゲットの正常性の評価

デフォルト値の [No] をそのまま使用します。

ルーティングポリシー

該当するルーティングポリシーを選択します。詳細については、「ルーティングポリシーの選択」を参照してください。

8. [レコードを作成] を選択します。
9. ディストリビューションに対して IPv6 が有効になっている場合は、ステップ 5 ～ 7 を繰り返します。ステップ 6 で説明したように、[レコードタイプ] フィールドを除いて、同じ設定を指定します。

Amazon EC2 インスタンスへのトラフィックのルーティング

Amazon EC2 は、 AWS クラウドでスケーラブルなコンピューティング容量を提供します。事前設定されたテンプレート (Amazon Machine Image または AMI) を使用して、EC2 仮想コンピューティング環境 (インスタンス) を起動できます。EC2 インスタンスを起動すると、EC2 によりオペレーティングシステム (Linux または Microsoft Windows) と、AMI に含まれる追加のソフトウェア (ウェブサーバーやデータベースソフトウェアなど) が自動的にインストールされます。

EC2 インスタンスでウェブサイトをホストしていたり、ウェブアプリケーションを実行していたりする場合に、Amazon Route 53 を使用してドメイン (example.com など) のトラフィックをサーバーにルーティングできます。

前提条件

使用開始には、以下が必要です。

- Amazon EC2 インスタンス。EC2 インスタンスの起動については、次のドキュメントを参照してください。
  - Linux –「Amazon EC2 ユーザーガイド」の「Amazon EC2 Linux インスタンスの開始方法」を参照してください。
  - Microsoft Windows –「Amazon EC2 ユーザーガイド」の「Amazon EC2 Windows インスタンスの開始方法」を参照してください。

  > **Important**
  >
  > Elastic IP アドレスを作成し、この IP アドレスを EC2 インスタンスに関連付けることもお勧めします。Elastic IP アドレスによって、Amazon EC2 インスタンスの IP アドレスが固定されます。料金については、「Elastic IP アドレス料金表」を参照してください。

- 登録済みドメイン名 ドメインレジストラとして、Amazon Route 53 を使用することも、あるいは別のレジストラを使用することもできます。
- ドメインの DNS サービスとしての Route 53。Route 53 を使用してドメイン名を登録した場合、Route 53 をドメインの DNS サービスとして自動的に設定します。

  Route 53 をドメインの DNS サービスプロバイダとして使用する方法の詳細については、「Amazon Route 53 を既存ドメインの DNS サービスとして使用する」を参照してください。

トラフィックを Amazon EC2 インスタンスにルーティングする Amazon Route 53 の設定

トラフィックが EC2 インスタンスにルーティングされるように Amazon Route 53 を設定するには、以下の手順を実行します。

Amazon EC2 インスタンスにトラフィックをルーティングするには

1. Amazon EC2 インスタンスの IP アドレスを取得します。

a. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/ec2/ で Amazon EC2 コンソールを開きます。

b. コンソールの右上隅にあるリージョンリストで、インスタンスを起動するリージョンを選択します。

c. ナビゲーションペインで、[インスタンス] を選択します。

d. 表で、トラフィックのルーティング先のインスタンスを選択します。

e. 下のペインの [Description] タブで [Elastic IPs] の値を取得します。

Elastic IP をインスタンスに関連付けなかった場合は、[IPv4 Public IP (IPv4 パブリック IP)] の値を取得します。

2. Route 53 コンソール (https://console.aws.amazon.com/route53/) を開きます。
3. ナビゲーションペインで [Hosted zones] を選択します。
4. トラフィックをルーティングするドメイン名と一致するホストゾーンの名前を選択します。
5. [Create record (レコードを作成)] を選択します。
6. 次の値を指定します。

ルーティングポリシー

該当するルーティングポリシーを選択します。詳細については、「ルーティングポリシーの選択」を参照してください

レコード名

EC2 インスタンスへのトラフィックのルーティングに使用するドメイン名を入力します。デフォルト値はホストゾーンの名前です。

たとえば、ホストゾーンの名前が example.com で、acme.example.com を使用してトラフィックを EC2 インスタンスにルーティングする場合、「acme」と入力します。

値/トラフィックのルーティング先

IP アドレス、またはレコードタイプに応じた別の値を選択します。ステップ 1 で取得した IP アドレスを入力します。

レコードタイプ

[A – IPv4 address (A – IPv4 address)] を選択します。

TTL (秒)

デフォルト値の [300] をそのまま使用します。

7. [レコードを作成] を選択します。

通常、変更は 60 秒以内にすべての Route 53 サーバーに伝播されます。伝達が完了すると、この手順で作成したレコードの名前を使用して EC2 インスタンスにトラフィックをルーティングできるようになります。

> **Important**
>
> Elastic IP を解放する場合は、それをポイントしている DNS レコードも必ず削除してください。削除しない場合、未承認のユーザーによって乗っ取られる可能性のあるダングリング DNS レコードが存在することになります。

AWS App Runner サービスへのトラフィックのルーティング

AWS App Runner はフルマネージド型サービスであり、開発者はコンテナ化されたウェブアプリケーションと APIs を大規模にデプロイでき、インフラストラクチャの事前経験は必要ありません。ソースコードから開始するか、コンテナイメージを使用します。App Runner は、ウェブアプリケーションを自動的に構築およびデプロイし、暗号化によるトラフィックの負荷分散を行い、トラフィックのニーズに合わせてスケーリングし、プライベート Amazon VPC で実行される他の AWS サービスやアプリケーションとサービスが簡単に通信できるようにします。App Runner により、サーバーやスケーリングについて考察する時間を、アプリケーションのために向けられるようになります。詳細については、「AWS App Runner デベロッパーガイド」の「AWS App Runnerとは」を参照してください。

> **Important**
>
> Amazon Route 53 は現在、2022 年 8 月 1 日以降に作成された AWS App Runner サービスのエイリアスレコードをサポートしています。

ドメイントラフィックを App Runner サービ。スにルーティングするには、Amazon Route 53 を使用して、その App Runner サービスをポイントするエイリアスレコードを作成します。エイリアスレコードは、DNS への Route 53 拡張です。これは、ルートドメイン (example.com など) とサブドメ

イン (www.example.com や http://www.example.com/ など) の両方にエイリアスレコードを作成できることを除いて、CNAME レコードに似ています。CNAME レコードは、サブドメインに対してのみ作成が可能です。

> **Note**
>
> Route 53 では、App Runner サービスや他の AWS リソースへのエイリアスクエリには料金が発生しません。

前提条件

使用開始には、以下が必要です。

- App Runner サービス。App Runner サービスの作成については、「Getting started with App Runner」(App Runner の使用開始) を参照してください。
- 登録済みドメイン名 Amazon Route 53 をドメインレジストラとして使用することも、別のレジストラを使用することもできます。
- ドメインの DNS サービスとしての Route 53。Route 53 を使用してドメイン名を登録した場合、Route 53 をドメインの DNS サービスとして自動的に設定します。

  Route 53 をドメインの DNS サービスプロバイダとして使用する方法の詳細については、「Amazon Route 53 を既存ドメインの DNS サービスとして使用する」を参照してください。
- カスタムドメインが App Runner サービスに関連付けられました。詳細については、「Managing custom domain names for App Runner」(App Runner サービスでのカスタムドメイン名の管理) を参照してください。
- App Runner から Route 53 ホストゾーンに返される証明書の検証レコードを設定して、ドメインの検証プロセスを開始します。詳細については、「AWS Certificate Manager ユーザーガイド」の「AWS Certificate Managerにおける DNS 検証」を参照してください。

Amazon Route 53 での App Runner サービスに対するトラフィックのルーティングの設定

トラフィックが App Runner サービスにルーティングされるように Amazon Route 53 を設定するには、以下の手順を実行します。

App Runner サービスにトラフィックをルーティングするには

1. Route 53 コンソール (https://console.aws.amazon.com/route53/) を開きます。
2. ナビゲーションペインで [Hosted zones] を選択します。
3. トラフィックをルーティングするドメイン名と一致するホストゾーンの名前を選択します。
4. [Create record (レコードを作成)] を選択します。
5. 次の値を指定します。

   ルーティングポリシー

   該当するルーティングポリシーを選択します。詳細については、「ルーティングポリシーの選択」を参照してください

   レコード名

   App Runner サービスへのトラフィックのルーティングに使用するドメイン名を入力します。デフォルト値はホストゾーンの名前です。

   例えば、ホストゾーンの名前が example.com であり、acme.example.com を使用してトラフィックを App Runner サービスにルーティングする場合には、「acme」と入力します。

   値/トラフィックのルーティング先

   [Alias to App Runner Service] (App Runner サービスのエイリアス) を選択し、次に AWS リージョンを選択します。トラフィックをルーティングする環境のドメイン名を選択します。

   レコードタイプ

   デフォルト値の [A – IPv4 address] を使用します。

   ターゲットの正常性の評価

   [No] (いいえ) を選択します。 ターゲットの状態の評価については、「ターゲットの正常性の評価」を参照してください。
6. [レコードを作成] を選択します。

通常、変更は 60 秒以内にすべての Route 53 サーバーに伝播されます。伝達が完了すると、この手順で作成したエイリアスレコードの名前を使用して、トラフィックを App Runner サービスにルーティングできるようになります。

へのトラフィックのルーティング AWS Global Accelerator

AWS Global Accelerator は、ローカルおよびグローバルユーザーのアプリケーションのパフォーマンスを向上させるアクセラレーターを作成するサービスです。このサービスは、ヘルスや設定の変化に即座に反応し、クライアントからのインターネットトラフィックが常に正常なエンドポイントに転送されるようにします。Global Accelerator には耐障害性アーキテクチャが含まれており、DDoS 攻撃からのインライン自動緩和のために AWS Shield Standardが組み込まれています。詳細については、「 AWS Global Accelerator デベロッパーガイド」の「Global Accelerator とは」を参照してください。

デフォルトでは、Global Accelerator はアクセラレーターに関連付ける静的 IP アドレスを提供します。静的 IP アドレスは AWS エッジネットワークからのエニーキャストです。アクセラレーターにはデフォルトの DNS 名が含まれていますが、ほとんどのシナリオでは、割り当てられた静的 IP アドレスやデフォルトの DNS 名を使用する代わりに、アクセラレーターでカスタムドメイン名 (www.example.com など) を使用するように DNS を設定できます。

> **Note**
>
> Route 53 では、Global Accelerator または他の AWS リソースへのエイリアスクエリには料金が発生しません。

前提条件

使用開始には、以下が必要です。

- アクセラレーター。標準アクセラレーターまたはカスタムルーティングアクセラレーターのいずれかを作成できます。詳細については、「標準アクセラレーターを作成する」および「カスタムルーティングアクセラレーターを作成する」を参照してください。
- 登録済みドメイン名 Amazon Route 53 をドメインレジストラとして使用することも、別のレジストラを使用することもできます。
- ドメインの DNS サービスとしての Route 53。Route 53 を使用してドメイン名を登録した場合、Route 53 をドメインの DNS サービスとして自動的に設定します。

  Route 53 をドメインの DNS サービスプロバイダとして使用する方法の詳細については、「Amazon Route 53 を既存ドメインの DNS サービスとして使用する」を参照してください。

トラフィックがアクセラレーターにルーティングされるように Amazon Route 53 を設定

トラフィックがアクセラレーターにルーティングされるように Amazon Route 53 を設定するには、以下の手順を実行します。

アクセラレーターにトラフィックをルーティングするには

1. Route 53 コンソール (https://console.aws.amazon.com/route53/) を開きます。
2. ナビゲーションペインで [Hosted zones] を選択します。
3. トラフィックをルーティングするドメイン名と一致するホストゾーンの名前を選択します。
4. [Create record (レコードを作成)] を選択します。
5. 次の値を指定します。

   ルーティングポリシー

   該当するルーティングポリシーを選択します。詳細については、「ルーティングポリシーの選択」を参照してください

   レコード名

   アクセラレーターへのトラフィックのルーティングに使用するドメイン名を入力します。デフォルト値はホストゾーンの名前です。

   たとえば、ホストゾーンの名前が example.com で、acme.example.com を使用してトラフィックを Global Accelerator にルーティングする場合、「acme」と入力します。

   値/トラフィックのルーティング先

   Global Accelerator のエイリアスを選択し、 AWS リージョンを選択します。アクセラレーターの DNS 名を選択します。

   現在の AWS アカウント または別の AWS アカウントを使用して作成したアクセラレーターの DNS 名を入力できます。

   レコードタイプ

   デフォルト値の [A – IPv4 address] を使用します。

   ターゲットの正常性の評価

   デフォルト値の [Yes] をそのまま使用します。

6. [レコードを作成] を選択します。

   通常、変更は 60 秒以内にすべての Route 53 サーバーに伝播されます。伝達が完了すると、この手順で作成したエイリアスレコードの名前を使用して、トラフィックをアクセラレーターにルーティングできるようになります。

AWS Elastic Beanstalk 環境へのトラフィックのルーティング

AWS Elastic Beanstalk を使用して AWS クラウドにアプリケーションをデプロイおよび管理する場合は、Amazon Route 53 を使用して、example.com などのドメインの DNS トラフィックを新規または既存の Elastic Beanstalk 環境にルーティングできます。

DNS トラフィックを Elastic Beanstalk 環境にルーティングするには、以下の各トピックの手順を参照してください。

> **Note**
>
> これらの手順は、既に Route 53 をドメインの DNS サービスとして使用していることを前提としています。別の DNS サービスを使用している場合は、ドメインの DNS サービスプロバイダとしての Route 53 の使用について「Amazon Route 53 を既存ドメインの DNS サービスとして使用する」を参照してください。

トピック

- Elastic Beanstalk 環境へのアプリケーションのデプロイ
- Elastic Beanstalk 環境のドメイン名の取得
- Elastic Beanstalk 環境にトラフィックをルーティングする Amazon Route 53 レコードの作成

Elastic Beanstalk 環境へのアプリケーションのデプロイ

トラフィックのルーティング先の Elastic Beanstalk 環境が既にある場合、「Elastic Beanstalk 環境のドメイン名の取得」にスキップしてください。

アプリケーションを作成し、Elastic Beanstalk 環境にデプロイするには

- アプリケーションを作成し、Elastic Beanstalk 環境にデプロイする方法については、AWS Elastic Beanstalk デベロッパーガイドの Elastic Beanstalk を使用して開始するを参照してください。

Elastic Beanstalk 環境のドメイン名の取得

Elastic Beanstalk 環境のドメイン名を既に知っている場合、「Elastic Beanstalk 環境にトラフィックをルーティングする Amazon Route 53 レコードの作成」にスキップしてください。

Elastic Beanstalk 環境のドメイン名を取得するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/elasticbeanstalk/ で Elastic Beanstalk コンソールを開きます。
2. アプリケーションのリストで、トラフィックをルーティングするアプリケーションを見つけ、[URL] の値を取得します。アプリケーションのリストが表示されない場合は、ナビゲーションペインで [Applications] を選択します。

   URL の詳細については、Elastic Beanstalk デベロッパーガイドの Elastic Beanstalk 環境のドメイン名を参照してください。

Elastic Beanstalk 環境にトラフィックをルーティングする Amazon Route 53 レコードの作成

Amazon Route 53 レコードには、トラフィックを Elastic Beanstalk 環境にルーティングする方法をコントロールする設定が含まれています。環境をデプロイしたリージョン (us-east-2 など) が環境のドメイン名に含まれているかどうかに応じて、CNAME レコードまたはエイリアスレコードを作成します。新しい環境では、ドメイン名にリージョンが含まれています。2016 年初期より前に作成された環境では含まれていません。CNAME とエイリアスレコードの比較については、「エイリアスレコードと非エイリアスレコードの選択」を参照してください。

ドメイン名にリージョンが含まれていない場合

CNAME レコードを作成する必要があります。ただし、DNS による制限のため、CNAME レコードはサブドメインに対してのみ作成でき、ルートドメイン名に対しては作成できません。例えば、ドメイン名が example.com の場合、acme.example.com のトラフィックを Elastic Beanstalk 環境にルーティングするレコードは作成できますが、example.com のトラフィックを Elastic Beanstalk 環境にルーティングするレコードは作成できません。

「CNAME レコードを作成してトラフィックを Elastic Beanstalk 環境にルーティングするには」の手順を参照してください。

ドメイン名にリージョンが含まれている場合

エイリアスレコードを作成できます。エイリアスレコードは Route 53 に固有であり、CNAME レコードに比べて、大きな利点が 2 つあります。

- エイリアスレコードは、ルートドメイン名またはサブドメインに作成できます。例えば、ドメイン名が example.com の場合、example.com または acme.example.com のリクエストを Elastic Beanstalk 環境にルーティングするレコードを作成できます。
- Route 53 では、トラフィックをルーティングするためにエイリアスレコードを使用するリクエストに料金は発生しません。

「Elastic Beanstalk 環境にトラフィックをルーティングするための Amazon Route 53 エイリアスレコードを作成するには」の手順を参照してください。

CNAME レコードを作成してトラフィックを Elastic Beanstalk 環境にルーティングするには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [Hosted zones] を選択します。
3. Elastic Beanstalk 環境へのトラフィックのルーティングに使用するホストゾーンの名前を選択します。
4. [Create record (レコードを作成)] を選択します。
5. [クイック作成に切り替える] を選択します
6. 次の値を指定します。

   ルーティングポリシー

   該当するルーティングポリシーを選択します。詳細については、「ルーティングポリシーの選択」を参照してください

   レコード名

   Elastic Beanstalk 環境へのトラフィックのルーティングに使用するドメイン名を入力します。デフォルト値はホストゾーンの名前です。

   たとえば、ホストゾーンの名前が example.com で、acme.example.com を使用してトラフィックを環境にルーティングする場合、「acme」と入力します。

> **Important**
> ホストゾーンと同じ名前を持つ CNAME レコードを作成することはできません。

エイリアス

クイック作成レコード作成方法を使用している場合、[エイリアス] をオンにします。

値/トラフィックのルーティング先

IP アドレス、またはレコードタイプに応じた別の値を選択して、トピック「Elastic Beanstalk 環境のドメイン名の取得」の手順を実行したときに取得する値を入力します。さまざまなアカウントを使用して Route 53 ホストゾーンおよび Elastic Beanstalk 環境を作成した場合は、Elastic Beanstalk 環境の CNAME 属性を入力します。

レコードタイプ

[CNAME] を選択します。

TTL (秒)

デフォルト値の [300] をそのまま使用します。

7. [レコードを作成] を選択します。

通常、変更は 60 秒以内にすべての Route 53 サーバーに伝播されます。

Elastic Beanstalk 環境にトラフィックをルーティングするための Amazon Route 53 エイリアスレコードを作成するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [Hosted zones] を選択します。
3. Elastic Beanstalk 環境へのトラフィックのルーティングに使用するホストゾーンの名前を選択します。
4. [Create record (レコードを作成)] を選択します。
5. 次の値を指定します。

ルーティングポリシー

該当するルーティングポリシーを選択します。詳細については、「ルーティングポリシーの選択」を参照してください

レコード名

Elastic Beanstalk 環境へのトラフィックのルーティングに使用するドメイン名を入力します。デフォルト値はホストゾーンの名前です。

たとえば、ホストゾーンの名前が example.com で、acme.example.com を使用してトラフィックを環境にルーティングする場合、「acme」と入力します。

値/トラフィックのルーティング先

[Elastic Beanstalk 環境へのエイリアス] を選択し、エンドポイントの元のリージョンを選択します。トラフィックをルーティングする環境のドメイン名を選択します。これは、トピック「Elastic Beanstalk 環境のドメイン名の取得」の手順を実行したときに取得する値です。

さまざまなアカウントを使用して Route 53 ホストゾーンおよび Elastic Beanstalk 環境を作成した場合は、Elastic Beanstalk 環境の CNAME 属性を入力します。

レコードタイプ

デフォルトの [A – IPv4 アドレス] を使用します。

ターゲットの正常性の評価

デフォルト値の [Yes] をそのまま使用します。

6. [レコードを作成] を選択します。

通常、変更は 60 秒以内にすべての Route 53 サーバーに伝播されます。伝播が完了すると、この手順で作成したエイリアスレコードの名前を使用して、トラフィックを Elastic Beanstalk 環境にルーティングできるようになります。

ELB ロードバランサーへのトラフィックのルーティング

複数の Amazon EC2 インスタンスでウェブサイトをホストしている場合、Elastic Load Balancing (ELB) ロードバランサーを使用して、ウェブサイトへのトラフィックを、インスタンスをまたがって分散できます。ELB サービスは、ウェブサイトへのトラフィックが時間の経過とともに変化するにつれてロードバランサーを自動的にスケーリングします。また、ロードバランサーは登録されている

インスタンスの状態を監視して、トラフィックを正常なインスタンスにのみルーティングすることができます。

ドメイントラフィックを ELB ロードバランサーにルーティングするには、Amazon Route 53 を使用して、ロードバランサーをポイントするエイリアスレコードを作成します。エイリアスレコードは、DNS への Route 53 拡張です。CNAME レコードに似ていますが、ルートドメイン (example.com など) とサブドメイン (www.example.com など) の両方にエイリアスレコードを作成できます (サブドメインのみに対して CNAME レコードを作成できます)。

> **Note**
>
> Route 53 では、ELB ロードバランサーまたは他の AWS リソースへのエイリアスクエリには料金が発生しません。

前提条件

使用開始には、以下が必要です。

- ELB ロードバランサー。ELB Classic、Application、または Network Load Balancer を使用できます。ロードバランサーの作成の詳細については、Elastic Load Balancing ユーザーガイドの「Elastic Load Balancing の使用開始」を参照してください。

  ロードバランサーには、覚えやすい意味を持った名前を設定してください。ロードバランサーの作成時に指定した名前は、Route 53 コンソールでエイリアスレコードを作成するときに選択する名前になります。
- 登録済みドメイン名 Route 53 をドメインレジストラとして使用することも、別のレジストラを使用することもできます。
- ドメインの DNS サービスとしての Route 53。Route 53 を使用してドメイン名を登録した場合、Route 53 をドメインの DNS サービスとして自動的に設定します。

  Route 53 をドメインの DNS サービスプロバイダとして使用する方法の詳細については、「Amazon Route 53 を既存ドメインの DNS サービスとして使用する」を参照してください。

トラフィックが ELB ロードバランサーにルーティングされるように Amazon Route 53 を設定

トラフィックが ELB ロードバランサーにルーティングされるように Amazon Route 53 を設定するには、以下の手順を実行します。

ELB ロードバランサーにトラフィックをルーティングするには

1. Route 53 ホストゾーンと ELB ロードバランサーの作成時に同じアカウントを使用した場合は、ステップ 2 に進みます。

   ホストゾーンと ELB ロードバランサーの作成時に異なるアカウントを使用した場合は、「Elastic Load Balancing ロードバランサーの DNS 名を取得する」の手順を実行して、ロードバランサーの DNS 名を取得します。
2. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
3. ナビゲーションペインで [Hosted zones] を選択します。
4. ロードバランサーへのトラフィックのルーティングに使用するドメイン名があるホストゾーンの名前を選択します。
5. [Create record (レコードを作成)] を選択します。
6. 次の値を指定します。

   ルーティングポリシー

   該当するルーティングポリシーを選択します。詳細については、「ルーティングポリシーの選択」を参照してください

   レコード名

   ELB ロードバランサーへのトラフィックのルーティングに使用するドメイン名またはサブドメインを入力します。デフォルト値はホストゾーンの名前です。

   たとえば、ホストゾーンの名前が example.com で、acme.example.com を使用してトラフィックをロードバランサーにルーティングする場合、「acme」と入力します。

   エイリアス

   クイック作成レコード作成方法を使用している場合、[エイリアス] をオンにします。

値/トラフィックのルーティング先

[アプリケーションおよび Classic Load Balancer エイリアス] または [Network Load Balancer エイリアス] を選択し、エンドポイントの元のリージョンを選択します。

同じ AWS アカウントを使用してホストゾーンと ELB ロードバランサーを作成した場合は、ロードバランサーの作成時に割り当てた DNS 名を選択します。

異なるアカウントでホストゾーンと ELB ロードバランサーを作成している場合には、この手順のステップ 1 で取得した値を入力します。

> **Note**
>
> コンソールはデュアルスタックの先頭に を付加します。 は、同じ AWS アカウントのアプリケーションと Classic Load Balancer の DNS 名にのみ付加されます。ウェブブラウザなどのクライアントが、ドメイン名 (example.com) またはサブドメイン名 (www.example.com) の IP アドレスをリクエストする場合、そのクライアントは IPv4 アドレス (A レコード)、IPv6 アドレス (AAAA レコード)、または IPv4 アドレスと IPv6 アドレスの両方を (IPv4 を先にして個別に) リクエストできます。[dualstack.] の指定により、Route 53 は、クライアントがリクエストした IP アドレス形式に基づいて、ロードバランサーに対する適切な IP アドレスで応答することができます。別のアカウントからのアプリケーションとClassic Load Balancer には、「dualstack.」を前に付加する必要があります。

レコードタイプ

[A – IPv4 address (A – IPv4 address)] を選択します。

ターゲットの正常性の評価

Route 53 で、リソースの状態に基づいてトラフィックをルーティングする場合は、[Yes] を選択します。リソースのヘルスチェックの詳細については、「Amazon Route 53 ヘルスチェックの作成」を参照してください。

7. [レコードを作成] を選択します。

通常、変更は 60 秒以内にすべての Route 53 サーバーに伝播されます。伝達が完了すると、この手順で作成したエイリアスレコードの名前を使用してロードバランサーにトラフィックをルーティングできるようになります。

Amazon S3 バケットでホストされているウェブサイトへのトラフィックのルーティング

このトピックでは、静的ウェブサイトホスティング用に設定された Amazon Simple Storage Service バケットに DNS トラフィックをルーティングする包括的な手順について説明します。Amazon Simple Storage Service で静的ウェブサイトを設定する場合の完全なチュートリアルについては、「Amazon S3 バケットの静的なウェブサイトにドメインを使用する」を参照してください。

Amazon Simple Storage Service (Amazon S3) では、安全で耐久性があり、拡張性の高いクラウドストレージを提供します。静的ウェブサイトをホストするように S3 バケットを設定し、ウェブページとクライアント側スクリプトを配置できます。(S3 ではサーバー側スクリプトがサポートされていません)。

ドメイントラフィックを S3 バケットにルーティングするには、Amazon Route 53 を使用して、バケットをポイントするエイリアスレコードを作成します。エイリアスレコードは、DNS への Route 53 拡張です。ルートドメイン (example.com など) とサブドメイン (www.example.com など) の両方にエイリアスレコードを作成できることを除いて、CNAME レコードに似ています。サブドメインのみに対して CNAME レコードを作成できます。

> **Note**
>
> Route 53 では、S3 バケットや他の AWS リソースへのエイリアスクエリには料金が発生しません。

前提条件

使用開始には、以下が必要です。

- 静的ウェブサイトをホストするように設定された S3 バケット。

  詳細については、「Amazon Simple Storage Service ユーザーガイド」の「チュートリアル: Route 53 に登録されたカスタムドメインを使用した静的ウェブサイトの設定」を参照してください。

> **Important**
>
> バケットは、ドメインまたはサブドメインと同じ名前にする必要があります。例えば、サブドメイン acme.example.com を使用している場合、バケットの名前は acme.example.com にする必要があります。

ドメインとそのサブドメイン (example.com と www.example.com など) のトラフィックは、単一のバケットにルーティングすることができます。ドメインと各サブドメインのバケットを作成してすべて設定します。ただし、1 つのバケットについては、残りのバケットにトラフィックをリダイレクトするように設定します。

> **Note**
>
> ウェブサイトエンドポイントとして設定されている S3 バケットは SSL/TLS をサポートしないため、トラフィックを CloudFront ディストリビューションにルーティングして、S3 バケットをディストリビューションのオリジンとして使用する必要があります。CloudFront ディストリビューションを作成する方法については、「ドメイン名を使用したトラフィックの Amazon CloudFront ディストリビューションへのルーティング」を参照してください。

- 登録済みドメイン名 Route 53 をドメインレジストラとして使用することも、別のレジストラを使用することもできます。
- ドメインの DNS サービスとしての Route 53。Route 53 を使用してドメイン名を登録した場合、Route 53 をドメインの DNS サービスとして自動的に設定します。

  Route 53 をドメインの DNS サービスプロバイダとして使用する方法の詳細については、「Amazon Route 53 を既存ドメインの DNS サービスとして使用する」を参照してください。

トラフィックが S3 バケットにルーティングされるように Amazon Route 53 を設定

静的ウェブサイトをホストするよう設定されている S3 バケットにトラフィックがルーティングされるように Amazon Route 53 を設定するには、以下の手順を実行します。

S3 バケットにトラフィックをルーティングするには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [Hosted zones] を選択します。
3. S3 バケットへのトラフィックのルーティングに使用するドメイン名があるホストゾーンの名前を選択します。
4. [Create record (レコードを作成)] を選択します。
5. 次の値を指定します。

   レコード名

   S3 バケットへのトラフィックのルーティングに使用するドメイン名を入力します。デフォルト値はホストゾーンの名前です。

   たとえば、ホストゾーンの名前が example.com で、acme.example.com を使用してトラフィックをバケットにルーティングする場合、「acme」と入力します。

   レコードタイプ

   [A – IPv4 address (A – IPv4 address)] を選択します。

   エイリアス

   エイリアスをオンにします。

   トラフィックのルーティング先

   [S3 ウェブサイトエンドポイントへのエイリアス] を選択し、エンドポイントの元のリージョンを選択します。

   [レコード名] に指定したのと同じ名前のバケットを選択します。

   リストには、次の要件を満たすバケットのみが含まれます。

   - バケットの名前は作成しているレコードの名前と同じである
   - バケットはウェブサイトエンドポイントとして構成されている。
   - バケットは現在の AWS アカウントによって作成されている

     別の AWS アカウントを使用してバケットを作成した場合は、S3 バケットを作成したリージョンの名前を入力します。リージョン名の正しい形式については、「Amazon Web

Services 全般のリファレンス」の「Amazon S3 ウェブサイトのエンドポイント」にアクセスし、表にあるウェブサイトのエンドポイント列を参照してください。

ターゲットの正常性の評価

[No] (いいえ) を選択します。 ターゲットの状態の評価については、「ターゲットの正常性の評価」を参照してください。

ルーティングポリシー

該当するルーティングポリシーを選択します。詳細については、「ルーティングポリシーの選択」を参照してください。

6. [レコードを作成] を選択します。

通常、変更は 60 秒以内にすべての Route 53 サーバーに伝播されます。伝達が完了すると、この手順で作成したエイリアスレコードの名前を使用して、トラフィックを S3 バケットにルーティングできるようになります。

ドメイン名を使用してトラフィックを Amazon Virtual Private Cloud インターフェイスエンドポイントにルーティングする

AWS PrivateLink を使用して、Amazon Virtual Private Cloud (Amazon VPC) インターフェイスエンドポイントで選択したサービスにアクセスできます。これらのサービスには、一部の AWS サービス、他の AWS 顧客やパートナーが独自の VPCs でホストするサービス、サポートされている AWS Marketplace パートナーサービスが含まれます。

ドメイントラフィックをインターフェイスエンドポイントにルーティングするには、Amazon Route 53 を使用してエイリアスレコードを作成します。エイリアスレコードは、DNS への Route 53 拡張です。CNAME レコードに似ていますが、ルートドメイン (example.com など) とサブドメイン (www.example.com など) の両方にエイリアスレコードを作成できます。サブドメインのみに対して CNAME レコードを作成できます。

> **Note**
>
> Route 53 では、インターフェイスエンドポイントやその他の AWS リソースへのエイリアスクエリには課金されません。

トピック

- 前提条件
- トラフィックを Amazon VPC インターフェイスエンドポイントにルーティングする Amazon Route 53 の設定

前提条件

使用開始には、以下が必要です。

- Amazon VPC インターフェイスエンドポイント。詳細については、「Amazon VPC ユーザーガイド」の「インターフェイス VPC エンドポイント (AWS PrivateLink)」を参照してください。
- 登録済みドメイン名 Amazon Route 53 をドメインレジストラとして使用することも、別のレジストラを使用することもできます。
- ドメインの DNS サービスとしての Route 53。Route 53 を使用してドメイン名を登録した場合、Route 53 をドメインの DNS サービスとして自動的に設定します。

  Route 53 をドメインの DNS サービスプロバイダとして使用する方法の詳細については、「Amazon Route 53 を既存ドメインの DNS サービスとして使用する」を参照してください。

トラフィックを Amazon VPC インターフェイスエンドポイントにルーティングする Amazon Route 53 の設定

トラフィックを Amazon VPC インターフェイスエンドポイントにルーティングするように Amazon Route 53 を設定するには、以下の手順を実行します。

トラフィックを Amazon VPC インターフェイスエンドポイントにルーティングするには

1. 同じアカウントを使用して Route 53 ホストゾーンと Amazon VPC インターフェイスエンドポイントを作成した場合は、ステップ 2 に進みます。

   異なるアカウントを使用してホストゾーンとインターフェイスエンドポイントを作成した場合は、インターフェイスエンドポイントのサービス名を取得します。

   a. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/vpc/ で Amazon VPC コンソールを開きます。
   b. ナビゲーションペインで、[エンドポイント] を選択します。
   c. 右側のペインで、インターネットトラフィックのルーティング先となるエンドポイントを選択します。

d. 下部のペインで、DNS 名の値 (vpce-0fd00dd593example-dexample.cloudtrail.us-west-2.vpce.amazonaws.com など) を取得します。

2. Route 53 コンソール (https://console.aws.amazon.com/route53/) を開きます。
3. ナビゲーションペインで [Hosted zones] を選択します。
4. インターフェイスエンドポイントへのトラフィックのルーティングに使用するドメイン名があるホストゾーンの名前を選択します。
5. [Create record (レコードを作成)] を選択します。
6. 次の値を指定します。

ルーティングポリシー

該当するルーティングポリシーを選択します。詳細については、「ルーティングポリシーの選択」を参照してください

レコード名

Amazon VPC インターフェイスエンドポイントへのトラフィックのルーティングに使用するドメイン名を入力します。

エイリアス

クイック作成レコード作成方法を使用している場合、[エイリアス] をオンにします。

値/トラフィックのルーティング先

[VPC エンドポイントへのエイリアス] を選択し、エンドポイントの元のリージョンを選択します。

エンドポイントの値を指定する方法は、同じ AWS アカウントまたは異なるアカウントを使用してホストゾーンとインターフェイスエンドポイントを作成したかどうかによって異なります。

- 同じアカウント – リストを選択し、[Amazon VPC エンドポイント] というカテゴリを見つけます。次に、インターネットトラフィックのルーティング先となるインターフェイスエンドポイントの DNS 名を選択します。
- 異なるアカウント – この手順のステップ 1 で取得した値を入力します。

レコードタイプ

[A – IPv4 address (A – IPv4 address)] を選択します。

ターゲットの正常性の評価

[No] (いいえ) を選択します。 ターゲットの状態の評価については、「ターゲットの正常性の評価」を参照してください。

7. [レコードを作成] を選択します。

通常、変更は 60 秒以内にすべての Route 53 サーバーに伝播されます。伝達が完了すると、この手順で作成したエイリアスレコードの名前を使用してトラフィックをインターフェイスエンドポイントにルーティングできるようになります。

Amazon WorkMail へのトラフィックのルーティング

Route 53 を使用すると、Amazon WorkMail の E メールドメインにトラフィックをルーティングできます。Route 53 ホストゾーンの名前 (example.com など) は、Amazon WorkMail ドメインの名前と一致する必要があります。

> **Note**
>
> Amazon WorkMailドメインにトラフィックをルーティングできるのは、パブリックホストゾーンの場合のみです。

Amazon WorkMail にトラフィックをルーティングするには、次の 4 つの手順を実行します。

Amazon Route 53 を DNS サービスとして設定し、Amazon WorkMail 組織およびメールドメインを追加するには

1. メールアドレス (john@example.com など) に使用するドメイン名を登録していない場合、ドメインが利用可能であることはわかっているため、ドメインを今すぐ登録します。詳細については、「新しいドメインの登録」を参照してください

   Amazon Route 53 が Amazon WorkMail に追加したメールドメインの DNS サービスでない場合は、該当するドメインの DNS サービスを Route 53 に移行します。詳細については、「Amazon Route 53 を既存ドメインの DNS サービスとして使用する」を参照してください
2. Amazon WorkMail 組織およびメールドメインを追加します。詳細については、Amazon WorkMail 管理者ガイドの「新規ユーザーの利用開始」を参照してください。

Amazon WorkMail の Route 53 TXT レコードを作成するには

1. Amazon WorkMail コンソールのナビゲーションペインで、[ドメイン] を選択します。
2. Amazon WorkMail へのトラフィックのルーティングに使用するメールドメインの名前 (example.com など) を選択します。
3. 別のブラウザタブで、[Route 53 コンソール] を開きます。
4. Route 53 コンソールで次の操作を行います。

   a. ナビゲーションペインで [Hosted zones] を選択します。

   b. Amazon WorkMail メールドメインに使用するホストゾーンの名前を選択します。
5. Amazon WorkMail コンソールの [ステップ 1: ドメイン所有者の確認] セクションで、[ホスト名] 列に移動し、値のメールドメイン名より前の部分をコピーします。

   例えば、Amazon WorkMail メールドメインが example.com で、[ホスト名] の値が _amazonses.example.com である場合は、_amazonses をコピーします。
6. Route 53 コンソールで次の操作を行います。

   a. [レコードを作成] を選択し、[シンプルルーティング] を選択します。

   b. [レコード名] に、ステップ 5 でコピーした値を貼り付けます。

   c. [レコードタイプ] で、[TXT – テキスト] を選択します。
7. Amazon WorkMail コンソールで、該当する TXT レコードの [値] 列の値 (引用符を含む) をコピーします。
8. Route 53 コンソールで次の操作を行います。

   a. [値/トラフィックのルーティング先] で、IP アドレス、またはレコードタイプに応じた別の値を選択し、ステップ 7 でコピーした値を貼り付けます。

      その他の設定は変更しないでください。

   b. [作成] を選択します。

Amazon WorkMail の Route 53 MX レコードを作成するには

1. Amazon WorkMail コンソールで、[Step 2: Finalize domain setup] (ステップ 2: ドメインセットアップの完了) のセクションで、[MX] の [Record type] (レコードタイプ) が表示されている行に移動して [Value] (値) 列の値をコピーします。
2. Route 53 コンソールで次の操作を行います。

a. [Create record (レコードを作成)] を選択します。

b. [値/トラフィックのルーティング先] で、IP アドレス、またはレコードタイプに応じた別の値を選択し、ステップ 1 でコピーした値を貼り付けます。

c. [レコードタイプ] で、[MX – Mail Exchange] を選択します。

その他の設定は変更しないでください。

d. [レコードを作成] を選択します。

Amazon WorkMail 用に 4 つの Route 53 CNAME レコードを作成するには

1. Amazon WorkMail コンソールの [ステップ 2: ドメインセットアップのファイナライズ] セクションで、[レコードタイプ] の値が [CNAME] である最初の行に移動します。[Hostname] 列で、値のメールドメイン名より前の部分をコピーします。

   例えば、Amazon WorkMail メールドメインが example.com で、[Hostname] の値が autodiscover.example.com である場合は、autodiscover をコピーします。

2. Route 53 コンソールで次の操作を行います。

   a. [Create record (レコードを作成)] を選択します。

   b. [レコード名] に、ステップ 1 でコピーした値を貼り付けます。

   c. [レコードタイプ] で、[CNAME - 正規化名] を選択します。

3. Amazon WorkMail コンソールの [レコードタイプ] が [CNAME] である最初の行で、[値] 列の値をコピーします。

4. Route 53 コンソールで次の操作を行います。

   a. [値/トラフィックのルーティング先] で、IP アドレス、またはレコードタイプに応じた別の値を選択し、ステップ 3 でコピーした値を貼り付けます。

   その他の設定は変更しないでください。

   b. [レコードを作成] を選択します。

5. Amazon WorkMail コンソールにリストされている残りの CNAME レコードに対して、ステップ 1 から 4 を繰り返します。

Amazon OpenSearch Service ドメインエンドポイントへのトラフィックのルーティング

Amazon OpenSearch Service は、 AWS クラウドにおける OpenSearch クラスターのデプロイ、オペレーション、スケーリングを容易にするマネージドサービスです。OpenSearch Service Service ドメインは、OpenSearch Service クラスターと同義です。ドメインは、指定した設定、インスタンスタイプ、インスタンスカウント、およびストレージリソースを持つクラスターです。詳細については、「Amazon OpenSearch Service デベロッパーガイド」の「Amazon OpenSearch Service とは?」を参照してください。

前提条件

使用開始には、以下が必要です。

作成する Route 53 レコードの名前と一致するカスタムドメイン名 (example.com など) を含む OpenSearch Service ドメイン。

詳細については、以下の各トピックを参照してください。

- 「Amazon OpenSearch Service デベロッパーガイド」の「開始方法」を参照してください。
- Amazon OpenSearch Service デベロッパーガイドのカスタムエンドポイントの作成。

Amazon Route 53 を Amazon OpenSearch Service ドメインエンドポイントにルーティングする Amazon Route 53 の設定

Route 53 を使用して OpenSearch Service にトラフィックをルーティングするには、まず OpenSearch Service が提供するドメインエンドポイントを取得します。このデュアルスタックエンドポイントは、デュアルスタックネットワークモードの OpenSearch Service ドメインでカスタムエンドポイントが有効になっている場合にのみ提供されます。詳細については、Amazon OpenSearch Service デベロッパーガイドの「カスタムエンドポイントの作成」を参照してください。

OpenSearch Service エンドポイントにトラフィックをルーティングするには

1. https://aws.amazon.com にアクセスし、[コンソールにサインイン] を選択します。
2. [分析] の下で、[Amazon OpenSearch Service] を選択します。
3. [Managed clusters] (マネージドクラスター) で [Domains] (ドメイン) を選択します。

4. [Domains] (ドメイン) ページで、トラフィックをルーティングするドメインの名前を選択します。
5. ドメインの詳細ページで、ドメインエンドポイント v2 (デュアルスタック) の値をコピーします。
6. Route 53 コンソール (https://console.aws.amazon.com/route53/) を開きます。
7. ナビゲーションペインで [Hosted zones] を選択します。
8. OpenSearch Service エンドポイントへのトラフィックのルーティングに使用するドメインのホストゾーンのリンク名を選択します。ドメイン名は、OpenSearch Service で定義されているカスタムエンドポイントと一致する必要があります。
9. [Create record] (レコードを作成) を選択します。

   レコードはウィザードを使用して作成するか、[Switch to quick create] (クイック作成に切り替え) を選択します。
10. 次の値を指定します。

    ルーティングポリシー

    該当するルーティングポリシーを選択します。詳細については、「ルーティングポリシーの選択」を参照してください

    レコード名

    OpenSearch Service ドメインエンドポイントへのトラフィックのルーティングに使用するドメイン名を入力します。デフォルト値はホストゾーンの名前です。

    たとえば、ホストゾーンの名前が example.com で、[acme.example.com] を使用してトラフィックをディストリビューションにルーティングする場合、「acme」と入力します。

    エイリアス

    クイック作成レコード作成方法を使用している場合、[エイリアス] をオンにします。

    値/トラフィックのルーティング先

    [Alias to OpenSearch Service domain endpoint] (OpenSearch Service ドメインエンドポイントへのエイリアス) を選択します。OpenSearch Service ドメインが作成されたリージョンを選択し、ステップ 5 で取得した値を選択します。

レコードタイプ

A – IPv4 アドレス、AAAA – IPv6 アドレス、デュアルスタックの場合はその両方を選択します。

ターゲットの正常性の評価

[No] (いいえ) を選択します。 ターゲットの状態の評価については、「ターゲットの正常性の評価」を参照してください。

11. [レコードを作成] を選択します。

Amazon VPC Lattice サービスドメインエンドポイントへのトラフィックのルーティング

Amazon VPC Lattice は、アプリケーションのサービスおよびリソースの接続、保護、モニタリングに使用する、フルマネージド型アプリケーションネットワーキングサービスです。VPC Lattice は、単一の仮想プライベートクラウド (VPC)、または 1 つ以上のアカウントの複数の VPC で使用できます。詳細については、「Amazon VPC Lattice ユーザーガイド」の「Amazon VPC Lattice のサービス」を参照してください。

前提条件

使用開始には、以下が必要です。

作成する Route 53 レコードの名前と一致するカスタムドメイン名 (example.com など) を含む VPC Lattice サービスドメイン。

詳細については、「Amazon VPC Lattice ユーザーガイド」の「カスタムドメイン名とサービスの関連付け」を参照してください。

VPC Lattice サービスドメインエンドポイントにトラフィックをルーティングするように Amazon Route 53 を設定する

Route 53 を使用して Amazon VPC Lattice サービスドメインにトラフィックをルーティングするには、まず VPC Lattice が提供するドメインサービスエンドポイントを取得します。詳細については、「Amazon VPC Lattice ユーザーガイド」の「カスタムドメイン名とサービスの関連付け」を参照してください。

VPC Lattice サービスドメインエンドポイントにトラフィックをルーティングするには

1. https://aws.amazon.com にアクセスし、[Sign In to the Console] (コンソールにサインイン) を選択します。
2. [Networking & Content Delivery] (ネットワーキング & コンテンツ配信) の中にある [VPC] を選択します。
3. [PrivateLink and Lattice] (PrivateLink と Lattice) で [Lattice Services] (Lattice サービス) を選択します。
4. VPC Lattice サービスを作成するか、既存の VPC Lattice サービスを選択します。

   > **Note**
   >
   > VPC Lattice サービスを作成するときは、カスタムドメイン設定を指定し、カスタムドメイン名を指定する必要があります。既存のサービスを選択する場合は、カスタムドメインも必要です。

5. [Domain configuration] (ドメイン設定) で、カスタムドメイン名の値をコピーします。
6. Route 53 コンソール (https://console.aws.amazon.com/route53/) を開きます。
7. ナビゲーションペインで [Hosted zones] を選択します。
8. [ドメイン名] には、VPC Lattice サービスドメインエンドポイントへのトラフィックのルーティングに使用するドメインのホストゾーンのリンク済みの名前を選択します。ドメイン名は、VPC Lattice で定義されているカスタムドメインエンドポイントと一致する必要があります。
9. [Create record] (レコードを作成) を選択します。

   レコードはウィザードを使用して作成するか、[Switch to quick create] (クイック作成に切り替え) を選択します。
10. 次の値を指定します。

    ルーティングポリシー

    該当するルーティングポリシーを選択します。詳細については、「ルーティングポリシーの選択」を参照してください

    レコード名

    VPC Lattice サービスドメインエンドポイントへのトラフィックのルーティングに使用するドメイン名を入力します。デフォルト値はホストゾーンの名前です。

たとえば、ホストゾーンの名前が example.com で、[acme.example.com] を使用してトラフィックをディストリビューションにルーティングする場合、「acme」と入力します。

エイリアス

クイック作成レコード作成方法を使用している場合、[エイリアス] をオンにします。

値/トラフィックのルーティング先

[Alias to VPC Lattice service] (VPC Lattice サービスへのエイリアス) を選択します。VPC Lattice サービスドメインが作成されたリージョンを選択し、ステップ 5 で取得した値を選択します。

レコードタイプ

A – IPv4 アドレス、AAAA – IPv6 アドレス、デュアルスタックの場合はその両方を選択します。

ターゲットの正常性の評価

[No] (いいえ) を選択します。 ターゲットの状態の評価については、「ターゲットの正常性の評価」を参照してください。

11. [レコードを作成] を選択します。

他の AWS リソースへのトラフィックのルーティング

以下は、他のサービスにおいて、Route 53 を使用してトラフィックをルーティングする方法を記載した各ガイダンスの一覧です。

- AWS Cloud Map ユーザーガイドの AWS Cloud Mapを使用。
- デ AWS App Runner ベロッパーガイドのカスタムドメインを管理します。
- [AWS Transfer Family user guide] (ユーザーガイド) の [Using Route 53 as a DNS provider] (DNS プロバイダーとしての Route 53 の使用)。
- Route 53 を使用してドメインを Amazon Lightsail インスタンスにポイントします。

Amazon Route 53 ヘルスチェックの作成

Amazon Route 53 ヘルスチェックでは、ウェブアプリケーション、ウェブサーバー、その他のリソースの正常性とパフォーマンスを監視します。作成した各ヘルスチェックは、次の方法のいずれかでモニタリングできます。

- ウェブサーバーなどの指定されたリソースのヘルスチェック
- そのほかのヘルスチェックのステータス
- Amazon CloudWatch アラームの状態
- さらに、Amazon Application Recovery Controller (ARC) を使用すると、DNS フェイルオーバーレコードを使用してルーティングコントロールのヘルスチェックをセットアップして、アプリケーションのトラフィックフェイルオーバーを管理できます。詳細については、「Amazon Application Recovery Controller (ARC) デベロッパーガイド」を参照してください。

ヘルスチェックの種類に関する概要については、「Amazon Route 53 ヘルスチェックの種類」を参照してください。ヘルスチェックの作成の詳細については、「ヘルスチェックの作成と更新」を参照してください。

ヘルスチェックの作成後、ヘルスチェックのステータスを確認する、ステータスが変更したときに通知を受け取る、そして DNS フェイルオーバーを設定できます。

ヘルスチェックのステータスと通知を表示する

ヘルスチェックの現在と最近のステータスをRoute 53 コンソールで表示できます。また、 AWS SDKs、、または Route 53 API のいずれかを使用して AWS Command Line Interface AWS Tools for Windows PowerShell、プログラムでヘルスチェックを使用することもできます。

ヘルスチェックのステータスが変更されたときに通知を受け取るには、各ヘルスチェックに Amazon CloudWatch アラームを設定できます。

ヘルスチェックのステータス表示と通知の受信の詳細については、「ヘルスチェックのステータス監視と通知の受信」を参照してください。

DNS フェイルオーバーの設定

同じ機能を実行するリソースが複数ある場合は、Route 53 がトラフィックを異常なリソースから正常なリソースにルーティングするように DNS フェイルオーバーを設定できます。例えば、2 つのウェブサーバーがあり、そのうち 1 つのウェブサーバーが異常になった場合、Route 53 はもう

1 つのウェブサーバーにトラフィックをルーティングできます。詳細については、「DNS フェイルオーバーの設定」を参照してください。

トピック

- Amazon Route 53 ヘルスチェックの種類
- Amazon Route 53 でヘルスチェックの正常性を判断する方法
- ヘルスチェックの作成、更新、削除
- DNS フェイルオーバーの設定
- ヘルスチェックの名前付けとタグ付け
- Amazon Route 53 API バージョン 2012-12-12 未満でのヘルスチェックの使用

Amazon Route 53 ヘルスチェックの種類

種類の Amazon Route 53 ヘルスチェックを作成できます。

エンドポイントをモニタリングするヘルスチェック

IP アドレスあるいはドメイン名で特定するエンドポイントをモニタリングするヘルスチェックを設定できます。指定された一定の間隔で、Route 53 は、自動リクエストをインターネット経由でアプリケーションやサーバーなどのリソースに送信して、そのリソースが到達可能、使用可能、機能中であることを確認します。オプションで、ユーザーが行ったものと同様のリクエスト (特定の URL へのウェブページのリクエストなど) を行うように、ヘルスチェックを設定できます。

他のヘルスチェック (算出したヘルスチェック) を監視するヘルスチェック

他のヘルスチェックの正常または異常の判断を、Route 53 が行うべきかどうかをモニタリングする、ヘルスチェックを作成できます。この方法が便利な状況のひとつが、複数のウェブサーバーなどの同じ機能を実行する複数のリソースがあるときに、最低限のリソースが正常であるかどうかに重点を置く場合です。ヘルスチェックの通知設定をせずに、各リソースにヘルスチェックを作成できます。続いて、そのほかのヘルスチェックのステータスをモニタリングするヘルスチェックを作成し、利用できるウェブリソース数が指定するしきい値を下回る場合に通知を行うように設定できます。

CloudWatch アラームをモニタリングするヘルスチェック

Amazon DynamoDB データベースへのスロットル読み込みイベント数や正常に機能していると推測される Elastic Load Balancing ホストの数などの CloudWatch メトリクスのステータスをモニタリングする CloudWatch アラームを作成できます。アラームを作成したら、そのアラームをモ

ニタリングする CloudWatch と同じデータストリームをモニタリングするヘルスチェックを作成できます。

耐障害性と可用性を向上させるため、Route 53 は CloudWatch アラーム が ALARM 状態になるまで待ちません。ヘルスチェックのステータスの正常から異常への変更は、CloudWatch アラームのデータストリームと基準に基づいて発生します。

Route 53 は、以下の機能で CloudWatch アラームをサポートしています。

- 標準解像度メトリクス。高解像度のメトリクスはサポートされていません。詳細については、Amazon CloudWatch ユーザーガイドの「高解像度メトリクス」を参照してください。
- 統計: 平均値、最小値、最大値、合計値、およびサンプル数。拡張統計はサポートされていません。
- Route 53 では、「N 個中 M 個」のアラームはサポートされていません。詳細については、Amazon CloudWatch ユーザーガイドの「アラームの評価」を参照してください。
- ヘルスチェックは、ヘルスチェックと同じ AWS アカウントに存在する CloudWatch アラームのみをモニタリングできます。
- Route 53 は、Metric Math を使用して複数の CloudWatch メトリクスをクエリするアラームをサポートしていません。

Amazon Application Recovery Controller (ARC) ルーティングコントローラー

ARC のヘルスチェックは、ルーティングコントロールに関連付けられ、オンまたはオフの単純切り替えになっています。フェールオーバー DNS レコードでルーティングコントロールのヘルスチェックをそれぞれ設定します。その後、ARC でルーティングコントロールを更新してトラフィックを再ルーティングし、アベイラビリティーゾーンや AWSリージョンをまたいでアプリケーションにフェイルオーバーできます。詳細については、ARC デベロッパーガイドの「ARC でのルーティングコントロール」を参照してください。

Amazon Route 53 でヘルスチェックの正常性を判断する方法

ヘルスチェックが正常かどうかを判断するために Amazon Route 53 が使用する方法は、ヘルスチェックのタイプによって異なります。

Route 53 がエンドポイントをモニタリングするヘルスチェックのステータスを決定する方法

Route 53 は、世界各地にヘルスチェッカーを持っています。エンドポイントをモニタリングするヘルスチェックを作成すると、ヘルスチェッカーは、エンドポイントが正常であるかどうかを判断する

ためにユーザーが指定するエンドポイントにリクエストの送信を開始します Route 53 で使用する口ケーションを選択することや、チェックの間隔 (10 秒ごとまたは 30 秒ごと) を指定することができます。異なるデータセンターの Route 53 ヘルスチェッカーは互いに調整しないため、選択した間隔に関係なく、1 秒あたり複数のリクエストを受け取った後、数秒間はヘルスチェックを受け取らないということが生じる場合があります。

各ヘルスチェッカーは、次の 2 つの値に基づいてエンドポイントの正常性を評価します。

- 応答時間。さまざまな理由から、ヘルスチェックリクエストに対するリソースの応答が遅くなったり、応答に失敗したりすることがあります。例えば、リソースがメンテナンスのためにシャットダウンしている、分散サービス妨害 (DDoS) 攻撃にあっている、ネットワークがダウンしている、などの理由です。
- エンドポイントが、指定した連続する回数のヘルスチェックに応答するかどうか (失敗のしきい値)

Route 53 はヘルスチェッカーからデータを集計し、エンドポイントが正常であるかどうかを判断します。

- 18% を超えるヘルスチェッカーがエンドポイントを正常であるとレポートした場合、Route 53 はそのエンドポイントを正常と見なします。
- 18% 以下のヘルスチェッカーがエンドポイントを正常であるとレポートした場合、Route 53 はそのエンドポイントを異常と見なします。

18% の値は、複数のリージョンのヘルスチェッカーがエンドポイントを正常と見なすように選択されました。これにより、ネットワークの状態によって一部のヘルスチェックの場所からエンドポイントが分離されたというだけで、エンドポイントを異常と見なすことを回避できます。この値は、将来のリリースで変更される可能性があります。

個々のヘルスチェッカーが、エンドポイントが正常であるかどうかを判断するために使用する応答時間は、ヘルスチェックのタイプによって異なります。

- HTTP/HTTPS ヘルスチェック – Route 53 が、エンドポイントとの TCP 接続を 4 秒以内に確立できることが必要です。加えて、接続後 2 秒以内に、HTTP ステータスコード 2xx または 3xx でエンドポイントが応答する必要があります。

> **Note**
>
> HTTPS ヘルスチェックでは SSL/TLS 証明書が検証されないため、証明書が無効または期限切れの場合でもチェックが不合格になることはありません。

- TCP ヘルスチェック: Route 53 が、エンドポイントとの TCP 接続を 10 秒以内に確立できることが必要です。
- HTTP/HTTPS ヘルスチェックと文字列一致: HTTP/HTTPS ヘルスチェックと同様に、Route 53 はエンドポイントとの TCP 接続を 4 秒以内に確立し、そのエンドポイントは接続後 2 秒以内に 2xx または 3xx の HTTP ステータスコードで応答する必要があります。

  Route 53 ヘルスチェッカーは、HTTP ステータスコードを受信後、続けて 2 秒以内にエンドポイントからレスポンス本文を受信する必要があります。Route 53 は、指定された文字列をレスポンス本文から検索します。その際、検索文字列全体が、レスポンス本文の最初の 5,120 バイト内に出現している必要があります。それ以外の場合、エンドポイントはヘルスチェックで不合格となります。Route 53 コンソールを使用している場合は、文字列の検索 フィールドに文字列を指定します。Route 53 API を使用している場合は、ヘルスチェックの作成時に、`SearchString` 要素で文字列を指定します。

エンドポイントを監視するヘルスチェック (TCP ヘルスチェックを除く) で、エンドポイントからの応答にヘッダーが含まれている場合、ヘッダーは RFC7230、Hypertext Transfer Protocol (HTTP/1.1): メッセージ構文とルーティング、セクション 3.2、「ヘッダーフィールド」で定義されている形式でなければなりません。

Route 53 は、実際のステータス (正常または非正常) を決定するための十分なデータを得るまでは、新しいヘルスチェックを正常と見なします。ヘルスチェックのステータスを反転するオプションを選択した場合、Route 53 は、十分なデータを得るまでは、新しいヘルスチェックを非正常と見なします。

Route 53 が他のヘルスチェックをモニタリングするヘルスチェックのステータスを決定する方法

ヘルスチェックは、他のヘルスチェックのステータスをモニタリングできます。このタイプのヘルスチェックは、算出したヘルスチェックとして知られています。監視を行うヘルスチェックが親ヘルスチェックで、監視されるヘルスチェックが子ヘルスチェックです。1 つの親ヘルスチェックは、最大 255 の子ヘルスチェックの状態を監視できます。以下に、監視活動の仕組みを示します。

- Route 53 は、正常であると考えられる子のヘルスチェックの数を合計します。
- Route 53 はその後、正常と見なされる親のヘルスチェックのステータスについて正常でなければならない子ヘルスチェック数と、その数を比較します。

詳細については、「ヘルスチェックを作成または更新するときに指定する値」の 他のヘルスチェック (算出したヘルスチェック) の監視 を参照してください。

Route 53 は、実際のステータス (正常または非正常) を決定するための十分なデータを得るまでは、新しいヘルスチェックを正常と見なします。ヘルスチェックのステータスを反転するオプションを選択した場合、Route 53 は、十分なデータを得るまでは、新しいヘルスチェックを非正常と見なします。

Route 53 が CloudWatch アラームをモニタリングするヘルスチェックのステータスを決定する方法

CloudWatch アラームに基づくヘルスチェックを作成した場合、Route 53 は該当するアラームの状態ではなくそのアラームのデータストリームをモニタリングします。データストリームがアラームの状態を [OK] と示している場合、ヘルスチェックは正常と見なされます。データストリームが状態を [アラーム] と示している場合、ヘルスチェックは異常と見なされます。アラームの状態を判断するための十分な情報がデータストリームから提供されない場合、ヘルスチェックのステータスは [ヘルスチェックステータス] の設定 (正常、異常、または最後の既知の状態) によって決まります (Route 53 API では、この設定は `InsufficientDataHealthStatus` です)。

Route 53 では、クロスアカウント CloudWatch アラームをサポートしていません。

> **Note**
>
> Route 53 のヘルスチェックでは、CloudWatch アラームの状態ではなく CloudWatch のデータストリームがモニタリングされるため、 CloudWatch の SetAlarmState API オペレーションを使用してヘルスチェックのステータスを強制的に変更することはできません。

Route 53 は、実際のステータス (正常または非正常) を決定するための十分なデータを得るまでは、新しいヘルスチェックを正常と見なします。ヘルスチェックのステータスを反転するオプションを選択した場合、Route 53 は、十分なデータを得るまでは、新しいヘルスチェックを非正常と見なします。

ヘルスチェックの作成、更新、削除

> **Important**
>
> これらの手順に進む前に、レコードに関連付けられているヘルスチェックを更新または削除する場合は、「DNS フェイルオーバーが設定されている場合のヘルスチェックの更新または削除」のタスクを確認してください。

このセクションでは、Route 53 ヘルスチェックの管理に関連する以下のトピックについて説明します。

1. ヘルスチェックの作成と更新:
   - Route 53 コンソールを使用してヘルスチェックを作成および更新する方法について説明します。
   - エンドポイントモニタリング、プロトコル、IP アドレス、ドメイン名、高度な設定オプションなど、ヘルスチェックを作成または更新するときに指定する必要がある値を理解します。
2. ヘルスチェックの作成時に表示される値:
   - 完全な URL や IP アドレス、ポートなど、ヘルスチェックを作成するときに Route 53 コンソールが入力内容に基づいて表示する値を確認します。
3. CloudWatch アラーム変更のヘルスチェックの更新:
   - 関連する CloudWatch アラームの設定を変更するときにヘルスチェックを更新する方法について説明します。
4. ヘルスチェックの削除:
   - Route 53 コンソールを使用してヘルスチェックを削除する手順に従います。
5. DNS フェイルオーバーが設定されている場合のヘルスチェックの更新または削除:
   - DNS レコードに関連付けられたヘルスチェックを更新または削除するときに実行する推奨タスクについて説明します。このタスクを実行することにより、適切なルーティングとフェイルオーバーの設定が保証されます。
6. ルーターとファイアウォールのルールの設定:
   - Route 53 ヘルスチェッカーからのインバウンドトラフィックを許可し、ヘルスチェックが成功するようにルーターとファイアウォールのルールを設定する方法を理解します。

このセクションの情報にしたがって、Route 53 ヘルスチェックの作成、更新、削除を効果的に行い、設定を管理して、DNS フェイルオーバーおよびルーティングポリシーとの適切な統合を確認することができます。

トピック

- ヘルスチェックの作成と更新
- ヘルスチェックを作成または更新するときに指定する値
- ヘルスチェックを作成すると Amazon Route 53 が表示する値
- CloudWatch アラーム設定を変更する場合のヘルスチェックの更新 (CloudWatch アラームのみをモニタリングするヘルスチェック)
- ヘルスチェックの無効化または有効化
- ヘルスチェックの反転
- ヘルスチェックの削除
- DNS フェイルオーバーが設定されている場合のヘルスチェックの更新または削除
- Amazon Route 53 のヘルスチェックができるようにルーターとファイアウォールのルールを設定する

ヘルスチェックの作成と更新

以下の手順では、Route 53 コンソールを使用してヘルスチェックを作成したり更新したりする方法について説明します。

> **Note**
>
> Route 53 はヘルスチェックコンソールを更新しています。旧コンソールは移行期間中も引き続きご使用いただけます。

お使いのコンソールのタブを選択します。

- 新しいコンソール
- 旧コンソール

New console

ヘルスチェックを作成または更新するには

1. 既にレコードに関連付けられているヘルスチェックを更新する場合は、「DNS フェイルオーバーが設定されている場合のヘルスチェックの更新または削除」で推奨されているタスクを実行します。
2. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
3. ナビゲーションペインで [Health Checks (ヘルスチェック)] を選択します。
4. 既存のヘルスチェックを更新する場合は、ヘルスチェックのリンクされた ID を選択してから、[編集] を選択します。

   ヘルスチェックを作成する場合は、[ヘルスチェックを作成] を選択します。
5. 適切な値を入力します。一部の値はヘルスチェックの作成後に変更できないのでご注意ください。詳細については、ヘルスチェックを作成または更新するときに指定する値を参照してください。
6. [ヘルスチェックの作成] を選択します。

   > **Note**
   >
   > Route 53 は、実際のステータス (正常または非正常) を決定するための十分なデータを得るまでは、新しいヘルスチェックを正常と見なします。
7. 1 つまたは複数の Route 53 レコードにヘルスチェックを関連付けます。レコードの作成と更新については、「レコードを使用する」を参照してください。

Old console

ヘルスチェックを作成または更新するには

1. 既にレコードに関連付けられているヘルスチェックを更新する場合は、「DNS フェイルオーバーが設定されている場合のヘルスチェックの更新または削除」で推奨されているタスクを実行します。
2. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
3. ナビゲーションペインで [ヘルスチェック] を選択します。

4. 既存のヘルスチェックを更新する場合は、目的のヘルスチェックを選択してから、[Edit Health Check] を選択します。

   ヘルスチェックを作成する場合は、[Create Health Check] を選択します。各設定の詳細については、ラベルの上にマウスポインタを移動してツールヒントを表示してください。
5. 適切な値を入力します。一部の値はヘルスチェックの作成後に変更できないのでご注意ください。詳細については、ヘルスチェックを作成または更新するときに指定する値を参照してください。
6. ヘルスチェックの作成 を選択します。

   > **Note**
   >
   > Route 53 は、実際のステータス (正常または非正常) を決定するための十分なデータを得るまでは、新しいヘルスチェックを正常と見なします。ヘルスチェックのステータスを反転するオプションを選択した場合、Route 53 は、十分なデータを得るまでは、新しいヘルスチェックを非正常と見なします。
7. 1 つまたは複数の Route 53 レコードにヘルスチェックを関連付けます。レコードの作成と更新については、「レコードを使用する」を参照してください。

ヘルスチェックを作成または更新するときに指定する値

ヘルスチェックを作成または更新する際は、該当する値を指定します。一部の値はヘルスチェックの作成後に変更できないのでご注意ください。

トピック

- エンドポイントの監視
- 他のヘルスチェック (算出したヘルスチェック) の監視
- CloudWatch アラームのモニタリング
- 高度な設定 (「エンドポイントを監視」する場合のみ)
- ヘルスチェックが失敗した場合の通知を取得する

名前

オプション (ただし推奨) : ヘルスチェックに割り当てる名前。[名前] に値が指定された場合、Route 53 は、ヘルスチェックにタグを追加し、そのタグのキーに Name という値を割り当

てたうえで、指定された値をタグの値に割り当てます。Name タグの値は Route 53 コンソールのヘルスチェックのリストに表示されるため、ヘルスチェックを簡単に区別できます。

タグ付けとヘルスチェックの詳細については、「ヘルスチェックの名前付けとタグ付け」を参照してください。

モニタリングの対象

このヘルスチェックで、エンドポイントを監視するか、または他のヘルスチェックのステータスを監視するか。

- エンドポイント: Route 53 は指定したエンドポイントの状態を監視します。ドメイン名または IP アドレスとポートを指定して、エンドポイントを指定できます。

  > **Note**
  >
  > AWS エンドポイント以外の を指定すると、追加料金が適用されます。 AWS エンドポイントの定義などの詳細については、Route 53 料金表の「ヘルスチェック」を参照してください。

- 他のヘルスチェック (計算されたヘルスチェック) のステータス: Route 53 は、指定した他のヘルスチェックの状態に基づいてこの状態チェックが正常であるかどうかを決定します。このヘルスチェックが正常であると判断されるために必要なヘルスチェック数も指定します。
- CloudWatch アラームのデータストリームの状態 - Route 53 は、CloudWatch アラームのデータストリームをモニタリングして、このヘルスチェックが正常かどうかを判断します。

エンドポイントの監視

> **Note**
>
> Route 53 はヘルスチェックコンソールを更新しています。旧コンソールは移行期間中も引き続きご使用いただけます。

お使いのコンソールのタブを選択します。

- 新しいコンソール
- 旧コンソール

New console

このヘルスチェックでエンドポイントを監視する場合、以下の値を指定します。

- エンドポイントの指定
- IP アドレス
- ドメイン名

エンドポイントの指定

IP アドレスまたはドメイン名を使用してエンドポイントを指定するかどうか。

ヘルスチェックの作成後は、[Specify endpoint by] の値を変更できません。

IP アドレス ([IP アドレスでエンドポイントを指定する] を選択した場合のみ)

ドロップダウンでプロトコルを選択して、テキストボックスに IP アドレス、ポート、パスを入力します。

- プロトコルは次のいずれかになります。

  HTTP: Route 53 は TCP 接続を確立しようとします。成功した場合、 Route 53 は HTTP リクエストを送信し、2xx または 3xx の HTTP ステータスコードを待機します。

- HTTPS: Route 53 は TCP 接続を確立しようとします。成功した場合、Route 53 は HTTPS リクエストを送信し、2xx または 3xx の HTTP ステータスコードを待機します。

  > **Important**
  >
  > [HTTPS] を選択する場合は、エンドポイントが TLS v1.0、v1.1、または v1.2 をサポートする必要があります。

  プロトコルの値に HTTPS を選択すると、追加料金が適用されます。詳細については、「Route 53 料金表」を参照してください。

- TCP: Route 53 は TCP 接続を確立しようとします。

詳細については、「Amazon Route 53 でヘルスチェックの正常性を判断する方法」を参照してください。

ヘルスチェックの作成後は、[Protocol] の値を変更できません。

[IP アドレス] では、[IP アドレスでエンドポイントを指定する] を選択した場合、Route 53 でヘルスチェックを実行するエンドポイントの IPv4 または IPv6 アドレスを入力できます。

エンドポイントの IP アドレスの範囲がローカル、プライベート、ルーティング範囲外、マルチキャストのいずれかに該当する場合、Route 53 は、エンドポイントの正常性をチェックできません。ヘルスチェックを作成できない IP アドレスの詳細については、以下のドキュメントを参照してください。

- RFC 5735, Special Use IPv4 Addresses (RFC 5735、特殊用途のIPv4アドレス)
- RFC 6598, IANA-Reserved IPv4 Prefix for Shared Address Space (RFC 6598、IANA-共有アドレス空間用に予約されたIPv4プレフィックス)。
- RFC 5156, Special-Use IPv6 Addresses (RFC 5156、特殊用途のIPv6アドレス)

エンドポイントが Amazon EC2 インスタンスである場合は、Elastic IP アドレス を作成して EC2 インスタンスに関連付け、Elastic IP アドレスを指定するようお勧めします。これによってインスタンスの IP アドレスが固定されます。詳細については、「Amazon EC2 ユーザーガイド」の「Elastic IP アドレス (EIP)」を参照してください。

Amazon EC2 インスタンスを削除する場合、EIP に関連付けられているヘルスチェックも削除してください。詳細については、「Amazon Route 53 ヘルスチェックのベストプラクティス」を参照してください。

> **Note**
>
> AWS エンドポイント以外の を指定すると、追加料金が適用されます。 AWS エンドポイントの定義などの詳細については、Route 53 料金表の「ヘルスチェック」を参照してください。

[ポート] では、Route 53 でヘルスチェックを実行するエンドポイントにポートを入力します。

[パス (HTTP および HTTPS プロトコルの場合のみ)] では、ヘルスチェックの実行時に Route 53 がリクエストするパスを入力します。エンドポイントが正常であるときに、2xx または 3xx の HTTP ステータスコードが返されるパスを指定してください (ファイル /docs/route53-health-check.html など)。クエリ文字列パラメータを含めることもできます (例: /welcome.html?language=jp&login=y)。先頭がスラッシュ文字 (/) でない場合、Route 53 はスラッシュ文字を自動的に追加します。

ドメイン名 (すべてのプロコルで、[エンドポイントをドメイン名で指定する] を選択した場合のみ)

[エンドポイントをドメイン名で指定する] を選択した場合の、Route 53 でヘルスチェックを実行するエンドポイントのドメイン名 (example.com) またはサブドメイン名 (backend.example.com)。

エンドポイントをドメイン名で指定するように選択した場合、Route 53 は [ドメイン名] に指定したドメイン名を解決するための DNS クエリを、[リクエスト間隔] に指定した間隔で送信します。DNS が返す IP アドレスを使用して、Route 53 はエンドポイントの正常性を確認します。

> **Note**
>
> ドメイン名で エンドポイントを指定した場合、Route 53 は、IPv4 のみを使用して、ヘルスチェックをエンドポイントに送信します。[Domain name] に指定した名前のタイプ A のレコードがない場合、ヘルスチェックは「DNS 解決策失敗」エラーで失敗します。

フェイルオーバー、位置情報、地理的近接性、レイテンシー、複数値、または加重のいずれかのレコードについて正常性をチェックする場合で、かつエンドポイントをドメイン名で指定した場合は、エンドポイントごとにヘルスチェックを作成することをお勧めします。例えば、www.example.com のコンテンツを配信する各 HTTP サーバーについて、ヘルスチェックを作成します。[Domain name] の値には、レコードの名前 (www.example.com) ではなく、サーバーのドメイン名 (us-east-2-www.example.com など) を指定します。

> **Important**
>
> この構成で、[ドメイン名] の値がレコードの名前と一致するヘルスチェックを作成し、それらのレコードにヘルスチェックを関連付けた場合、ヘルスチェックで予想できない結果が生じます。

さらに、[Protocol] の値が [HTTP] または [HTTPS] である場合、前述の [Host name] (ホスト名) で説明したように、`Host` ヘッダーの [Domain name] (ドメイン名) の値が Route 53 から渡されます。[Protocol] の値が [TCP] である場合、Route 53 は `Host` ヘッダーを渡しません。

> **Note**
>
> AWS エンドポイント以外の を指定すると、追加料金が適用されます。 AWS エンドポイントの定義などの詳細については、Route 53 料金表の「ヘルスチェック」を参照してください。

Old console

このヘルスチェックでエンドポイントを監視する場合、以下の値を指定します。

- エンドポイントの指定
- プロトコル
- IP アドレス
- ホスト名
- ポート
- ドメイン名
- パス

エンドポイントの指定

IP アドレスまたはドメイン名を使用してエンドポイントを指定するかどうか。

ヘルスチェックの作成後は、[Specify endpoint by] の値を変更できません。

プロトコル

エンドポイントの正常性をチェックする際に Route 53 が使用する方法。

- HTTP: Route 53 は TCP 接続を確立しようとします。成功した場合、 Route 53 は HTTP リクエストを送信し、2xx または 3xx の HTTP ステータスコードを待機します。
- HTTPS: Route 53 は TCP 接続を確立しようとします。成功した場合、Route 53 は HTTPS リクエストを送信し、2xx または 3xx の HTTP ステータスコードを待機します。

> **Important**
>
> [HTTPS] を選択する場合は、エンドポイントが TLS v1.0、v1.1、または v1.2 をサポートする必要があります。

プロトコルの値に HTTPS を選択すると、追加料金が適用されます。詳細については、「Route 53 料金表」を参照してください。

- TCP: Route 53 は TCP 接続を確立しようとします。

詳細については、「Amazon Route 53 でヘルスチェックの正常性を判断する方法」を参照してください。

ヘルスチェックの作成後は、[Protocol] の値を変更できません。

IP アドレス ([IP アドレスでエンドポイントを指定する] を選択した場合のみ)

Route 53 でヘルスチェックを実行するエンドポイントの IPv4 または IPv6 アドレス ([IP アドレスでエンドポイントを指定する] を選択した場合のみ)。

エンドポイントの IP アドレスの範囲がローカル、プライベート、ルーティング範囲外、マルチキャストのいずれかに該当する場合、Route 53 は、エンドポイントの正常性をチェックできません。ヘルスチェックを作成できない IP アドレスの詳細については、以下のドキュメントを参照してください。

- RFC 5735, Special Use IPv4 Addresses (RFC 5735、特殊用途のIPv4アドレス)
- RFC 6598, IANA-Reserved IPv4 Prefix for Shared Address Space (RFC 6598、IANA-共有アドレス空間用に予約されたIPv4プレフィックス)。
- RFC 5156, Special-Use IPv6 Addresses (RFC 5156、特殊用途のIPv6アドレス)

エンドポイントが Amazon EC2 インスタンスである場合は、Elastic IP アドレス を作成して EC2 インスタンスに関連付け、Elastic IP アドレスを指定するようお勧めします。これによってインスタンスの IP アドレスが固定されます。詳細については、「Amazon EC2 ユーザーガイド」の「Elastic IP アドレス (EIP)」を参照してください。

Amazon EC2 インスタンスを削除する場合、EIP に関連付けられているヘルスチェックも削除してください。詳細については、「Amazon Route 53 ヘルスチェックのベストプラクティス」を参照してください。

> **Note**
>
> AWS エンドポイント以外の を指定すると、追加料金が適用されます。 AWS エンドポイントの定義などの詳細については、Route 53 料金表の「ヘルスチェック」を参照してください。

ホスト名 ([IP アドレスでエンドポイントを指定する] を選択した場合で、HTTP および HTTPSの場合のみ)

HTTP/HTTPS ヘルスチェックで Route 53 から `Host` ヘッダーに渡す値。通常は、Route 53 でヘルスチェックを実行するウェブサイトの完全修飾 DNS 名を指定します。Route 53 がエンドポイントの正常性をチェックするときに、`Host` ヘッダーがどのように構築されるかを以下に示します。

- [Protocol] の [Port] と [HTTP] に **`80`** の値を指定すると、Route 53 は ホスト名の値を含んだ `Host` ヘッダーをエンドポイントに渡します。
- [Protocol] の [Port] と [HTTP] に **`443`** の値を指定すると、Route 53 は ホスト名の値を含んだ `Host` ヘッダーをエンドポイントに渡します。
- [Protocol] の [Port] と [HTTP] または [HTTPS] に 別の値を指定すると、Route 53 は *`###`*`#:`*`Port`*の値を含んだ `Host` ヘッダーをエンドポイントに渡します。

エンドポイントを IP アドレスで指定することを選択し、ホスト名に値を指定しない場合、Route 53 は `Host` ヘッダーの IP アドレスの値を、以前の値に置き換えます。

ポート

Route 53 でヘルスチェックを実行するエンドポイント上のポート。

ドメイン名 (すべてのプロコルで、[エンドポイントをドメイン名で指定する] を選択した場合のみ)

[エンドポイントをドメイン名で指定する] を選択した場合の、Route 53 でヘルスチェックを実行するエンドポイントのドメイン名 (example.com) またはサブドメイン名 (backend.example.com)。

エンドポイントをドメイン名で指定するように選択した場合、Route 53 は [ドメイン名] に指定したドメイン名を解決するための DNS クエリを、[リクエスト間隔] に指定した間隔で送信します。DNS が返す IP アドレスを使用して、Route 53 はエンドポイントの正常性を確認します。

> **Note**
>
> ドメイン名で エンドポイントを指定した場合、Route 53 は、IPv4 のみを使用して、ヘルスチェックをエンドポイントに送信します。[Domain name] に指定した名前のタイプ A のレコードがない場合、ヘルスチェックは「DNS 解決策失敗」エラーで失敗します。

フェイルオーバー、位置情報、地理的近接性、レイテンシー、複数値、または加重のいずれかのレコードについて正常性をチェックする場合で、かつエンドポイントをドメイン名で指定した場合は、エンドポイントごとにヘルスチェックを作成することをお勧めします。例えば、www.example.com のコンテンツを配信する各 HTTP サーバーについて、ヘルスチェックを作成します。[Domain name] の値には、レコードの名前 (www.example.com) ではなく、サーバーのドメイン名 (us-east-2-www.example.com など) を指定します。

> **Important**
>
> この構成で、[ドメイン名] の値がレコードの名前と一致するヘルスチェックを作成し、それらのレコードにヘルスチェックを関連付けた場合、ヘルスチェックで予想できない結果が生じます。

さらに、[Protocol] の値が [HTTP] または [HTTPS] である場合、前述の [Host name] (ホスト名) で説明したように、`Host` ヘッダーの [Domain name] (ドメイン名) の値が Route 53 から渡されます。[Protocol] の値が [TCP] である場合、Route 53 は `Host` ヘッダーを渡しません。

> **Note**
>
> AWS エンドポイント以外の を指定すると、追加料金が適用されます。 AWS エンドポイントの定義などの詳細については、Route 53 料金表の「ヘルスチェック」を参照してください。

パス (HTTP および HTTPS プロトコルの場合のみ)

ヘルスチェックの実行時に Route 53 でリクエストするパス。エンドポイントが正常であるときに、`2xx` または `3xx` の HTTP ステータスコードが返されるパスを指定してください (ファイル `/docs/route53-health-check.html` など)。クエリ文字列パラメータ (`/welcome.html?language=jp&login=y` など) を含めることもできます。先頭がスラッシュ文字 (/) でない場合、Route 53 はスラッシュ文字を自動的に追加します。

他のヘルスチェック (算出したヘルスチェック) の監視

> **Note**
>
> Route 53 はヘルスチェックコンソールを更新しています。旧コンソールは移行期間中も引き続きご使用いただけます。

お使いのコンソールのタブを選択します。

- 新しいコンソール
- 旧コンソール

New console

このヘルスチェックで他のヘルスチェックのステータスを監視する場合、以下の値を指定します。

- 監視対象のヘルスチェック
- 次の場合に正常であると報告します。

監視対象のヘルスチェック

Route 53 で監視するヘルスチェック。監視によりヘルスチェックの状態を判断します。

[Health checks to monitor] に最大 256 個のヘルスチェックを追加できます。リストからヘルスチェックを削除するには、対象のヘルスチェックの強調表示部分の右にある [x] を選択します。

> **Note**
>
> 算出したヘルスチェックを、算出したその他のヘルスチェックの状態を監視するように設定することはできません。

算出したヘルスチェックの監視対象であるヘルスチェックを無効にすると、Route 53 は無効にしたヘルスチェックを正常であるとみなした上で、算出したヘルスチェックが正常かどうか

を計算します。無効にしたヘルスチェックが異常とみなされるようにするには、[Invert health check status (ヘルスチェックのステータスの反転)] チェックボックスをオンにします。

次の場合に正常であると報告します。

このヘルスチェックが正常かどうかを判断するために、Route 53 で実行する計算

- [選択したヘルスチェック y 個のうち少なくとも x 個が正常な場合に正常と報告する]: Route 53 は、[モニターするヘルスチェック] に追加したヘルスチェックのうち指定数のヘルスチェックが正常である場合に、そのヘルスチェックが正常であると見なします。次の点に注意してください。
  - [モニターするヘルスチェック] に指定したヘルスチェックの数より大きい数値を指定した場合、Route 53 は必ずこのヘルスチェックに不具合があると見なします。
  - 0 を指定した場合、Route 53 は常にこのヘルスチェックが正常であると見なします。
- [すべてのヘルスチェックが正常である場合に正常であると報告する (AND)]: Route 53 は、[モニターするヘルスチェック] に追加したヘルスチェックがすべて正常である場合にのみ、このヘルスチェックを正常であると見なします。
- [1 つ以上のヘルスチェックが正常な場合に正常と報告する (OR)]: Route 53 は、[モニターするヘルスチェック] に追加したヘルスチェックのうち少なくとも 1 つが正常である場合に、このヘルスチェックが正常であると見なします。

Old console

このヘルスチェックで他のヘルスチェックのステータスを監視する場合、以下の値を指定します。

- 監視対象のヘルスチェック
- 次の場合に正常であると報告します。
- ヘルスチェックのステータスを反転させる
- Disabled

監視対象のヘルスチェック

Route 53 で監視するヘルスチェック。監視によりヘルスチェックの状態を判断します。

[Health checks to monitor] に最大 256 個のヘルスチェックを追加できます。リストからヘルスチェックを削除するには、対象のヘルスチェックの強調表示部分の右にある [x] を選択します。

> **Note**
>
> 算出したヘルスチェックを、算出したその他のヘルスチェックの状態を監視するように設定することはできません。

算出したヘルスチェックの監視対象であるヘルスチェックを無効にすると、Route 53 は無効にしたヘルスチェックを正常であるとみなした上で、算出したヘルスチェックが正常かどうかを計算します。無効にしたヘルスチェックが異常とみなされるようにするには、[Invert health check status (ヘルスチェックのステータスの反転)] チェックボックスをオンにします。

次の場合に正常であると報告します。

このヘルスチェックが正常かどうかを判断するために、Route 53 で実行する計算

- [選択したヘルスチェック y 個のうち少なくとも x 個が正常な場合に正常と報告する]: Route 53 は、[モニターするヘルスチェック] に追加したヘルスチェックのうち指定数のヘルスチェックが正常である場合に、そのヘルスチェックが正常であると見なします。次の点に注意してください。
  - [モニターするヘルスチェック] に指定したヘルスチェックの数より大きい数値を指定した場合、Route 53 は必ずこのヘルスチェックに不具合があると見なします。
  - 0 を指定した場合、Route 53 は常にこのヘルスチェックが正常であると見なします。
- [すべてのヘルスチェックが正常である場合に正常であると報告する (AND)]: Route 53 は、[モニターするヘルスチェック] に追加したヘルスチェックがすべて正常である場合にのみ、このヘルスチェックを正常であると見なします。
- [1 つ以上のヘルスチェックが正常な場合に正常と報告する (OR)]: Route 53 は、[モニターするヘルスチェック] に追加したヘルスチェックのうち少なくとも 1 つが正常である場合に、このヘルスチェックが正常であると見なします。

ヘルスチェックステータスを反転させる (古いコンソールのみ)

新しいコンソールでヘルスチェックを反転させるには、「ヘルスチェックの反転」を参照してください。

Route 53 でヘルスチェックのステータスを反転させるかどうかを選択します。このオプションを選択した場合、Route 53 はステータスが正常であればヘルスチェックに不具合があると見なします。逆も同様です。

無効 (古いコンソールのみ)

新しいコンソールでヘルスチェックを無効にするには、「ヘルスチェックの無効化または有効化」を参照してください。

Route 53 によるヘルスチェックの実行を停止させます。ヘルスチェックを無効にすると、Route 53 は、参照するヘルスチェックのステータスの集計を停止します。

ヘルスチェックを無効にすると、Route 53 は、そのヘルスチェックのステータスを常に正常とみなすようになります。DNS フェイルオーバーを設定した場合、Route 53 はトラフィックを引き続き該当するリソースにルーティングします。リソースへのトラックのルーティングを停止させるには、ヘルスチェックを反転させます。

> **Note**
>
> ヘルスチェックを無効にしても、ヘルスチェックの料金は適用されます。

CloudWatch アラームのモニタリング

> **Note**
>
> Route 53 はヘルスチェックコンソールを更新しています。旧コンソールは移行期間中も引き続きご使用いただけます。

お使いのコンソールのタブを選択します。

- 新しいコンソール
- 旧コンソール

New console

このヘルスチェックで CloudWatch アラームのアラーム状態を監視する場合は、以下の値を指定します。

- CloudWatch アラーム
- ヘルスチェックステータス

CloudWatch アラーム

このヘルスチェックが正常かどうかを判断するために Route 53 が使用する CloudWatch アラームを選択します。CloudWatch アラームは、ヘルスチェック AWS アカウント と同じ にある必要があります。

> **Note**
>
> Route 53 は、以下の機能で CloudWatch アラームをサポートしています。
>
> - 標準解像度メトリクス。高解像度のメトリクスはサポートされていません。詳細については、Amazon CloudWatch ユーザーガイド の「高解像度メトリクス」を参照してください。
> - 統計: `Average`、`Minimum`、`Maximum`、`Sum`、および `SampleCount`。拡張統計はサポートされていません。
> - Route 53 では、「N 個中 M 個」のアラームはサポートされていません。詳細については、Amazon CloudWatch ユーザーガイド の「アラームの評価」を参照してください。
>
> Route 53 は、Metric Math を使用して複数の CloudWatch メトリクスをクエリするアラームをサポートしていません。

アラームを作成する場合は、次の手順を実行します。

1. [作成] を選択します。ブラウザの新しいタブに CloudWatch コンソールが表示されます。
2. 適切な値を入力します。詳細については、Amazon CloudWatch ユーザーガイド の「CloudWatch アラームの作成または編集」を参照してください。
3. Route 53 コンソールが表示されているブラウザタブに戻ります。
4. [CloudWatch alarm] の横にある更新ボタンを選択します。
5. リストから新しいアラームを選択します。

> **Important**
>
> ヘルスチェックを作成したあとで CloudWatch アラームの設定を変更する場合、ヘルスチェックを更新する必要があります。詳細については、「CloudWatch アラーム設

定を変更する場合のヘルスチェックの更新 (CloudWatch アラームのみをモニタリングするヘルスチェック)」を参照してください。

ヘルスチェックステータス

CloudWatch アラームで選択したアラーム状態を判断するための、十分なデータが CloudWatch にない場合に、ヘルスチェックのステータス (正常、異常、または最後の既知の状態) を選択します。既知の最新ステータスを使用することを選択した場合、Route 53 は、アラームの状態を判断するための十分なデータが CloudWatch にあった最新のヘルスチェックのステータスを使用します。既知の最新ステータスがない新しいヘルスチェックの場合、ヘルスチェックのデフォルトステータスは "正常" になります。

ヘルスチェックステータスの値は、一時的に CloudWatch メトリクスのデータストリームを用できなかった場合の、一時的なステータスを提供します。(Route 53 は、対応するアラームの状態ではなく、CloudWatch メトリックスのデータストリームを監視します。) メトリクスが頻繁に、または長時間 (数時間以上) 使用できなくなる場合は、既知の最新ステータスを使用しないことをお勧めします。

Old console

このヘルスチェックで CloudWatch アラームのアラーム状態を監視する場合は、以下の値を指定します。

- CloudWatch アラーム
- ヘルスチェックステータス
- ヘルスチェックのステータスを反転させる
- Disabled

CloudWatch アラーム

このヘルスチェックが正常かどうかを判断するために Route 53 が使用する CloudWatch アラームを選択します。CloudWatch アラームは、ヘルスチェック AWS アカウント と同じ にある必要があります。

> **Note**
>
> Route 53 は、以下の機能で CloudWatch アラームをサポートしています。

- 標準解像度メトリクス。高解像度のメトリクスはサポートされていません。詳細については、Amazon CloudWatch ユーザーガイド の「高解像度メトリクス」を参照してください。
- 統計: `Average`、`Minimum`、`Maximum`、`Sum`、および `SampleCount`。拡張統計はサポートされていません。
- Route 53 では、「N 個中 M 個」のアラームはサポートされていません。詳細については、Amazon CloudWatch ユーザーガイド の「アラームの評価」を参照してください。

Route 53 は、Metric Math を使用して複数の CloudWatch メトリクスをクエリするアラームをサポートしていません。

アラームを作成する場合は、次の手順を実行します。

1. [作成] を選択します。ブラウザの新しいタブに CloudWatch コンソールが表示されます。
2. 適切な値を入力します。詳細については、Amazon CloudWatch ユーザーガイド の「CloudWatch アラームの作成または編集」を参照してください。
3. Route 53 コンソールが表示されているブラウザタブに戻ります。
4. [CloudWatch alarm] の横にある更新ボタンを選択します。
5. リストから新しいアラームを選択します。

> **Important**
>
> ヘルスチェックを作成したあとで CloudWatch アラームの設定を変更する場合、ヘルスチェックを更新する必要があります。詳細については、「CloudWatch アラーム設定を変更する場合のヘルスチェックの更新 (CloudWatch アラームのみをモニタリングするヘルスチェック)」を参照してください。

ヘルスチェックステータス

CloudWatch アラームで選択したアラーム状態を判断するための、十分なデータが CloudWatch にない場合に、ヘルスチェックのステータス (正常、異常、または最後の既知の状態) を選択します。既知の最新ステータスを使用することを選択した場合、Route 53 は、アラームの状態を判断するための十分なデータが CloudWatch にあった最新のヘルスチェックの

ステータスを使用します。既知の最新ステータスがない新しいヘルスチェックの場合、ヘルスチェックのデフォルトステータスは "正常" になります。

ヘルスチェックステータスの値は、一時的に CloudWatch メトリクスのデータストリームを用できなかった場合の、一時的なステータスを提供します。(Route 53 は、対応するアラームの状態ではなく、CloudWatch メトリックスのデータストリームを監視します。) メトリクスが頻繁に、または長時間 (数時間以上) 使用できなくなる場合は、既知の最新ステータスを使用しないことをお勧めします。

ヘルスチェックステータスを反転させる (古いコンソールのみ)

新しいコンソールでヘルスチェックを反転させるには、「ヘルスチェックの反転」を参照してください。

Route 53 でヘルスチェックのステータスを反転させるかどうかを選択します。このオプションを選択した場合、Route 53 はステータスが正常であればヘルスチェックに不具合があると見なします。逆も同様です。

無効 (古いコンソールのみ)

新しいコンソールでヘルスチェックを無効にするには、「ヘルスチェックの無効化または有効化」を参照してください。

Route 53 によるヘルスチェックの実行を停止させます。ヘルスチェックを無効にすると、Route 53 は該当する CloudWatch メトリクスのモニタリングを停止します。

ヘルスチェックを無効にすると、Route 53 は、そのヘルスチェックのステータスを常に正常とみなすようになります。DNS フェイルオーバーを設定した場合、Route 53 はトラフィックを引き続き該当するリソースにルーティングします。リソースへのトラックのルーティングを停止させるには、ヘルスチェックを反転させます。

> **Note**
>
> ヘルスチェックを無効にしても、ヘルスチェックの料金は適用されます。

高度な設定 (「エンドポイントを監視」する場合のみ)

> **Note**
>
> Route 53 はヘルスチェックコンソールを更新しています。旧コンソールは移行期間中も引き続きご使用いただけます。

- 新しいコンソール
- 旧コンソール

New console

- リクエストの間隔
- 失敗しきい値
- 文字列の一致
- 検索文字列
- レイテンシーグラフ
- SNI の有効化
- ホスト名

リクエストの間隔

各 Route 53 ヘルスチェッカーがエンドポイントから応答を受け取ってから、次のヘルスチェックリクエストを送信するまでの秒数。30 秒の間隔を選択した場合、世界各地のデータセンターにあるそれぞれの Route 53 ヘルスチェッカーは、30 秒あたりに 1 つのヘルスチェックリクエストをエンドポイントに送信します。平均して、エンドポイントは約 2 秒ごとにヘルスチェックリクエストを受け取ることになります。10 秒の間隔を選択した場合、エンドポイントは 1 秒にあたりに複数のヘルスチェックリクエストを受け取ることになります。

異なるデータセンターの Route 53 ヘルスチェッカーは互いに調整しないため、選択した間隔に関係なく、1 秒あたり複数のリクエストを受け取った後、数秒間はヘルスチェックを受け取らないということが生じる場合があります。

ヘルスチェックの作成後は、[リクエストの間隔] の値を変更できません。

> **Note**
>
> リクエストの間隔の値で [高速 (10 秒)] を選択すると、追加料金が適用されます。詳細については、「Route 53 料金表」を参照してください。

失敗しきい値

Route 53 がエンドポイントの最新ステータスを異常から正常または正常から異常に変更するまでに必要な、エンドポイントが連続してヘルスチェックに合格または不合格になる回数。詳細については、「Amazon Route 53 でヘルスチェックの正常性を判断する方法」を参照してください。

文字列マッチング (HTTP または HTTPS の場合のみ)

Route 53 で、HTTP または HTTPS リクエストをエンドポイントに送信、または指定文字列でレスポンス本文を検索することにより、エンドポイントの状態を判断するかどうか。[文字列の検索] で指定した値がレスポンス本文に含まれる場合、Route 53 は、そのエンドポイントが正常であると見なします。レスポンス本文に含まれない場合、またはエンドポイントが応答しない場合、Route 53 は、そのエンドポイントを異常と見なします。検索文字列全体が、レスポンス本文の最初の 5,120 バイト内に出現している必要があります。

ヘルスチェックの作成後は、[String Matching] の値を変更できません。

> **Note**
>
> [文字列マッチング] の値で [はい] を選択すると、追加料金が適用されます。詳細については、「Route 53 料金表」を参照してください。

ヘルスチェッカーが圧縮されたレスポンスを処理する方法

エンドポイントが圧縮されたレスポンスを返す Web サーバーである場合、Route 53 ヘルスチェッカーは、ヘルスチェッカーがサポートする圧縮アルゴリズムを使用して Web サーバーがレスポンスを圧縮した場合にのみ、指定された検索文字列をチェックする前に、レスポンスを解凍します。Health チェッカーは、次の圧縮アルゴリズムをサポートしています。

- Gzip
- Deflate

別のアルゴリズムを使用してレスポンスが圧縮されている場合、ヘルスチェッカーは文字列を検索する前にレスポンスを解凍できません。この場合、検索はたいていいつも失敗し、Route 53 はエンドポイントを異常と見なします。

文字列の検索 ([文字列マッチング] が有効の場合のみ)

エンドポイントからのレスポンス本文内で Route 53 が検索する文字列 。最大長は 255 文字です。

Route 53 は、[文字列の検索] でレスポンス本文内を検索する場合、大文字小文字を識別します。

レイテンシーグラフ

Route 53 で複数の AWS リージョンのヘルスチェッカーとエンドポイント間のレイテンシーを測定するかどうかを選択します。このオプションを選択した場合、CloudWatch のレイテンシーのグラフは、Route 53 コンソールの [ヘルスチェック] ページの [レイテンシー] タブに表示されます。Route 53 ヘルスチェッカーがエンドポイントに接続できない場合、Route 53 はそのエンドポイントのレイテンシーグラフを表示できません。

ヘルスチェックの作成後は、[Latency Measurements] の値を変更できません。

> **Note**
>
> ヘルスチェッカーとエンドポイント間のレイテンシーを計測するように Route 53 を設定する場合、追加料金が適用されます。詳細については、「Route 53 料金表」を参照してください。

SNI の有効化 (HTTPS のみ)

TLS ネゴシエーション中に、Route 53 が `client_hello` メッセージでエンドポイントにホスト名を送信するかどうかを指定します。これにより、エンドポイントは該当する SSL/TLS 証明書で HTTPS リクエストに応答することができます。

一部のエンドポイントでは、HTTPS リクエストで client_hello メッセージにホスト名を含める必要があります。SNI を有効にしない場合、ヘルスチェックのステータスに失敗が表示される場合があります。エラーメッセージは、SNI 情報を含まないリクエストに応答するようにサーバーがどう設定されているかによって異なります。ヘルスチェックは、他の理由でも失敗のステータスになる場合があります。SNI が有効であるのにこのエラーが表示される場合は、エンドポイントの SSL/TLS 設定を調べて証明書が有効であることを確認します。

次の要件に注意してください。

- エンドポイントは SNI をサポートする必要があります。
- エンドポイントの SSL/TLS 証明書には、`Common Name` フィールドにドメイン名が 1 つ含まれており、`Subject Alternative Names` フィールドにいくつか含まれている場合もあります。証明書内のドメイン名のいずれかが [ホスト名] で指定している値と一致する必要があります。

ヘルスチェックリージョン

Route 53 でエンドポイントの正常性をチェックする場合には、推奨リージョンでヘルスチェッカーを使用するか、お客様が指定したリージョンでヘルスチェッカーを使用するかを指定してください。

ヘルスチェックを更新してヘルスチェックを実行しているリージョンを削除すると、Route 53 はそのリージョンから最大 1 時間チェックを引き続き実行します。これにより、一部のヘルスチェッカーが常にエンドポイントをチェックしていることが保証されます (たとえば、3 つのリージョンを 4 つの異なるリージョンに置き換えた場合) 。

カスタマイズ を選択した場合は、削除するリージョンの x を選択します。リストの下部にあるスペースを選択して、リージョンをリストに戻します。少なくとも 3 つのリージョンを指定する必要があります。

ホスト名 ([IP アドレスでエンドポイントを指定する] を選択した場合で、HTTP および HTTPS の場合のみ)

HTTP/HTTPS ヘルスチェックで Route 53 から `Host` ヘッダーに渡す値。通常は、Route 53 でヘルスチェックを実行するウェブサイトの完全修飾 DNS 名を指定します。Route 53 がエンドポイントの正常性をチェックするときに、`Host` ヘッダーがどのように構築されるかを以下に示します。

- [Protocol] の [Port] と [HTTP] に **`80`** の値を指定すると、Route 53 は ホスト名の値を含んだ `Host` ヘッダーをエンドポイントに渡します。
- [プロトコル] の [ポート] と [HTTPS] に **`443`** の値を指定すると、Route 53 は [ホスト名] の値を含んだ `Host` ヘッダーをエンドポイントに渡します。
- [Protocol] の [Port] と [HTTP] または [HTTPS] に別の値を指定すると、Route 53 は *`###`*`#:`*`Port`* の値を含んだ `Host` ヘッダーをエンドポイントに渡します。

エンドポイントを IP アドレスで指定することを選択し、ホスト名に値を指定しない場合、Route 53 は `Host` ヘッダーの IP アドレスの値を、以前の値に置き換えます。

Old console

エンドポイントを監視するオプションを選択した場合、以下の設定も指定できます。

- リクエストの間隔
- 失敗しきい値
- 文字列の一致
- 検索文字列
- レイテンシーグラフ
- SNI の有効化
- ヘルスチェックリージョン
- ヘルスチェックのステータスを反転させる
- Disabled

リクエストの間隔

各 Route 53 ヘルスチェッカーがエンドポイントから応答を受け取ってから、次のヘルスチェックリクエストを送信するまでの秒数。30 秒の間隔を選択した場合、世界各地のデータセンターにあるそれぞれの Route 53 ヘルスチェッカーは、30 秒あたりに 1 つのヘルスチェックリクエストをエンドポイントに送信します。平均して、エンドポイントは約 2 秒ごとにヘルスチェックリクエストを受け取ることになります。10 秒の間隔を選択した場合、エンドポイントは 1 秒にあたりに複数のヘルスチェックリクエストを受け取ることになります。

異なるデータセンターの Route 53 ヘルスチェッカーは互いに調整しないため、選択した間隔に関係なく、1 秒あたり複数のリクエストを受け取った後、数秒間はヘルスチェックを受け取らないということが生じる場合があります。

ヘルスチェックの作成後は、[リクエストの間隔] の値を変更できません。

> **Note**
>
> リクエストの間隔の値で [高速 (10 秒)] を選択すると、追加料金が適用されます。詳細については、「Route 53 料金表」を参照してください。

失敗しきい値

Route 53 がエンドポイントの最新ステータスを異常から正常または正常から異常に変更するまでに必要な、エンドポイントが連続してヘルスチェックに合格または不合格になる回数。詳細については、「Amazon Route 53 でヘルスチェックの正常性を判断する方法」を参照してください。

文字列マッチング (HTTP または HTTPS の場合のみ)

Route 53 で、HTTP または HTTPS リクエストをエンドポイントに送信、または指定文字列でレスポンス本文を検索することにより、エンドポイントの状態を判断するかどうか。[文字列の検索] で指定した値がレスポンス本文に含まれる場合、Route 53 は、そのエンドポイントが正常であると見なします。レスポンス本文に含まれない場合、またはエンドポイントが応答しない場合、Route 53 は、そのエンドポイントを異常と見なします。検索文字列全体が、レスポンス本文の最初の 5,120 バイト内に出現している必要があります。

ヘルスチェックの作成後は、[String Matching] の値を変更できません。

> **Note**
>
> [文字列マッチング] の値で [はい] を選択すると、追加料金が適用されます。詳細については、「Route 53 料金表」を参照してください。

ヘルスチェッカーが圧縮されたレスポンスを処理する方法

エンドポイントが圧縮されたレスポンスを返す Web サーバーである場合、Route 53 ヘルスチェッカーは、ヘルスチェッカーがサポートする圧縮アルゴリズムを使用して Web サーバーがレスポンスを圧縮した場合にのみ、指定された検索文字列をチェックする前に、レスポンスを解凍します。Health チェッカーは、次の圧縮アルゴリズムをサポートしています。

- Gzip
- Deflate

別のアルゴリズムを使用してレスポンスが圧縮されている場合、ヘルスチェッカーは文字列を検索する前にレスポンスを解凍できません。この場合、検索はたいていいつも失敗し、Route 53 はエンドポイントを異常と見なします。

文字列の検索 ([文字列マッチング] が有効の場合のみ)

エンドポイントからのレスポンス本文内で Route 53 が検索する文字列 。最大長は 255 文字です。

Route 53 は、[文字列の検索] でレスポンス本文内を検索する場合、大文字小文字を識別します。

レイテンシーグラフ

Route 53 で複数の AWS リージョンのヘルスチェッカーとエンドポイント間のレイテンシーを測定するかどうかを選択します。このオプションを選択した場合、CloudWatch のレイテンシーのグラフは、Route 53 コンソールの [ヘルスチェック] ページの [レイテンシー] タブに表示されます。Route 53 ヘルスチェッカーがエンドポイントに接続できない場合、Route 53 はそのエンドポイントのレイテンシーグラフを表示できません。

ヘルスチェックの作成後は、[Latency Measurements] の値を変更できません。

> **Note**
>
> ヘルスチェッカーとエンドポイント間のレイテンシーを計測するように Route 53 を設定する場合、追加料金が適用されます。詳細については、「Route 53 料金表」を参照してください。

SNI の有効化 (HTTPS のみ)

TLS ネゴシエーション中に、Route 53 が `client_hello` メッセージでエンドポイントにホスト名を送信するかどうかを指定します。これにより、エンドポイントは該当する SSL/TLS 証明書で HTTPS リクエストに応答することができます。

一部のエンドポイントでは、HTTPS リクエストで `client_hello` メッセージにホスト名を含める必要があります。SNI を有効にしない場合、ヘルスチェックのステータスに失敗が表示される場合があります。エラーメッセージは、SNI 情報を含まないリクエストに応答するようにサーバーがどう設定されているかによって異なります。ヘルスチェックは、他の理由でも失敗のステータスになる場合があります。SNI が有効であるのにこのエラーが表示される場合は、エンドポイントの SSL/TLS 設定を調べて証明書が有効であることを確認します。

次の要件に注意してください。

- エンドポイントは SNI をサポートする必要があります。
- エンドポイントの SSL/TLS 証明書には、`Common Name` フィールドにドメイン名が 1 つ含まれており、`Subject Alternative Names` フィールドにいくつか含まれている場合もあります。証明書内のドメイン名のいずれかが [ホスト名] で指定している値と一致する必要があります。

ヘルスチェックリージョン

Route 53 でエンドポイントの正常性をチェックする場合には、推奨リージョンでヘルスチェッカーを使用するか、お客様が指定したリージョンでヘルスチェッカーを使用するかを指定してください。

ヘルスチェックを更新してヘルスチェックを実行しているリージョンを削除すると、Route 53 はそのリージョンから最大 1 時間チェックを引き続き実行します。これにより、一部のヘルスチェッカーが常にエンドポイントをチェックしていることが保証されます (たとえば、3 つのリージョンを 4 つの異なるリージョンに置き換えた場合) 。

カスタマイズ を選択した場合は、削除するリージョンの x を選択します。リストの下部にあるスペースを選択して、リージョンをリストに戻します。少なくとも 3 つのリージョンを指定する必要があります。

ヘルスチェックステータスを反転させる (古いコンソールのみ)

新しいコンソールでヘルスチェックを反転させるには、「ヘルスチェックの反転」を参照してください。

Route 53 でヘルスチェックのステータスを反転させるかどうかを選択します。このオプションを選択した場合、Route 53 はステータスが正常であればヘルスチェックに不具合があると見なします。逆も同様です。例えば、文字列マッチングを設定していて、指定した値をエンドポイントが返した場合に、Route 53 がヘルスチェックを [異常] と見なすようにできます。

無効 (古いコンソールのみ)

新しいコンソールでヘルスチェックを無効にするには、「ヘルスチェックの無効化または有効化」を参照してください。

Route 53 によるヘルスチェックの実行を停止させます。ヘルスチェックを無効にすると、Route 53 は、エンドポイントとの TCP 接続確立を中断しようとします。

ヘルスチェックを無効にすると、Route 53 は、そのヘルスチェックのステータスを常に正常とみなすようになります。DNS フェイルオーバーを設定した場合、Route 53 はトラフィックを引き続き該当するリソースにルーティングします。リソースへのトラックのルーティングを停止させるには、ヘルスチェックを反転させます。

> **Note**
>
> ヘルスチェックを無効にしても、ヘルスチェックの料金は適用されます。

ヘルスチェックが失敗した場合の通知を取得する

ヘルスチェックが不合格の場合、次のオプションを使用してメールでの通知を設定します。

- Create alarm
- Send notification to
- Topic name
- Recipient email addresses

アラームの作成 (ヘルスチェックの作成時のみ)

デフォルトの CloudWatch アラームを作成するかどうかを指定します。[はい] を選択すると、このエンドポイントのステータスが異常に変わって、そのエンドポイントの異常状態が 1 分間続いていると Route 53 が判断した場合に、CloudWatch が Amazon SNS 通知を送信します。

> **Note**
>
> ステータスが正常に戻ったときに CloudWatch が別の Amazon SNS 通知を送信するようにするには、ヘルスチェックの作成後にアラームをもう 1 つ作成します。詳細については、Amazon CloudWatch ユーザーガイドの「Amazon CloudWatch アラームの作成 」を参照してください。

既存のヘルスチェックにアラームを作成する場合、または、エンドポイントが 1 分 (デフォルト値) とは異なる時間、Route 53 に異常な状態とみなされると通知を受け取る場合は、[いいえ] を選択し、ヘルスチェックの作成後にアラームを追加します。詳細については、「CloudWatch を使用したヘルスチェックのモニタリング」を参照してください。

通知の送信先 (アラームの作成時のみ)

CloudWatch が既存または新規の Amazon SNS トピックに通知を送信するかどうかを指定します。

- [既存の SNS トピック]- リストからトピック名を選択します。トピックは、米国東部 (バージニア北部) リージョンにある必要があります。
- 新規 SNS トピック - [Topic Name (トピック名)] にトピック名を入力し、[受信者] に通知を送信したい [E メールアドレス] を入力します。複数のアドレスがある場合は、カンマ (,)、セミコロン (;)、または空白で区切ります。

Route 53 は、米国東部 (バージニア北部) リージョンにトピックを作成します。

Topic Name (新しい SNS トピックの作成時のみ)

[New SNS Topic] を指定した場合、新しいトピック名を入力します。

Recipient email addresses (新しい SNS トピックを作成する場合のみ)

[New SNS Topic] を指定した場合、通知の送信先となるメールアドレスを入力します。複数ある場合は、カンマ (,)、セミコロン (;)、または空白で区切ります。

ヘルスチェックを作成すると Amazon Route 53 が表示する値

[Create Health Check (ヘルスチェックの作成)] ページには、入力した値に応じて以下の値が表示されます。

URL

ヘルスチェックを実行する際に Route 53 がリクエストを送信する完全な URL (HTTP/HTTPS ヘルスチェックの場合) または IP アドレスとポート (TCP ヘルスチェックの場合)。

ヘルスチェックタイプ

[Basic] または [Basic + additional options] (このヘルスチェックに対して指定した設定による)。追加オプションの料金については、「Route 53 料金表」を参照してください。

CloudWatch アラーム設定を変更する場合のヘルスチェックの更新 (CloudWatch アラームのみをモニタリングするヘルスチェック)

CloudWatch アラームへのデータストリームをモニタリングする Route 53 ヘルスチェックを作成した後に CloudWatch アラームの設定を更新すると、Route 53 ではヘルスチェックのアラーム設定は自動的に更新されません。新しいアラーム設定を使用してヘルスチェックを開始するためには、ヘルスチェックを更新する必要があります。

> **Note**
>
> ヘルスチェックの更新をプログラムするには、`UpdateHealthCheck` API を使用できます。`AlarmIdentifier` と `Region` の現在の値を指定するだけで、Route 53 が CloudWatch

から最新の設定を取得します。詳細については、Amazon Route 53 API リファレンスの「UpdateHealthCheck」を参照してください。

> **Note**
>
> Route 53 はヘルスチェックコンソールを更新しています。旧コンソールは移行期間中も引き続きご使用いただけます。

お使いのコンソールのタブを選択します。

- 新しいコンソール
- 旧コンソール

New console

新しい CloudWatch アラーム設定があるヘルスチェックを更新するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [ヘルスチェック] を選択します。
3. 更新するヘルスチェックのリンクされた ID を選択します。
4. [編集] を選択します。

   ヘルスチェックの CloudWatch アラームが変更されたことのお知らせが表示されます。[Details] フィールドには、新しいアラーム設定が表示されます。
5. [保存] を選択します。

Old console

新しい CloudWatch アラーム設定があるヘルスチェックを更新するには (コンソール)

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [Health Checks (ヘルスチェック)] を選択します。

3. 更新するヘルスチェックのチェックボックスを選択します。
4. [Edit health check] を選択します。

   ヘルスチェックの CloudWatch アラームが変更されたことのお知らせが表示されます。[Details] フィールドには、新しいアラーム設定が表示されます。
5. [保存] を選択します。

ヘルスチェックの無効化または有効化

ヘルスチェックを無効にすると、Route 53 がヘルスチェックを実行できなくなります。ヘルスチェックを無効にすると、Route 53 は、参照するヘルスチェックのステータスの集計を停止します。ヘルスチェックを無効にすると、Route 53 は、そのヘルスチェックのステータスを常に正常とみなすようになります。DNS フェイルオーバーを設定した場合、Route 53 はトラフィックを引き続き該当するリソースにルーティングします。リソースへのトラックのルーティングを停止させるには、[Inverted] (転置) の値を変更します。

> **Note**
>
> Route 53 はヘルスチェックコンソールを更新しています。旧コンソールは移行期間中も引き続きご使用いただけます。

ヘルスチェックを作成または編集するときに、古いコンソールでヘルスチェックを無効または有効にすることができます。詳細については、「ヘルスチェックを作成または更新するときに指定する値」を参照してください。

新しいコンソールでヘルスチェックを無効にするには、次の手順を実行します。

ヘルスチェックを無効または有効にするには (新しいコンソールのみ)

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [ヘルスチェック] を選択します。
3. [アクション] 列で 3 つのドットを選択し、[無効化] または [有効化] を選択します。

   または、有効化または無効化するヘルスチェックのリンクされた ID を選択します。
4. [設定] テーブルの [ステータス] フィールドでは、ヘルスチェックが有効か無効かを指定します。

5. ヘルスチェックを有効または無効にするには、[無効化] または [有効化] を選択します。

ヘルスチェックの反転

ヘルスチェックを反転させた場合、Route 53 はステータスが正常であればヘルスチェックに不具合があると見なします。逆も同様です。

> **Note**
>
> Route 53 はヘルスチェックコンソールを更新しています。旧コンソールは移行期間中も引き続きご使用いただけます。

ヘルスチェックを作成または編集するときに、古いコンソールでヘルスチェックを反転させることができます。詳細については、「ヘルスチェックを作成または更新するときに指定する値」を参照してください。

新しいコンソールでヘルスチェックを反転させるには、次の手順を実行します。

ヘルスチェックを反転させるには (新しいコンソールのみ)

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [ヘルスチェック] を選択します。
3. [アクション] 列で 3 つのドットを選択し、[反転] を選択します。

   または、反転させるヘルスチェックのリンクされた ID を選択します。
4. [設定] テーブルの [反転] フィールドは、ヘルスチェックが反転されている ([はい]) または反転されていない ([いいえ]) かどうかを指定します。
5. ヘルスチェックを反転させるには [反転] を選択します。

   反転ステータスを元に戻す場合、[反転] フィールドが [はい] の場合は、もう一度 [反転] を選択します。

ヘルスチェックの削除

ヘルスチェックを無効にするには、次の手順を実行します。

> **Note**
>
> を使用して AWS Cloud Map いて、インスタンスの登録時に Route 53 ヘルスチェックを作成する AWS Cloud Map ように を設定している場合、Route 53 コンソールを使用してヘルスチェックを削除することはできません。インスタンスの登録を解除すると、ヘルスチェックが自動的に削除されます。ヘルスチェックが Route 53 コンソールに表示されなくなるまでに数時間かかる場合があります。

> **Note**
>
> Route 53 はヘルスチェックコンソールを更新しています。旧コンソールは移行期間中も引き続きご使用いただけます。

お使いのコンソールのタブを選択します。

- 新しいコンソール
- 旧コンソール

New console

ヘルスチェックを削除するには

1. レコードに関連付けられているヘルスチェックを削除する場合は、「DNS フェイルオーバーが設定されている場合のヘルスチェックの更新または削除」で推奨されているタスクを実行します。
2. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
3. ナビゲーションペインで [ヘルスチェック] を選択します。
4. 削除するヘルスチェックのリンクされた ID を選択します。
5. [削除] を選択します。
6. テキストボックスに **`confirm`** を入力し、[削除] を選択します。

Old console

ヘルスチェックを削除するには (コンソール)

1. レコードに関連付けられているヘルスチェックを削除する場合は、「DNS フェイルオーバーが設定されている場合のヘルスチェックの更新または削除」で推奨されているタスクを実行します。
2. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
3. ナビゲーションペインで [Health Checks (ヘルスチェック)] を選択します。
4. 右側のペインで、削除するヘルスチェックを選択します。
5. [Delete Health Check] を選択します。
6. [Yes, Delete] を選択して確定します。

DNS フェイルオーバーが設定されている場合のヘルスチェックの更新または削除

レコードに関連付けられているヘルスチェックを更新または削除するとき、あるいは、ヘルスチェックが関連付けられているレコードに変更を加えるときは、そうした変更が DNS クエリのルーティングや DNS フェイルオーバーの構成に及ぼす影響を考慮する必要があります。

> **Important**
>
> Route 53 に、ヘルスチェックの削除を防止する機構はありません。ヘルスチェックがレコードに関連付けられていたとしても同様です。ヘルスチェックを削除したにもかかわらず、そこに関連付けられていたレコードを更新しなかった場合、以後そのヘルスチェックのステータスが予測不能となり、ステータスが変化する可能性もあります。この場合、DNS フェイルオーバー設定の DNS クエリのルーティングが影響を受けます。

既にレコードに関連付けられているヘルスチェックを更新または削除するには、次のタスクを実行するようお勧めします。

1. ヘルスチェックに関連付けられているレコードを特定します。ヘルスチェックに関連付けられているレコードを特定するには、次のいずれかを実行する必要があります。

- Route 53 コンソールを使用して各ホストゾーンのレコードを確認します。詳細については、「レコードの一覧表示」を参照してください。
- 各ホストゾーンで ListResourceRecordSets API アクションを実行し、そのレスポンスを確認します。詳細については、Amazon Route 53 API リファレンスの「ListResourceRecordSets」を参照してください。

2. ヘルスチェックの更新や削除、レコードの更新によって生じる動作の変化を推定します。この評価に基づいて、実際に行う変更を決めます。

   詳細については、「ヘルスチェックを省略するとどうなるか」を参照してください。

3. ヘルスチェックおよびレコードに適宜変更を加えます。詳細については、以下のトピックを参照してください。

   - ヘルスチェックの作成と更新
   - レコードの編集

4. 今後使用しないヘルスチェックがあれば削除します。詳細については、「ヘルスチェックの削除」を参照してください。

Amazon Route 53 のヘルスチェックができるようにルーターとファイアウォールのルールを設定する

Route 53 は、エンドポイントの正常性をチェックする際、ヘルスチェックの作成時に指定された IP アドレスおよびポートに対し、HTTP、HTTPS、TCP のいずれかのリクエストを送信します。ヘルスチェックが成功するためには、Route 53 ヘルスチェッカーが使用する IP アドレスからのインバウンドトラフィックを、ルーターとファイアウォールのルールで許可する必要があります。

Route 53 ヘルスチェッカー、Route 53 ネームサーバー、およびその他の AWS サービスの IP アドレスの現在のリストについては、「」を参照してくださいAmazon Route 53 サーバーの IP アドレス範囲。

Amazon EC2 では、セキュリティグループがファイアウォールとして機能します。詳細については、Amazon EC2 ユーザーガイド」の「Amazon EC2 セキュリティグループ」を参照してください。Route 53 ヘルスチェックを許可するようにセキュリティグループを設定するには、各 IP アドレス範囲からのインバウンドトラフィックを許可するか、 AWSマネージドプレフィックスリストを使用できます。 Amazon EC2

AWSマネージドプレフィックスリストを使用するには、セキュリティグループを変更して からのインバウンドトラフィックを許可します。ここでcom.amazonaws.<region>.route53-healthchecks、 <region> は Amazon EC2 インスタンスまたはリソース AWS リージョン の です。Route 53 ヘルスチェックを使用して IPv6 エンドポイントをチェックしている場合は、com.amazonaws.<region>.ipv6.route53-healthchecks からのインバウンドトラフィックも許可する必要があります。

AWSマネージドプレフィックスリストの詳細については、「Amazon VPC ユーザーガイド AWS」の「マネージドプレフィックスリストの使用」を参照してください。

> **Important**
>
> 許可された IP アドレスのリストに IP アドレスを追加するときは、ヘルスチェックの作成時に指定した各 AWS リージョンの CIDR 範囲内のすべての IP アドレスとグローバル CIDR 範囲を追加します。リージョン内の 1 つの IP アドレスから送信されたヘルスチェックリクエストが表示される場合があります。ただし、この IP アドレスを、そのリージョンの別の IP アドレスにいつでも変更することができます。
>
> 現在のヘルスチェッカー IP アドレスと、古いヘルスチェッカー IP アドレスの両方が含まれていることを確認する場合は、/26 および /18 の IP アドレス範囲を、すべて許可リストに追加します。完全なリストについては、「AWS 全般のリファレンス」の「AWS IP アドレス範囲」を参照してください。
>
> AWSマネージドプレフィックスリストをインバウンドセキュリティグループに追加すると、必要な範囲がすべて自動的に追加されます。

DNS フェイルオーバーの設定

複数の HTTP サーバー、あるいは複数のメールサーバーなど、同じ機能を実行するリソースが重複して存在する場合、それらのリソースの正常性をチェックし正常なリソースのみを使用して DNS クエリに応答するように、Amazon Route 53 を設定することができます。例えば、ウェブサイト (example.com) が、世界各地の 3 拠点のデータセンターにそれぞれ 2 台ずつ、合計 6 台のサーバーでホストされているとします。それらのサーバーの正常性をチェックし、その時点で正常なサーバーのみを使用して example.com の DNS クエリに応答するように Route 53 を設定することができます。

Route 53 では、構成が単純な場合と複雑な場合の両方で、リソースの正常性をチェックすることができます。

- シンプルな構成では、example.com のタイプ A の加重レコードのグループなど、すべてが同じ名前とタイプのレコードグループを作成します。その上で、対応するリソースの正常性をチェックするように Route 53 を設定します。Route 53 は、リソースの正常性に基づいて DNS クエリへの応答を実行します。詳細については、「Amazon Route 53 のシンプルな構成でのヘルスチェックの動作」を参照してください
- より複雑な構成では、複数の基準に基づいてトラフィックをルーティングするレコードのツリーを作成します。例えば、ユーザーのレイテンシーが最も重要な基準である場合、レイテンシーエイリアスレコードを使用して、レイテンシーが最も高いリージョンにトラフィックをルーティングできます。レイテンシーエイリアスレコードには、エイリアスターゲットとして各リージョンに加重レコードがある場合があります。加重レコードは、インスタンスタイプに基づいてトラフィックを EC2 インスタンスにルーティングします。シンプルな構成の場合と同様に、Route 53 は、リソースの正常性に基づいてトラフィックをルーティングするように設定することができます。詳細については、「Amazon Route 53 の複雑な構成でのヘルスチェックの動作」を参照してください

トピック

- DNS フェイルオーバーを設定するためのタスクリスト
- Amazon Route 53 のシンプルな構成でのヘルスチェックの動作
- Amazon Route 53 の複雑な構成でのヘルスチェックの動作
- ヘルスチェックが設定されている場合に Amazon Route 53 がレコードを選択する方法
- フェイルオーバー (アクティブ/アクティブとアクティブ/パッシブ) の設定
- プライベートホストゾーンのフェイルオーバーの設定
- Amazon Route 53 でフェイルオーバーの問題を回避する方法

DNS フェイルオーバーを設定するためのタスクリスト

Route 53 を使用して DNS のフェイルオーバーを設定するには、以下のタスクを実行します。

1. 全体的な設定の概略図を作成し、作成するレコードのタイプ (加重エイリアス、フェイルオーバー、レイテンシーなど) をノードごとに指定します。ツリーの上部には、ユーザーがウェブサイトやウェブアプリケーションにアクセスするために使用する example.com などのドメイン名のレコードを入れます。

   概略図に表示されるレコードの種類は、設定の複雑さによって異なります。

- シンプルな構成では、概略図にエイリアスレコードは含まれません。エイリアスレコードは、別の Route 53 レコードではなく、ELB ロードバランサーなどのリソースにトラフィックを直接ルーティングします。詳細については、「Amazon Route 53 のシンプルな構成でのヘルスチェックの動作」を参照してください
- 複雑な構成の場合は、エイリアスレコード (加重エイリアスやフェイルオーバーエイリアスなど) と非エイリアスレコードを複数レベルのツリーで組み合わせます (「Amazon Route 53 の複雑な構成でのヘルスチェックの動作」トピックの例を参照)。

> **Note**
>
> 複雑なルーティング設定のレコードをすばやく簡単に作成して、レコードをヘルスチェックに関連付けるには、トラフィックフロービジュアルエディターを使用して、設定をトラフィックポリシーとして保存することができます。その後、トラフィックポリシーを、同じホストゾーンまたは複数のホストゾーンで 1 つ以上のドメイン名 (example.com など) またはサブドメイン名 (www.example.com など) に関連付けることができます。さらに、新しい設定が期待どおりに機能していない場合は、更新を元に戻すことができます。詳細については、「DNS トラフィックのルーティングにトラフィックフローを使用する」を参照してください

詳細については、次のドキュメントを参照してください。

- ルーティングポリシーの選択
- エイリアスレコードと非エイリアスレコードの選択

2. データセンターで実行されている Amazon EC2 サーバーや E メールサーバーなど、エイリアスレコードを作成できないリソースのヘルスチェックを作成します。これらのヘルスチェックは、非エイリアスレコードに関連付けます。

   詳細については、「ヘルスチェックの作成、更新、削除」を参照してください
3. 必要に応じて、ヘルスチェックで指定したエンドポイントに対し、 Route 53 が定期的なリクエストを送信できるように、ルーターとファイアウォールのルールを設定します。詳細については、「Amazon Route 53 のヘルスチェックができるようにルーターとファイアウォールのルールを設定する」を参照してください
4. 概略図の中の非エイリアスレコードをすべて作成し、ステップ 2 で作成したヘルスチェックを該当するレコードに関連付けます。

エイリアスレコードを含まない設定で DNS フェイルオーバーを設定する場合、以降の作業は不要です。

5. ELB ロードバランサーや CloudFront ディストリビューションなどの AWS リソースにトラフィックをルーティングするエイリアスレコードを作成します。リソースが異常な場合に、Route 53 がツリーの別のブランチを試すようにするには、各エイリアスレコードの [ターゲットの正常性の評価] の値を [Yes (あり)] に設定してください。(ターゲットヘルスの評価は一部の AWS リソースではサポートされていません)。
6. ステップ 1 で作成した概略図の一番下から、ステップ 4 と 5 で作成したレコードにトラフィックをルーティングするエイリアスレコードを作成します。ツリーの 1 つのブランチの中で、非エイリアスレコードがすべて異常なときに別のブランチを試すように Route 53 を設定する場合は、各エイリアスレコードの [ターゲットの正常性の評価] の値を [Yes (あり)] に設定します。

   別のレコードを作成するまで、トラフィックを別のレコードにルーティングするエイリアスレコードを作成することはできません。

Amazon Route 53 のシンプルな構成でのヘルスチェックの動作

example.com を対象とした 2 つ以上のウェブサーバーなど、同じ機能を実行する 2 つ以上のリソースがある場合、次のヘルスチェック機能を使用して、正常なリソースにのみトラフィックをルーティングできます。

EC2 インスタンスおよびその他のリソース (非エイリアスレコード) の正常性をチェックする

エイリアスレコードを作成できないリソース (EC2 インスタンスなど) にトラフィックをルーティングする場合は、各リソースのレコードとヘルスチェックを作成します。次に、各ヘルスチェックを該当するレコードに関連付けます。ヘルスチェックは、対応するリソースの正常性を定期的にチェックし、Route 53 は、ヘルスチェックが正常とレポートするリソースにのみトラフィックをルーティングします。

AWS リソース (エイリアスレコード) の状態を評価する

エイリアスレコードを使用して ELB ロードバランサーなどの選択した AWS リソースにトラフィックをルーティングする場合は、リソースの正常性を評価し、正常なリソースにのみトラフィックをルーティングするように Route 53 を設定できます。エイリアスレコードを設定してリソースの正常性を評価する場合、リソースのヘルスチェックを作成する必要はありません。

シンプルな構成でリソースの正常性をチェックするように、Route 53 を設定する方法の概要を以下に示します。

1. どのリソースの正常性を Route 53 で監視するかを明確にします。例えば、example.com のリクエストに応答するすべての HTTP サーバーを監視対象にするとします。
2. データセンターで実行されている EC2 インスタンスやサーバーなど、エイリアスレコードを作成できないリソースのヘルスチェックを作成します。リソースにヘルスチェックリクエストを送信する方法を指定します。具体的には、使用するプロトコル (HTTP、HTTPS、TCP)、使用する IP アドレスとポート、さらに、HTTP/HTTPS ヘルスチェックの場合はドメインの名前とパスが伝えられます。

   > **Note**
   >
   > ELB ロードバランサーなどのエイリアスレコードを作成できるリソースを使用している場合は、それらのリソースのヘルスチェックを作成しないでください。

   リソースごとにヘルスチェックを 1 つ作成し、ヘルスチェックのエンドポイントには、リソースと同じ IP アドレスを使用するのが一般的な構成です。ヘルスチェックは、指定された IP アドレスに要求を送信します。

   > **Note**
   >
   > Route 53 では、リソースの IP アドレスがローカル、プライベート、ルーティング範囲外、またはマルチキャストのいずれかに該当する場合、正常性をチェックすることはできません。ヘルスチェックを作成できない IP アドレスの詳細については、「RFC 5735, Special Use IPv4 Addresses」と「RFC 6598, IANA-Reserved IPv4 Prefix for Shared Address Space」を参照してください。

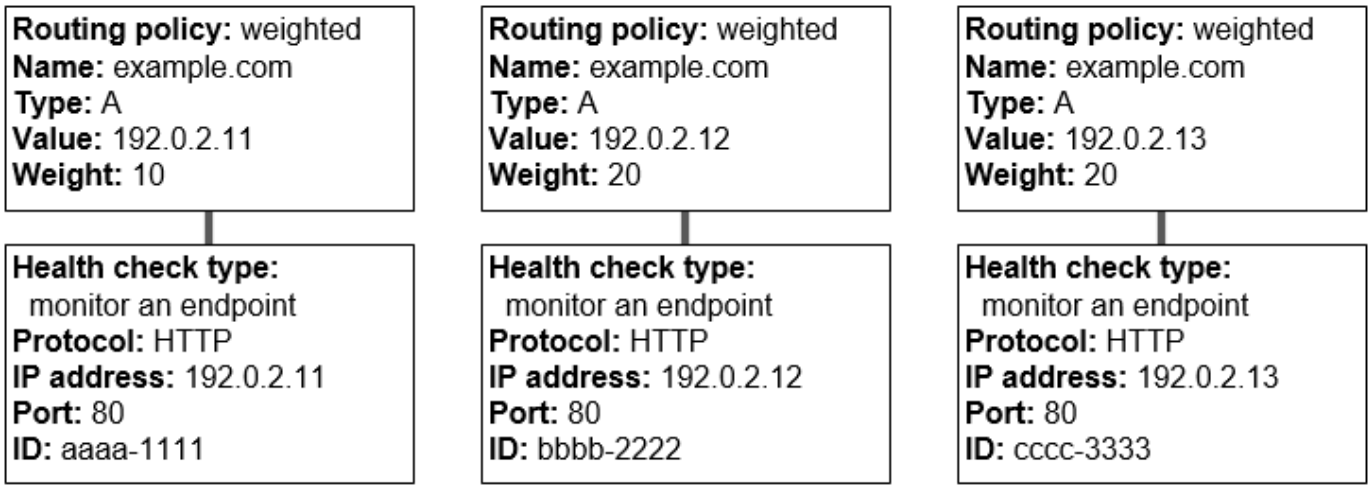
   ヘルスチェック作成の詳細については、「ヘルスチェックの作成、更新、削除」を参照してください。
3. ヘルスチェックで指定したエンドポイントに対し、Route 53 が定期的なリクエストを送信できるように、ルーターとファイアウォールのルールを設定する必要があります。詳細については、「Amazon Route 53 のヘルスチェックができるようにルーターとファイアウォールのルールを設定する」を参照してください。

4. 例えば、加重レコードのグループなど、リソースのレコードのグループを作成します。エイリアスと非エイリアスレコードを混在させることができますが、[名前]、[タイプ]、および [ルーティングポリシー] のすべての値が同じである必要があります。

   リソースの正常性をチェックするために Route 53 を設定する方法は、エイリアスレコードを作成するか非エイリアスレコードを作成するかによって異なります。

   - エイリアスレコード – [Evaluate Target Health (ターゲットの正常性の評価)] で [Yes (あり)] を指定します。
   - 非エイリアスレコード– ステップ 2 で作成したヘルスチェックを、対応するレコードと関連付けます。

   設定が完了したら、次の図のような設定になります。この図には、非エイリアスレコードのみが含まれています。



   Route 53 コンソールを使用したレコード作成の詳細については、「Amazon Route 53 コンソールを使用したレコードの作成」を参照してください。

5. ヘルスチェックを作成した場合、Route 53 はヘルスチェックごとに定期的にエンドポイントにリクエストを送信します。つまり、DNS クエリを受信したときにヘルスチェックが実行されるわけではありません。Route 53 は、その応答に応じてエンドポイントが正常であるかどうかを判断し、その情報をもとにクエリへの応答方法を決定します。詳細については、「Amazon Route 53 でヘルスチェックの正常性を判断する方法」を参照してください。

   Route 53 によって正常性がチェックされるのは、レコードで指定されたリソース (example.com の A レコードで指定された IP アドレスなど) ではありません。レコードにヘルスチェックが関連付けられた場合、Route 53 では、ヘルスチェックで指定されたエンドポイントの

正常性のチェックを開始します。また、他のヘルスチェックの正常性をモニタリングしたり、CloudWatch アラームのデータストリームをモニタリングしたりするように Route 53 を設定することもできます。詳細については、「Amazon Route 53 ヘルスチェックの種類」を参照してください。

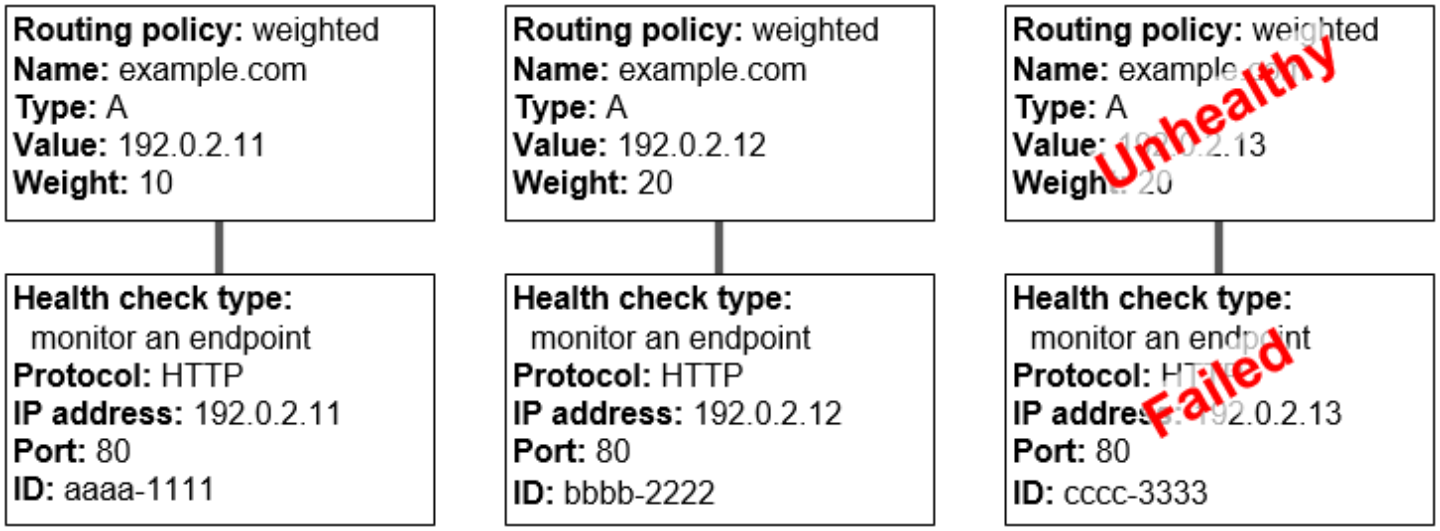
Route 53 が example.com のクエリを受信した場合の動作を以下に示します。

1. Route 53 が、ルーティングポリシーに基づいてレコードを選択します。このケースでは、重みに基づいてレコードが選択されます。
2. そのレコードのヘルスチェックのステータスをチェックして、選択されたレコードの現在の正常性を調べます。
3. 選択したレコードに異常がある場合、Route 53 は別のレコードを選択します。このとき、異常のあるレコードは候補から外されます。

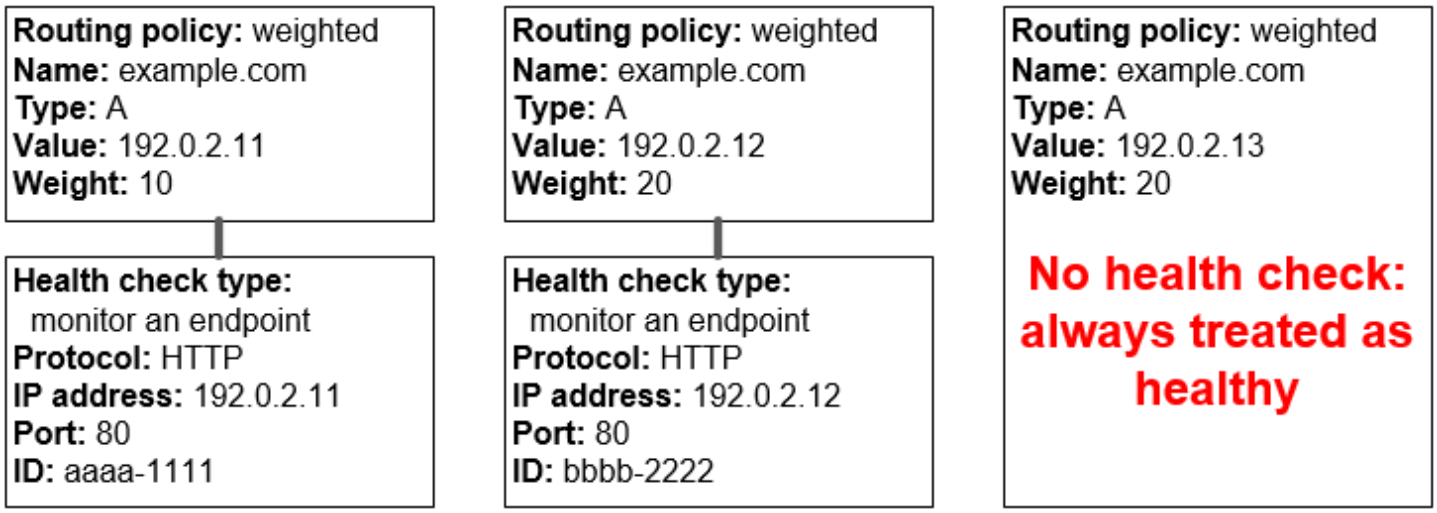
   詳細については、「ヘルスチェックが設定されている場合に Amazon Route 53 がレコードを選択する方法」を参照してください。
4. 正常なレコードを検出した Route 53 は、A レコードの IP アドレスなどの適切な値でクエリに応答します。

次の例は、加重レコードのグループを示しています。3 つ目のレコードに異常がみられます。まず、Route 53 は、3 つすべてのレコードの重みに基づいてレコードを選択します。最初に選択したレコードに異常が見つかると、Route 53 は別のレコードを選択します。このとき、3 つ目のレコードの重みは計算から除外されます。

- 初めに Route 53 が 3 つすべてのレコードからの選択を行った際に、1 つ目のレコードがリクエストへの応答に使用される時間は全体の 20% (= 10/(10 + 20 + 20)) となります。
- Route 53 により、3 つ目のレコードに異常が発見された場合、1 つ目のレコードがリクエストへの応答に使用される時間は、全体の 33% (=10/(10 + 20)) となります。



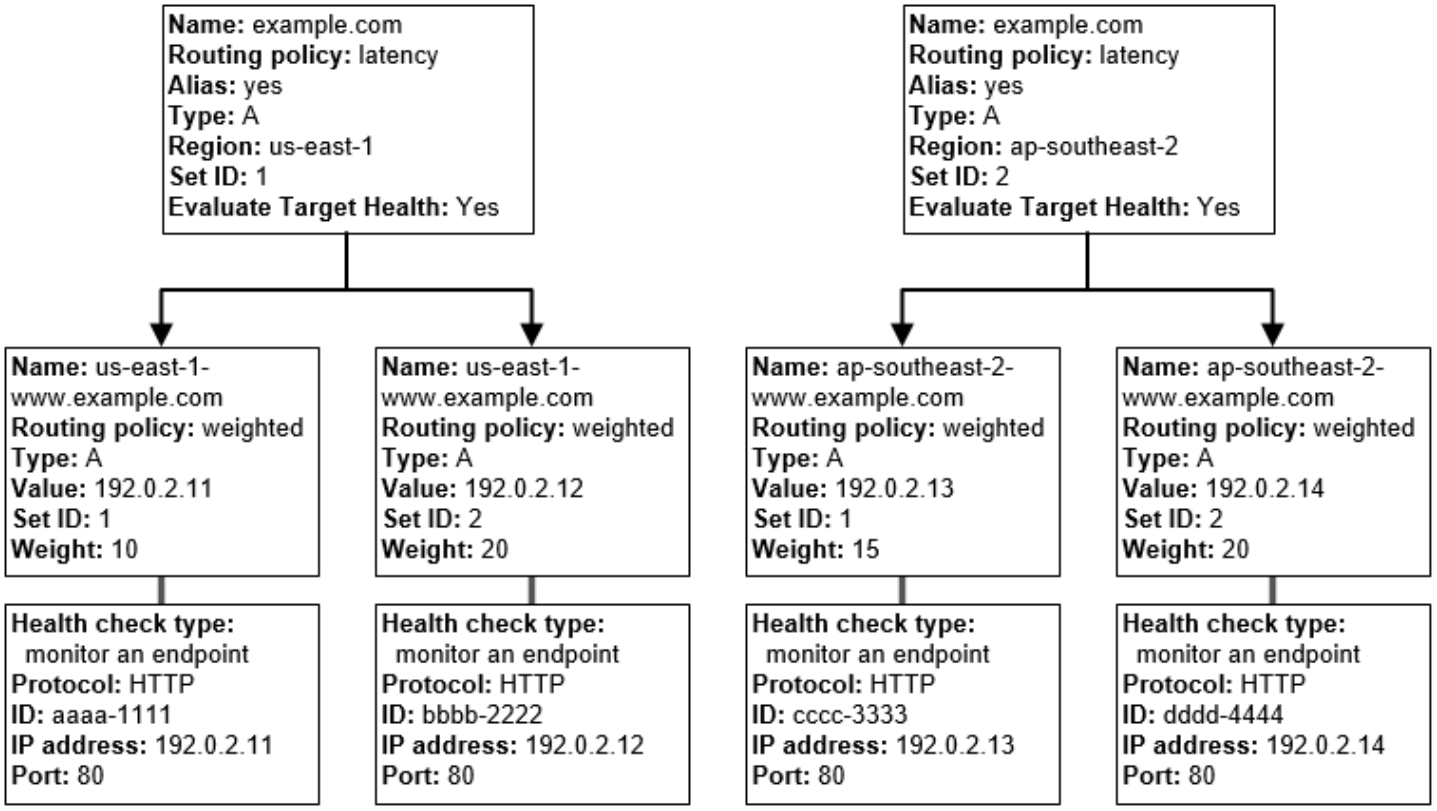
レコードグループ内の 1 つ以上のレコードからヘルスチェックを省略すると、Route 53 には対応するリソースの正常性を判断する方法がなくなります。Route 53 は、それらのレコードを正常と見なします。



Amazon Route 53 の複雑な構成でのヘルスチェックの動作

複雑な構成であっても、リソースの正常性をチェックする方法は同じです。ただし、複雑な構成では、エイリアスレコード (加重エイリアスやフェイルオーバーエイリアスなど) と非エイリアスレコードを組み合わせてデシジョンツリーを構築し、リクエストに対する Route 53 の応答を柔軟に制御することができます。

たとえば、レイテンシーエイリアスレコードを使用してユーザーに近いリージョンを選択し、各リージョン内の 2 つ以上のリソースの加重レコードを使用して、単一のエンドポイントまたはアベイラビリティーゾーンの障害から保護できます。この設定は以下の図のようになります。



Amazon EC2 と Route 53 の設定方法は次のとおりです。ツリーの一番下から始めましょう。これはレコードを作成する順序です。

- us-east-1 と ap-southeast-2 という 2 つのリージョンのそれぞれに、2 つの EC2; インスタンスが存在します。EC2 インスタンスが正常であるかどうかを判断して、Route 53 がトラフィックをルーティングするように、各インスタンスのヘルスチェックを作成します。各ヘルスチェックを設定して、インスタンスの Elastic IP アドレスで対応するインスタンスにヘルスチェックリクエストを送信します。

  Route 53 はグローバルサービスであるため、ヘルスチェックを作成するリージョンを指定しません。

- インスタンスタイプに基づいて各リージョンの 2 つのインスタンスにトラフィックをルーティングするため、各インスタンスの加重レコードを作成し、各レコードに重みを付けます。(後で加重を変更して、より多くのトラフィックを、またはより少ないトラフィックをインスタンスにルーティングできます。) また、該当するヘルスチェックを各インスタンスに関連付けます。

  レコードを作成するとき、us-east-1-www.example.com. や ap-southeast-2-www.example.com. などの名前を使用します。ツリーの一番上に到達するまで待って、ユーザーがウェブサイトやウェ

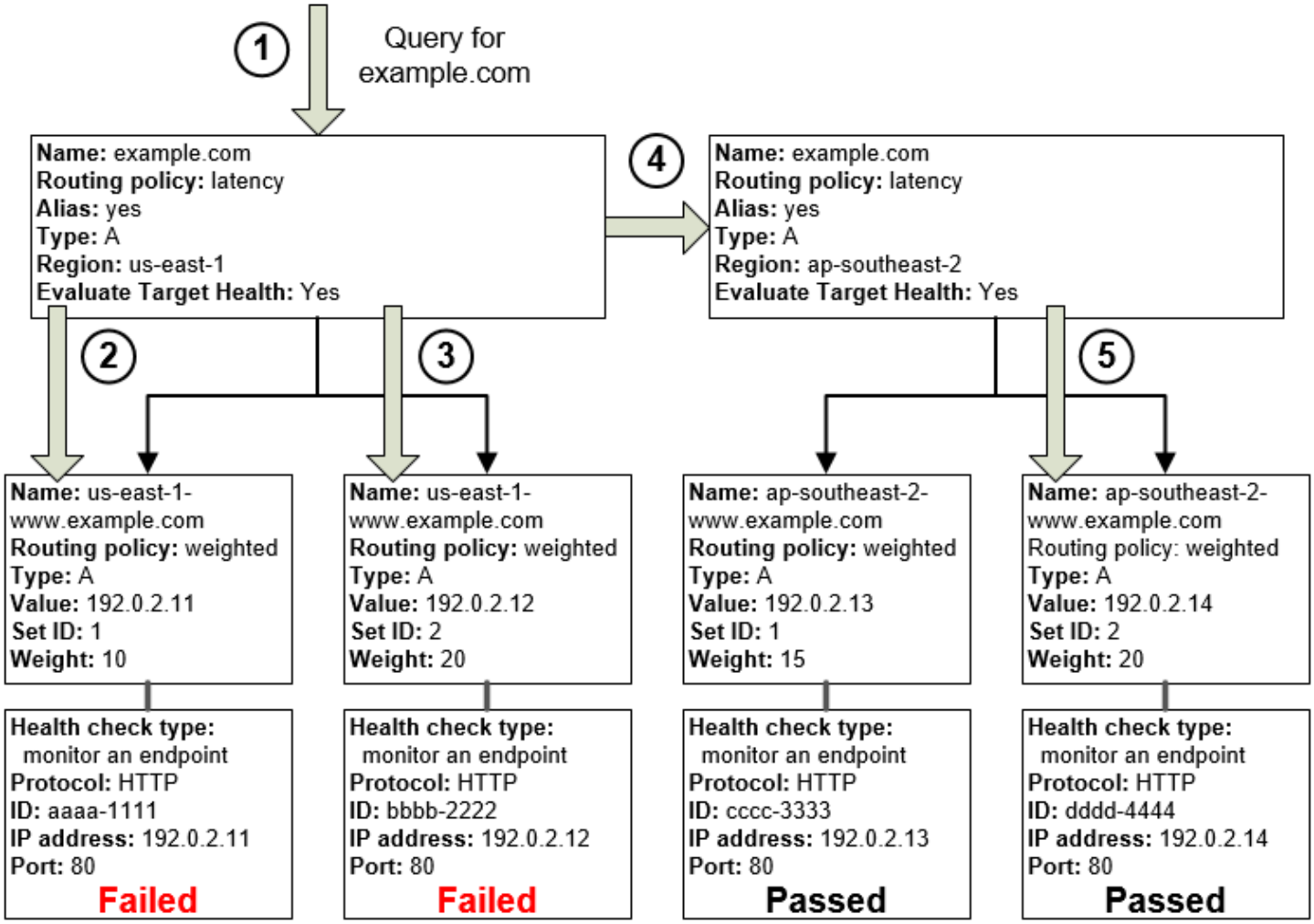
ブアプリケーションにアクセスするために使用する名前 (example.com など) をレコードに渡します。

- ユーザーのレイテンシーが最も低いリージョンにトラフィックをルーティングするため、ツリーの上部にあるレコードのレイテンシー[ルーティングポリシー]を選択します。

  トラフィックを各リージョンのリソースに直接ルーティングするのではなく、各リージョンのレコードにルーティングします (加重レコードは既にルーティングしています) 。その結果、レイテンシーの[エイリアスレコード]を作成することになります。

  エイリアスレコードを作成するときに、ユーザーがウェブサイトやウェブアプリケーションにアクセスするために使用する名前 (example.com など) を指定します。エイリアスレコードは、example.com のトラフィックを us-east-1-www.example.com と ap-southeast-2-www.example.com のレコードにルーティングします。

  レイテンシーエイリアスレコードの [Evaluate Target Health] の値は、どちらも [Yes] に設定します。これにより、Route 53 は、トラフィックをルーティングする前に、リージョンに正常なリソースがあるかどうかを判断します。そうでない場合、Route 53 は他のリージョンの正常なリソースを選択します。



前の図は、以下の一連のイベントを示したものです。

1. Route 53 が example.com のクエリを受信します。要求元のユーザーに対するレイテンシーに基づいて、Route 53 は us-east-1 リージョンのレイテンシーエイリアスレコードを選択します。
2. Route 53 は、重みに基づいて加重レコードを選択します。レイテンシーエイリアスレコードの [Evaluate Target Health (ターゲットの正常性の評価)] が [Yes (あり)] であるため、Route 53 は、選択された加重レコードの正常性をチェックします。
3. ヘルスチェックで不合格と判明した場合、Route 53 は、別の加重レコードを重みに基づいて選択し、その正常性をチェックします。そのレコードも異常であると判明します。
4. Route 53 は、ブランチの出発点に戻り、次善のレイテンシーを持つレイテンシーエイリアスレコードを検索して、ap-southeast-2 のレコードを選択します。
5. Route 53 は再度、重みに基づいてリソースを選択し、その正常性をチェックします。リソースは正常なので、Route 53 はクエリに対応した適切な値を返します。

トピック

- エイリアスレコードにヘルスチェックを関連付けるとどうなるか
- ヘルスチェックを省略するとどうなるか
- [Evaluate Target Health] を [No] に設定するとどうなるか

エイリアスレコードにヘルスチェックを関連付けるとどうなるか

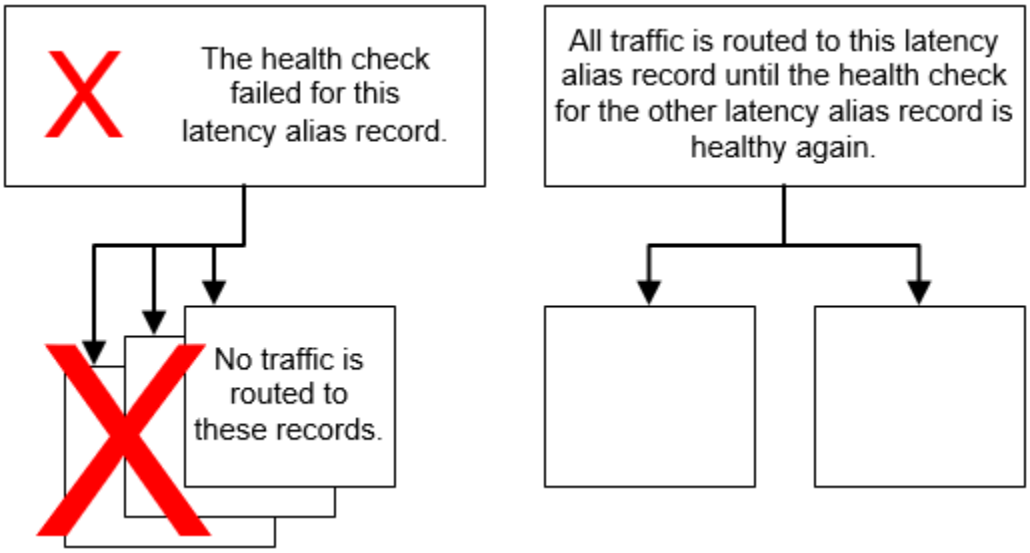
[Evaluate Target Health] の値を [Yes] に設定する代わりに (または設定したうえで)、エイリアスレコードにヘルスチェックを関連付けることができます。ただし、実用性の面からいうと、基盤になるリソース (HTTP サーバー、データベースサーバーなど、エイリアスレコードの参照先となるリソース) の正常性に基づいて Route 53 がクエリに応答する、という構成の方が一般的です。例えば、次の構成を考えてみます。

- 一連の加重レコードをエイリアスターゲットとするレイテンシーエイリアスレコードにヘルスチェックを割り当てます。
- レイテンシーエイリアスレコードの [Evaluate Target Health] の値は、[Yes] に設定します。

この設定で、加重レコードに応じた値を Route 53 が返すためには、次の 2 点が満たされなければなりません。

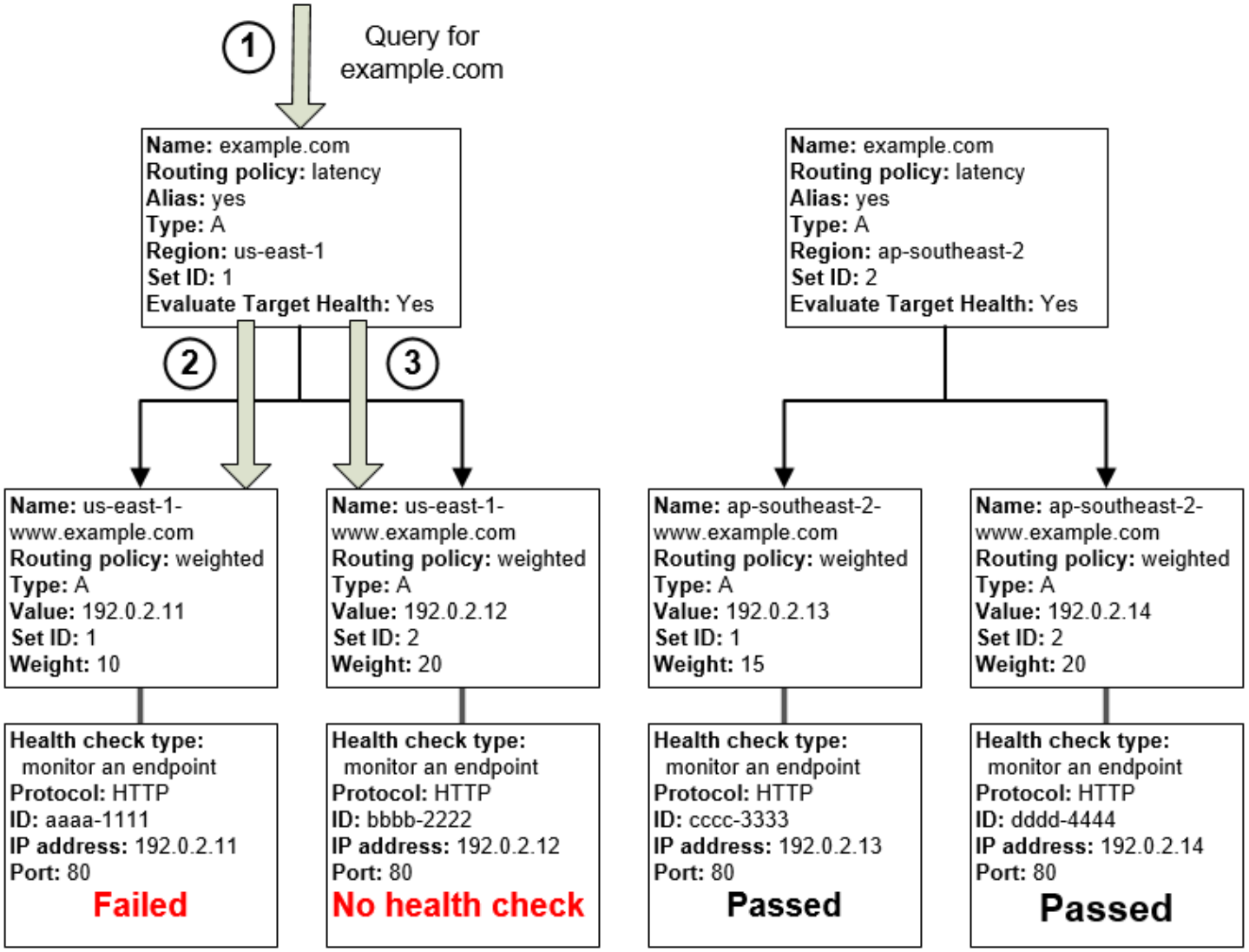
- レイテンシーエイリアスレコードに関連付けられているヘルスチェックが合格すること。
- 少なくとも 1 つの加重レコードが、合格したヘルスチェックに関連付けられているか、またはヘルスチェックそのものに関連付けられていないことから、正常と見なされること。後者のケースでは、Route 53 は常に加重レコードを正常と見なします。

次の図では、左上のレイテンシーエイリアスレコードのヘルスチェックに失敗しています。結果として、Route 53 は、加重レコードのすべてが正常であっても、レイテンシーエイリアスレコードが参照する加重レコードのいずれかを使用したクエリの応答を停止します。Route 53 は、レイテンシーエイリアスレコードのヘルスチェックが再び正常となった場合にのみ、これらの加重レコードの再チェックを開始します。(例外については、「ヘルスチェックが設定されている場合に Amazon Route 53 がレコードを選択する方法」を参照してください。)



ヘルスチェックを省略するとどうなるか

複雑な構成では、エイリアス以外のすべてのレコードにヘルスチェックを関連付けることが大切です。次の例では、us-east-1 リージョンのいずれかの加重レコードでヘルスチェックが欠落しています。



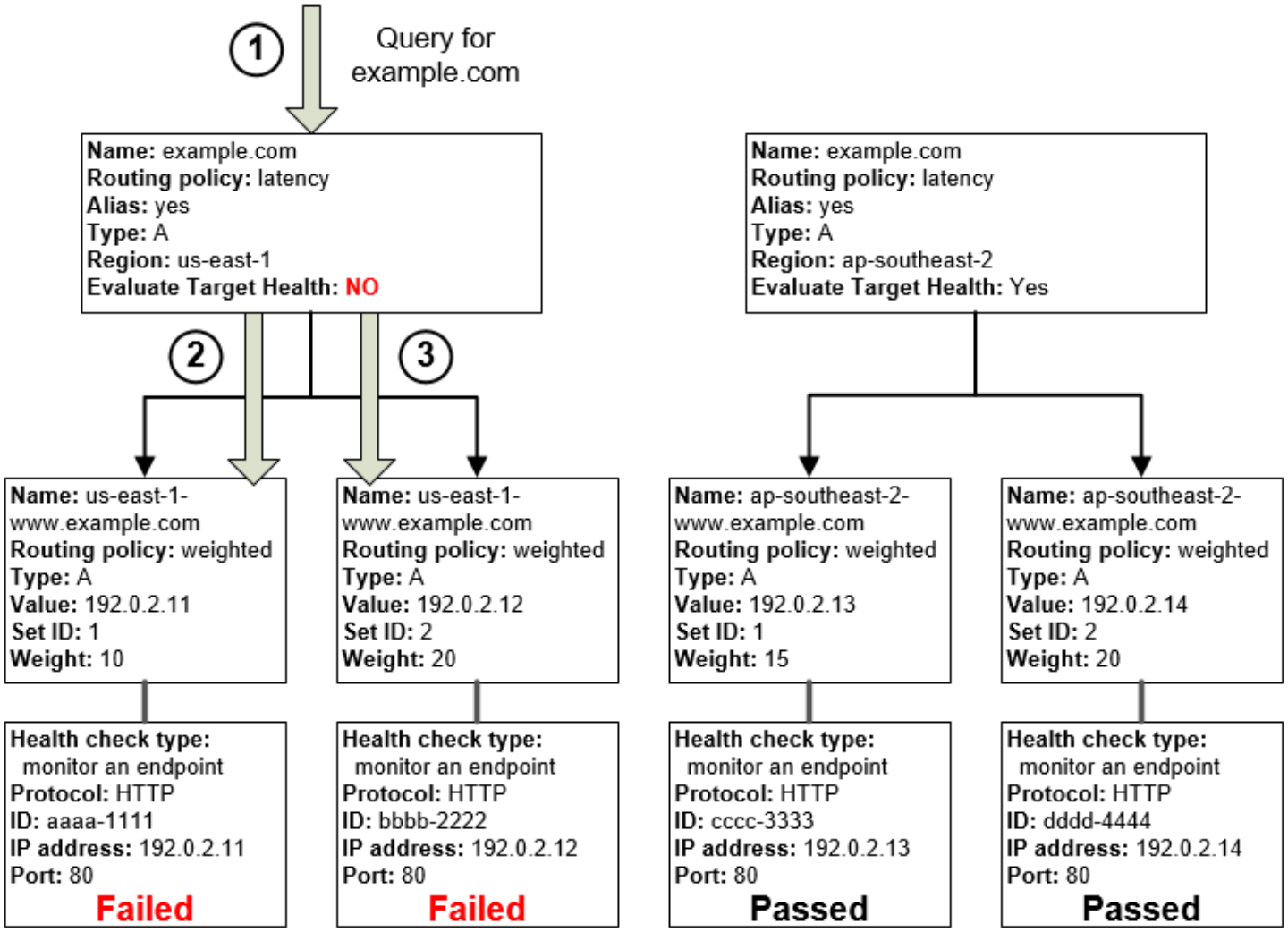
以下に、この構成の非エイリアスレコードでヘルスチェックを省略した場合の動作を説明します。

1. Route 53 が example.com のクエリを受信します。要求元のユーザーに対するレイテンシーに基づいて、Route 53 は us-east-1 リージョンのレイテンシーエイリアスレコードを選択します。
2. Route 53 は、レイテンシーエイリアスレコードのエイリアスターゲットを探し、対応するヘルスチェックのステータスをチェックします。一方の加重レコードのヘルスチェックが不合格となり、そのレコードは考慮の対象から除外されます。
3. us-east-1 リージョンのエイリアスターゲット内のもう一方の加重レコードにはヘルスチェックが関連付けられていません。ヘルスチェックを行わない限り、対応するリソースが正常であるかどうかを Route 53 が認識する方法はありません。リソースは正常なので、Route 53 はクエリに応じて適切な値を返します。

[Evaluate Target Health] を [No] に設定するとどうなるか

一般に、ツリー内のすべてのエイリアスレコードについて、[ターゲットの正常性の評価] を [Yes (あり)] に設定する必要があります。[Evaluate Target Health (ターゲットの正常性の評価)] を [No (なし)] に設定した場合、Route 53 は、レコードのヘルスチェックが失敗した場合でも、エイリアスレコードが参照するレコードにトラフィックをルーティングし続けます。

次の例では、すべての加重レコードに関連付けられたヘルスチェックがありますが、us-east-1 リージョンのレイテンシーエイリアスレコードの [ターゲットの正常性の評価] は [No (なし)] に設定されています。



この構成でエイリアスレコードの [Evaluate Target Health] を [No] に設定した場合の動作を以下に説明します。

1. Route 53 が example.com のクエリを受信します。要求元のユーザーに対するレイテンシーに基づいて、Route 53 は us-east-1 リージョンのレイテンシーエイリアスレコードを選択します。

2. Route 53 は、レイテンシーエイリアスレコードのエイリアスターゲットを特定し、対応するヘルスチェックを調べます。どちらも不合格です。
3. us-east-1 リージョンでは、レイテンシーエイリアスレコードの [Evaluate Target Health] の値が [No] であるため、Route 53 は、このブランチの中からいずれかのレコードを選ぶ必要があります。ブランチの出発点に戻って ap-southeast-2 リージョンから正常なレコードを探すことはありません。

ヘルスチェックが設定されている場合に Amazon Route 53 がレコードを選択する方法

同じ名前、同じタイプ (A または AAAA など)、および同じルーティングポリシー (加重またはフェイルオーバーなど) を持つレコードグループ内のすべてのレコードのヘルスチェックを設定すると、Route 53 は正常なレコードを選択し、そのレコードから該当する値を返すことによって、DNS クエリに応答します。

例えば、3 つの加重された A レコードを作成し、そのすべてにヘルスチェックを割り当てたとします。1 つのレコードでヘルスチェックが正常でない場合、Route 53 は他の 2 つのレコードのいずれかの IP アドレスで DNS クエリに応答します。

正常なレコードを Route 53 が選択する際の動作を以下に示します。

1. 最初に Route 53 は、ルーティングポリシーと各レコードに指定した値に基づいてレコードを選択します。例えば、加重レコードの場合、Route 53 は各レコードに指定した重みに基づいてレコードを選択します。
2. Route 53 は、レコードが正常であるかどうかを判断します。
   - 関連付けられたヘルスチェックを持つ非エイリアスレコード – ヘルスチェックを非エイリアスレコードに関連付けた場合、Route 53 はヘルスチェックの現在のステータスをチェックします。

     Route 53 は、ヘルスチェックで指定されたエンドポイントの正常性を定期的にチェックします。DNS クエリが到着した時点でヘルスチェックを実行するわけではありません。

     ヘルスチェックはエイリアスレコードに関連付けることができますが、ヘルスチェックはエイリアス以外のレコードにのみ関連付けることをお勧めします。詳細については、「エイリアスレコードにヘルスチェックを関連付けるとどうなるか」を参照してください。

- [Evaluate Target Health (ターゲットの正常性の評価)] が [Yes (あり)] に設定されたエイリアスレコード – Route 53 は、エイリアスレコードが参照するリソース (例えば、ELB ロードバランサーまたは同じホストゾーン内の別のレコード) のヘルスステータスをチェックします。

3. レコードが正常であれば、Route 53 は、適切な値 (IP アドレスなど) でクエリに応答します。

   レコードが異常である場合、Route 53 は同じ基準で別のレコードを選択し、正常なレコードが見つかるまでそのプロセスを繰り返します。

レコードを選択する際、Route 53 は以下の基準を使用します。

ヘルスチェックのないレコードは常に正常

同じ名前とタイプを持つレコードのグループ内で、レコードに関連付けられているヘルスチェックがない場合、Route 53 はそのレコードを常に正常と見なします。クエリへの応答の候補には、そのレコードが常に含まれます。

レコードが正常でない場合は、すべてのレコードが正常

レコードのグループ内に正常なレコードが 1 つも存在しなかった場合でも、Route 53 は DNS クエリへの応答として何かを返す必要がありますが、レコードの優劣を選択するための判断材料がありません。この状況では、グループに含まれるすべてのレコードが正常と見なされ、Route 53 はルーティングポリシーと各レコードに指定した値に基づいて 1 つを選択します。

重みが 0 である加重レコード

加重レコードのグループ内のすべてのレコードにヘルスチェックを追加する一方で、一部のレコードにゼロ以外の重みを付け、他のレコードの重みをゼロにした場合、ヘルスチェックは、次の例外を除いて、すべてのレコードの重みがゼロ以外の場合と同様に動作します。

- 最初に Route 53 は、ゼロ以外の加重レコード (存在する場合) のみを対象とします。
- 重みが 0 より大きいレコードがいずれも異常であった場合、Route 53 は、重みがゼロである加重レコードを対象にします。

一部の状況では Route 53 は重みがゼロである加重レコードを考慮するので、重みがゼロのターゲットにも DNS クエリに対する実行可能な回答があるようにすることが重要です。

加重レコードの詳細については、「ヘルスチェックと加重ルーティング」を参照してください。

エイリアスレコード

各エイリアスレコードに対して [ターゲットの正常性の評価] を [Yes (あり)] に設定することで、エイリアスレコードのヘルスチェックを設定することもできます。これにより Route 53 は、レ

コードがトラフィックをルーティングする先のリソース (例えば、ELB ロードバランサーまたは同じホストされたゾーン内の別のレコード) で、その正常性を評価します。

例えば、エイリアスレコードのエイリアスターゲットが、一連の加重レコードから成るグループであり、そのグループの加重レコードの重みがいずれもゼロ以外であるとします。

- 正常な加重レコードが 1 つでもあれば、Route 53 は、そのエイリアスレコードを正常と見なします。
- 正常な加重レコードが存在しない場合、Route 53 は、そのエイリアスレコードを異常と見なします。
- 少なくとも 1 つの加重レコードが正常に戻るまで、Route 53 は、そのツリーのブランチのレコードを候補から除外します。

詳細については、「Amazon Route 53 の複雑な構成でのヘルスチェックの動作」を参照してください。

フェイルオーバーレコード

フェイルオーバーレコードは、通常、他のルーティングタイプと同じように動作します。ヘルスチェックを作成し、それらを非エイリアスレコードに関連付けて、エイリアスレコードの [ターゲットの正常性の評価] を [Yes (あり)] に設定します。次の点に注意してください。

- プライマリレコードとセカンダリレコードは、どちらも非エイリアスレコードまたはエイリアスレコードです。
- プライマリフェイルオーバーレコードとセカンダリフェイルオーバーレコードの両方にヘルスチェックが関連付けられている場合、Route 53 は、リクエストに対して次のように応答します。
  - プライマリレコードが正常 (ヘルスチェックのエンドポイントが正常) であると判断した Route 53 は、 DNS クエリへの応答としてプライマリレコードのみを返します。
  - プライマリレコードが異常でありセカンダリレコードが正常であると Route 53 が判断した場合は、セカンダリレコードが返されます。
  - プライマリレコードとセカンダリレコードの両方が異常であると Route 53 が判断した場合は、プライマリレコードが返されます。
- セカンダリレコードを設定する際、ヘルスチェックを追加するかどうかは任意です。セカンダリのヘルスチェックが省略されていて、プライマリレコードのヘルスチェックエンドポイントが異常だった場合、Route 53 は常にセカンダリレコードで DNS クエリに応答します。セカンダリレコードが異常であったとしても同様です。

詳細については、以下のトピックを参照してください。

- 1 つのプライマリリソースおよび 1 つのセカンダリリソースを使用したフェイルオーバー (アクティブ/パッシブ) の設定
- 複数のプライマリリソースおよびセカンダリリソースを使用したフェイルオーバー (アクティブ/パッシブ) の設定

フェイルオーバー (アクティブ/アクティブとアクティブ/パッシブ) の設定

Route 53 のヘルスチェックを使用して、フェイルオーバー (アクティブ/アクティブとアクティブ/パッシブ) を設定できます。フェイルオーバー以外のいずれかのルーティングポリシー (またはルーティングポリシーの組み合わせ) を使用して、フェイルオーバー (アクティブ/アクティブ) を設定し、フェイルオーバールーティングポリシーを使用してフェイルオーバー (アクティブ/パッシブ) を設定します。

トピック

- フェイルオーバー (アクティブ/アクティブ)
- アクティブ/パッシブ (フェイルオーバー)。

フェイルオーバー (アクティブ/アクティブ)

すべてのリソースをほとんどの時間で利用できるようにするには、このフェイルオーバー設定を使用します。利用不可能になったリソースについては、Route 53 は異常として検出できるので、以後、クエリへの応答に使用しなくなります。

アクティブ/アクティブのフェイルオーバーでは、Route 53 がそれらを異常と見なさない限り、同じ名前、同じタイプ (A または AAAAなど)、および同じルーティングポリシー (加重またはレイテンシーなど) を持つすべてのレコードがアクティブとなります。Route 53 は、正常な任意のレコードを使用して DNS クエリに応答できます。

アクティブ/パッシブ (フェイルオーバー)。

プライマリリソースまたはリソースグループをほとんどの時間で利用可能にして、すべてのプライマリリソースが使用できなくなった場合に備えて、セカンダリリソースまたはリソースグループをスタンバイ状態にする場合は、フェイルオーバー (アクティブ/パッシブ) 設定を使用します。クエリへの応答で Route 53 が返すのは、正常なプライマリリソースのみです。すべてのプライマリリソースで異常が発生した場合、Route 53 は、DNS クエリへの応答として正常なセカンダリリソースのみを返します。

トピック

- 1 つのプライマリリソースおよび 1 つのセカンダリリソースを使用したフェイルオーバー (アクティブ/パッシブ) の設定
- 複数のプライマリリソースおよびセカンダリリソースを使用したフェイルオーバー (アクティブ/パッシブ) の設定
- 加重レコードを使用してフェイルオーバー (アクティブ/パッシブ) を構成する

1 つのプライマリリソースおよび 1 つのセカンダリリソースを使用したフェイルオーバー (アクティブ/パッシブ) の設定

1 つのプライマリレコードと 1 つのセカンダリレコードでフェイルオーバー (アクティブ/パッシブ) 設定を作成するには、レコードを作成し、ルーティングポリシーとして [フェイルオーバー] を指定します。プライマリリソースが正常な場合、Route 53 はプライマリレコードを使用して DNS クエリに応答します。プライマリリソースが異常な場合、Route 53 はセカンダリレコードを使用して DNS クエリに応答します。

複数のプライマリリソースおよびセカンダリリソースを使用したフェイルオーバー (アクティブ/パッシブ) の設定

プライマリレコード、セカンダリレコード、またはその両方に複数のリソースを関連付けることもできます。この構成では、 関連付けられたリソースの少なくとも 1 つが正常である限り、Route 53 はプライマリフェイルオーバーレコードが正常であると見なします。詳細については、「ヘルスチェックが設定されている場合に Amazon Route 53 がレコードを選択する方法」を参照してください。

プライマリまたはセカンダリレコードの複数のリソースでフェイルオーバー (アクティブ/パッシブ) を設定するには、次のタスクを実行します。

1. トラフィックをルーティングするリソース (EC2 インスタンスやデータセンター内のウェブサーバーなど) ごとに、ヘルスチェックを作成します。

   > **Note**
   >
   > エイリアスレコードを作成できる AWS リソースにトラフィックをルーティングする場合は、それらのリソースのヘルスチェックを作成しないでください。エイリアスレコードを作成する場合は、[ターゲットの正常性の評価] を [Yes (あり)] に設定します。

   詳細については、「ヘルスチェックの作成と更新」を参照してください。
2. プライマリリソースのレコードを作成し、次の値を指定します。

- 各レコードに同じ名前、タイプ、ルーティングポリシーを割り当てます。例えば、すべてが failover-primary.example.com という名前の 3 つの加重 A レコードを作成することができます。
- エイリアスレコードを作成できる AWS リソースを使用している場合は、ターゲットの状態の評価に「はい」と指定します。

  エイリアスレコードを作成できないリソースを使用している場合は、ステップ 1 の該当するヘルスチェックを各レコードに関連付けます。

詳細については、「Amazon Route 53 コンソールを使用したレコードの作成」を参照してください。

3. 該当する場合、セカンダリリソースのレコードを作成し、次の値を指定します。
   - 各レコードに同じ名前、タイプ、ルーティングポリシーを割り当てます。例えば、すべてが failover-secondary.example.com という名前の 3 つの加重 A レコードを作成することができます。
   - エイリアスレコードを作成できる AWS リソースを使用している場合は、ターゲットの状態の評価に「はい」と指定します。

     エイリアスレコードを作成できないリソースを使用している場合は、ステップ 1 の該当するヘルスチェックを各レコードに関連付けます。

   > **Note**
   >
   > 一部のお客様は、プライマリリソースとしてウェブサーバーを使用し、ウェブサイトエンドポイントとして構成された Amazon S3 バケットをセカンダリリソースとして使用されています。S3 バケットには、「一時的に使用できません」という簡単なメッセージが含まれています。その構成を使用している場合は、この手順をスキップして、ステップ 4 でセカンダリリソースのフェイルオーバーエイリアスレコードを作成します。

4. プライマリとセカンダリの 2 つのフェイルオーバーエイリアスレコードを作成し、次の値を指定します。

   プライマリレコード

   - Name (名前) – Route 53 でトラフィックをルーティングさせるドメイン名 (example.com)、またはサブドメイン名 (www.example.com) を指定します。
   - エイリアス – **あり** を指定します。
   - エイリアス先 - ステップ 2 で作成したレコードの名前を指定します。
   - ルーティングポリシー – フェイルオーバーを指定します。

- フェイルオーバーレコードのタイプ – プライマリを指定します。
- ターゲットの正常性の評価 – あり を指定します。
- ヘルスチェックとの関連付け – なし を指定します。

セカンダリレコード

- 名前 - プライマリレコードに指定したものと同じ名前を指定します。
- エイリアス – ありを指定します。
- エイリアス先 – ステップ 3 でセカンダリリソースのレコードを作成している場合は、レコードの名前を指定します。セカンダリリソースに Amazon S3 バケットを使用している場合は、ウェブサイトエンドポイントの DNS 名を指定します。
- ルーティングポリシー - フェイルオーバーを指定します。
- フェイルオーバーレコードのタイプ – セカンダリ を指定します。
- ターゲットの正常性の評価 - あり を指定します。
- ヘルスチェックとの関連付け - なしを指定します。

加重レコードを使用してフェイルオーバー (アクティブ/パッシブ) を構成する

また、警告付きのフェイルオーバー (アクティブ/パッシブ) のために加重されたレコードを使用することもできます。一部のレコードに対してゼロ以外の重みを指定し、他のレコードに対してゼロの重みを指定した場合、Route 53 は重みがゼロ以外の健全なレコードのみを使用して DNS クエリに応答します。重みがゼロより大きいレコードがいずれも異常であった場合、Route 53 は重みがゼロであるレコードを使用してクエリに応答します。

> **Note**
>
> Route 53 がゼロの重みを持つレコードを使用して DNS クエリに応答するためには、ゼロ以外の重みを持つすべてのレコードが異常とみなされる必要があります。これにより、ウェブサーバーなどの最後の正常なリソースが、他のリソースが利用できないときにすべてのトラフィックを処理できない場合、ウェブアプリケーションまたはウェブサイトが信頼できなくなる可能性があります。

プライベートホストゾーンのフェイルオーバーの設定

プライベートホストゾーンにフェイルオーバーレコードを作成する方法は、次の点に注意してください。

- Route 53 ヘルスチェッカーは VPC の外にあります。IP アドレスを使用して VPC 内のエンドポイントの正常性をチェックするには、VPC 内のインスタンスにパブリック IP アドレスを割り当てる必要があります。
- また、CloudWatch メトリクスを作成し、アラームをメトリクスに関連付けて、アラームのデータストリームに基づくヘルスチェックを作成することもできます。例えば、EC2 の `StatusCheckFailed` メトリクスのステータスをチェックする CloudWatch メトリクスを作成、このメトリクスにアラームを追加、さらにアラームのデータストリームに基づいたヘルスチェックを作成することが可能であり、バーチャルプライベートクラウド (VPC) 内にプライベート IP アドレスのみがあるインスタンスをチェックします。CloudWatch コンソールを使用して CloudWatch メトリクスおよびアラームを作成する方法について詳細は、Amazon CloudWatch ユーザーガイドを参照してください。

詳細については、「プライベートホストゾーンの使用」および「CloudWatch を使用したヘルスチェックのモニタリング」を参照してください。

Amazon Route 53 でフェイルオーバーの問題を回避する方法

Route 53 に実装されたフェイルオーバーアルゴリズムは、正常なエンドポイントにトラフィックをルーティングするだけでなく、ヘルスチェックやアプリケーションの設定ミス、エンドポイントの過負荷、パーティションの障害などに起因する最悪のシナリオを回避するように設計されています。

トピック

- Amazon Route 53 でカスケードの失敗を回避する方法
- Amazon Route 53 でのインターネットの分断への対処方法

Amazon Route 53 でカスケードの失敗を回避する方法

カスケードの失敗に対する第一の備えとして、すべてのリクエストルーティングアルゴリズム (加重やフェイルオーバーなど) には、最後の手段となるモードが用意されています。この特殊なモードでは、レコードがすべて異常と判断された場合に、Route 53 アルゴリズムは、再びすべてのレコードを正常と見なすようになります。

例えば、いくつかのホスト上で、アプリケーションの全インスタンスがヘルスチェックリクエストを拒否している場合、Route 53 の DNS サーバーは、DNS 応答を拒否したり NXDOMAIN (存在しないドメイン) 応答を返したりするのではなく、何等かの応答を返します。アプリケーションがユーザーに応答しても、ヘルスチェックには不合格になることがあるため、設定ミスから生じる問題をある程度防ぐことができます。

同様に、アプリケーションに過剰な負荷がかかっていて、3 つのエンドポイントのうち 1 つがヘルスチェックで不合格と判断され、Route 53 の DNS 応答から除外された場合、Route 53 は残りの 2 つのエンドポイントを使って応答を返します。残りのエンドポイントがそれ以上の負荷に耐えきれず障害が発生した場合、Route 53 は再度、3 つすべてのエンドポイントにリクエストを分配するようになります。

Amazon Route 53 でのインターネットの分断への対処方法

一般的ではありませんが、インターネットに重大な分断が生じる場合があります。つまり、大規模な地理的リージョン間でインターネット経由の相互通信ができなくなることがあります。インターネットに分断が生じている間、エンドポイントの正常性ステータスに関して導き出される結論が Route 53 の拠点によって違ったり、CloudWatch に報告されるステータスと異なることがあります。各 AWS リージョンの Route 53 ヘルスチェッカーは、すべての Route 53 ロケーションにヘルスチェックステータスを常に送信しています。インターネットの分断が生じている間は、Route 53 の各拠点は、そうしたステータスの一部 (通常は最も近いリージョンのステータス) にしかアクセスできなくなります。

例えば、インターネットの分断で南米との接続に影響が生じているとします。その間、 南米 (サンパウロ) にある Route 53 DNS サーバーは、 AWS リージョンの南米 (サンパウロ) にあるヘルスチェックエンドポイントには問題なくアクセスできますが、その他のエンドポイントには正常にアクセスできない可能性があります。同時に、米国東部 (オハイオ) の Route 53 は、南米 (サンパウロ) リージョンのヘルスチェックエンドポイントへのアクセスに支障があるとして、対応するレコードを異常と判断することが考えられます。

こうした分断によって、Route 53 の各拠点が、それぞれ域内のエンドポイントの可視性によってエンドポイントの正常性ステータスを判断するようになり、最終的に拠点ごとにその結論が異なる、という状況に発展する可能性があります。そのため、Route 53 の各拠点は、到達可能なごく一部のヘルスチェッカーがエンドポイントを正常と判断していれば、そのエンドポイントを正常と見なします。

ヘルスチェックの名前付けとタグ付け

Amazon Route 53 ヘルスチェックにタグを追加して、各ヘルスチェックにヘルスチェック ID よりもわかりやすい名前を付けることができます。これらは、 が AWS 請求書を整理するために AWS Billing and Cost Management 提供するのと同じタグです。コスト配分でタグがどのように使用されているかについては、AWS Billing ユーザーガイドの コスト配分タグを使用したカスタム請求レポートを参照してください。

それぞれのタグは、キー (タグの名前) と値で構成されます。キーと値は、どちらもお客様が定義します。ヘルスチェックにタグを追加するときは、キーと値に次の値を持つタグを 1 つ追加することをお勧めします。

- キー - 名前
- 値: ヘルスチェックに割り当てる名前。

Name タグの値は Route 53 コンソールのヘルスチェックのリストに表示されるため、ヘルスチェックを互いに簡単に区別できます。ヘルスチェックのタグを表示するには、ヘルスチェックを選択し、[タグ] タブをクリックします。

タグの詳細については、次のトピックを参照してください。

- Route 53 コンソールでヘルスチェックを追加または編集するときに、名前タグを追加、編集、または削除する場合は、ヘルスチェックの作成と更新 をご覧ください。
- Route 53 リソースにタグを付ける方法の概要については、「Amazon Route 53 リソースのタグ付け」を参照してください。

タグの制限

タグには以下のベーシックな制限があります。

- リソースあたりのタグの最大数 – 新しいコンソールは 50、古いコンソールは 10。
- キーの最大長 - 128 文字 (Unicode)
- 値の最大長 - 256 文字 (Unicode)
- キーと値に使用できる文字: アルファベットの大文字と小文字 (UTF-8 文字セット)、数字、スペース、および以下の記号文字 (_ . : / = + - @) です。
- タグのキーと値は大文字と小文字が区別されます。
- キーまたは値に aws: プレフィックスを使用しないでください。 AWS 用に予約されています。

ヘルスチェックに対するタグの追加、編集、削除

次の手順は、ヘルスチェックのタグを Route 53 コンソールで使用する方法を示しています。

> **Note**
>
> Route 53 はヘルスチェックコンソールを更新しています。旧コンソールは移行期間中も引き続きご使用いただけます。

お使いのコンソールのタブを選択します。

- 新しいコンソール
- 旧コンソール

New console

ヘルスチェックにタグを追加するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [ヘルスチェック] を選択します。
3. タグを追加するヘルスチェックのリンクされた ID を選択します。
4. 下部ページで、[タグ] タブ、[管理]、[新しいタグを追加] の順に選択します。
5. [キー] フィールドにタグの名前を入力し、[値] フィールドに値を入力します。
6. [保存] を選択します。

ヘルスチェックのタグを編集するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [ヘルスチェック] を選択します。
3. ヘルスチェックのリンクされた ID を選択します。
4. 下部のペインで [タグ] タブ、[管理] の順に選択します。
5. タグを編集および追加することができるようになりました。
6. [保存] を選択します。

ヘルスチェックのタグを削除するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [ヘルスチェック] を選択します。
3. ヘルスチェックのリンクされた ID を選択します。
4. 下部のペインで [タグ] タブ、[管理] の順に選択します。
5. 削除するタグの横にある [削除] を選択します。
6. [保存] を選択します。

Old console

ヘルスチェックにタグを追加するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [Health Checks (ヘルスチェック)] を選択します。
3. ヘルスチェックを選択します。同じタグを複数のヘルスチェックに追加する場合は、複数のヘルスチェックを選択してください。
4. 下部のペインで [Tags] タブ、[Add/Edit Tags] の順に選択します。
5. [Add/Edit Tags] ダイアログボックスの [Key] フィールドにタグの名前を入力し、[Value] フィールドに値を入力します。
6. [Apply changes (変更の適用)] を選択します。

ヘルスチェックのタグを編集するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [Health Checks (ヘルスチェック)] を選択します。
3. ヘルスチェックを選択します。

   同じタグを共有する複数のヘルスチェックを選択した場合に、すべてのタグの値を一度に編集することはできません。ただし、指定したタグを含むヘルスチェックと共に含まないヘルスチェックを 1 つ以上選択した場合、複数のヘルスチェックに表示されるタグの値を編集できます。

たとえば、Cost Center タグが含まれている複数のヘルスチェックと、含まれていない 1 つのヘルスチェックを選択したとします。このとき、タグを追加するオプションを選択して、キーに「Cost Center」、値に「777」を指定します。選択されたヘルスチェックのうち、既に Cost Center タグが設定されているヘルスチェックに対して、Route 53 はその値を 777 に変更します。Cost Center タグを持たないヘルスチェックに対しては、 Route 53 がそのタグを追加し、値を 777 に設定します。

4. 下部のペインで [Tags] タブ、[Add/Edit Tags] の順に選択します。
5. [Add/Edit Tags] ダイアログボックスで値を編集します。
6. [保存] を選択します。

ヘルスチェックのタグを削除するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [Health Checks (ヘルスチェック)] を選択します。
3. ヘルスチェックを選択します。同じタグを複数のヘルスチェックから削除する場合は、複数のヘルスチェックを選択してください。
4. 下部のペインで [Tags] タブ、[Add/Edit Tags] の順に選択します。
5. [Add/Edit Tags] ダイアログボックスで、削除するタグの横にある赤色の *X* を選択します。
6. [Save] を選択します。

Amazon Route 53 API バージョン 2012-12-12 未満でのヘルスチェックの使用

ヘルスチェックは、Amazon Route 53 API 2012-12-12 以降のバージョンでサポートされます。ヘルスチェックが設定されているレコードがホストゾーンに存在する場合は、2012-12-12 API 以降のみを使用するようお勧めします。それより前の API バージョンでのヘルスチェックの使用には、次の制限があります。

- `EvaluateTargetHealth`、`Failover`、`HealthCheckId` のいずれかの要素を含んだレコードを `ChangeResourceRecordSets` アクションで作成したり削除したりすることができません。

- それらの要素を含んだレコードを ListResourceRecordSets アクションでリストすることはできますが、出力結果にはそれらの要素が含まれません。サポート外の属性がレコードに含まれていることを示すメッセージが、レスポンスの Value 要素に格納されます。

ヘルスチェックのステータス監視と通知の受信

Amazon Route 53 コンソールで、ヘルスチェックのステータスを監視できます。ヘルスチェックのステータスが変更されたら自動通知を受け取るように、CloudWatch アラームを設定することもできます。

トピック

- ヘルスチェックのステータスと失敗理由を表示する
- ヘルスチェッカーとエンドポイント間のレイテンシーのモニタリング
- CloudWatch を使用したヘルスチェックのモニタリング

ヘルスチェックのステータスと失敗理由を表示する

Route 53 コンソールでは、ヘルスチェックのステータス (正常または異常) を、 Route 53 ヘルスチェッカーのレポートにより表示できます。計算されたヘルスチェックグラフを除くすべてのヘルスチェックでは、最後のヘルスチェックが失敗した理由を確認できます (例: ヘルスチェッカーがエンドポイントとの接続を確立できなかった)。

> **Note**
>
> Route 53 のヘルスチェックコンソールを更新中です。旧コンソールは移行期間中も引き続きご使用いただけます。

お使いのコンソールのタブを選択します。

- 新しいコンソール
- 旧コンソール

New console

ヘルスチェックのステータスと最後の失敗の理由を表示するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。

2. ナビゲーションペインで [ヘルスチェック] を選択します。
3. 全ヘルスチェックのステータスの概要 (正常または異常) を確認するには、[Status] (ステータス) 列を参照します。詳細については、「Amazon Route 53 でヘルスチェックの正常性を判断する方法」を参照してください。
4. 計算されたヘルスチェックグラフを除くすべてのヘルスチェックについて、指定されたエンドポイントの状態をチェックする Route 53 ヘルスチェッカーのステータスを確認できます。
5. 詳細を表示するヘルスチェックのリンク ID を選択します。
6. 下部のペインで、[ヘルスチェッカー] タブを選択します。

> **Note**
>
> ヘルスチェックのステータスと最後の失敗理由が [Status] 列に表示されるには、新しいヘルスチェックが Route 53 の各ヘルスチェッカーに伝達される必要があります。伝達が完了するまで、その列にはステータスが利用できない旨を示すメッセージが表示されます。

7. 表には、次の値が含まれています。

   Health checker IP

   ヘルスチェックを実行した Route 53 ヘルスチェッカーの IP アドレス。

   Last checked

   ヘルスチェックの日付と時刻または最後の障害の日付と時刻。

   ステータス

   ヘルスチェックの現在のステータスまたは最後にヘルスチェックが失敗した理由。

Old console

ヘルスチェックのステータスと最後の失敗の理由を表示するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [Health Checks (ヘルスチェック)] を選択します。

3. 全ヘルスチェックのステータスの概要 (正常または異常) を確認するには、[Status] (ステータス) 列を参照します。詳細については、「Amazon Route 53 でヘルスチェックの正常性を判断する方法」を参照してください。
4. 計算されたヘルスチェックグラフを除くすべてのヘルスチェックについて、指定されたエンドポイントの状態をチェックする Route 53 ヘルスチェッカーのステータスを確認できます。ヘルスチェックを選択します。
5. 下部のペインで、[Health Checkers] タブを選択します。

> **Note**
>
> ヘルスチェックのステータスと最後の失敗理由が [Status] 列に表示されるには、新しいヘルスチェックが Route 53 の各ヘルスチェッカーに伝達される必要があります。伝達が完了するまで、その列にはステータスが利用できない旨を示すメッセージが表示されます。

6. ヘルスチェックの現在のステータスを表示するか、最後の失敗の日時と理由を表示するかを選択します。[Status] タブの表には次の値が表示されます。

   Health checker IP

   ヘルスチェックを実行した Route 53 ヘルスチェッカーの IP アドレス。

   Last checked

   [Status] タブの上部で選択したオプションに応じて、ヘルスチェックの日時または最後の失敗の日時。

   ステータス

   [Status] タブの上部で選択したオプションに応じて、ヘルスチェックの現在のステータスまたは最後にヘルスチェックが失敗した理由。

ヘルスチェッカーとエンドポイント間のレイテンシーのモニタリング

ヘルスチェックの作成時に、 (他のヘルスチェックのステータスではない) エンドポイントのステータスの監視を選択して [Latency graphs (レイテンシーグラフ)] オプションを選択した場合、Route 53 コンソールの CloudWatch グラフに次の値を表示することができます。

- Route 53 ヘルスチェッカーがエンドポイントとの TCP 接続を確立するのにかかる平均時間 (ミリ秒)
- Route 53 ヘルスチェッカーが HTTP または HTTPS リクエストへの応答の先頭バイトを受け取るまでにかかった平均時間 (ミリ秒)
- Route 53 ヘルスチェッカーが SSL/TLS ハンドシェイクを完了するまでにかかった平均時間 (ミリ秒)

> **Note**
>
> 既存のヘルスチェックではレイテンシーのモニタリングを有効にできません。

> **Important**
>
> ヘルスチェッカーは 16 個の冗長アベイラビリティーゾーンで実行されます。デプロイ、更新、メンテナンスなどの理由で、アベイラビリティーゾーンを使用できないことがあります。ヘルスチェックシステムは、お客様に影響を及ぼすことがないように、これを考慮して設計されています。

> **Note**
>
> Route 53 のヘルスチェックコンソールを更新中です。旧コンソールは移行期間中も引き続きご使用いただけます。

お使いのコンソールのタブを選択します。

- 新しいコンソール
- 旧コンソール

New console

Route 53 ヘルスチェッカーとエンドポイント間のレイテンシーを確認するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。

2. ナビゲーションペインで [ヘルスチェック] を選択します。
3. メトリクスを表示するヘルスチェックのリンク ID を選択します。エンドポイントの状態を監視し、[Latency graphs] オプションが有効になっているヘルスチェックについてのみ、レイテンシーデータを表示できます。
4. 下部のペインで、[メトリクス] タブを選択します。
5. レイテンシーグラフを表示する時間範囲と地理的リージョンを選択します。

   グラフは、指定された時間範囲のステータスを表示します。

   TCP 接続時間 (HTTP および TCP のみ)

   選択した地理的リージョンのRoute 53 ヘルスチェッカーが、エンドポイントとの TCP 接続を確立するのにかかった平均時間 (ミリ秒)。

   先頭バイトまでの時間 (HTTP および HTTPS のみ)

   選択した地理的リージョンの Route 53 ヘルスチェッカーが、HTTP または HTTPS リクエストへの応答の先頭バイトを受け取るまでにかかった平均時間 (ミリ秒)。

   SSL ハンドシェイク (HTTPS のみ) を完了するまでの時間

   選択した地理的リージョンの Route 53 ヘルスチェッカーが、SSL/TLS ハンドシェイクを完了するまでにかかった平均時間 (ミリ秒)。
6. より大きなグラフを表示して異なる設定を指定するには、グラフの右上にある 3 つのドットを選択します。以下の設定を指定することができます。

   Statistic

   CloudWatch がデータに対して実行する計算内容を変更します。

   時間範囲

   夜間、過去 1 週間など、期間ごとのヘルスチェックのステータスを表示します。

   Period

   グラフのデータポイントの間隔を変更します。

   次の点に注意してください。

- ヘルスチェックを作成した直後は、グラフにデータが表示されたり、利用可能なメトリクスのリストにヘルスチェックのメトリクスが表示されたりするまでに数分かかる場合があります。
- グラフは自動的には更新されません。表示を更新するには、更新 () アイコンを選択します。
- ヘルスチェックが接続タイムアウトなどの何らかの理由で失敗した場合、Route 53 はレイテンシーを測定できず、レイテンシーデータは、障害が起きた期間のグラフには表示されなくなります。

Old console

Route 53 ヘルスチェッカーとエンドポイント間のレイテンシーを確認するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [Health Checks (ヘルスチェック)] を選択します。
3. 目的のヘルスチェックの行を選択します。エンドポイントの状態を監視し、[Latency graphs] オプションが有効になっているヘルスチェックについてのみ、レイテンシーデータを表示できます。
4. 下部のペインで、[Latency] タブを選択します。
5. レイテンシーグラフを表示する時間範囲と地理的リージョンを選択します。

   グラフは、指定された時間範囲のステータスを表示します。

   TCP 接続時間 (HTTP および TCP のみ)

   選択した地理的リージョンのRoute 53 ヘルスチェッカーが、エンドポイントとの TCP 接続を確立するのにかかった平均時間 (ミリ秒)。

   先頭バイトまでの時間 (HTTP および HTTPS のみ)

   選択した地理的リージョンの Route 53 ヘルスチェッカーが、HTTP または HTTPS リクエストへの応答の先頭バイトを受け取るまでにかかった平均時間 (ミリ秒)。

SSL ハンドシェイク (HTTPS のみ) を完了するまでの時間

選択した地理的リージョンの Route 53 ヘルスチェッカーが、SSL/TLS ハンドシェイクを完了するまでにかかった平均時間 (ミリ秒)。

> **Note**
>
> 複数のヘルスチェックを選択した場合、グラフには、各ヘルスチェックに対応する行が色分けして表示されます。

6. より大きなグラフを表示し、異なる設定を指定するには、グラフを選択します。以下の設定を指定することができます。

   Statistic

   CloudWatch がデータに対して実行する計算内容を変更します。

   時間範囲

   夜間、過去 1 週間など、期間ごとのヘルスチェックのステータスを表示します。

   Period

   グラフのデータポイントの間隔を変更します。

   次の点に注意してください。

   - ヘルスチェックを作成した直後は、グラフにデータが表示されたり、利用可能なメトリクスのリストにヘルスチェックのメトリクスが表示されたりするまでに数分かかる場合があります。
   - グラフは自動的には更新されません。表示を更新するには、更新 () アイコンを選択します。
   - ヘルスチェックが接続タイムアウトなどの何らかの理由で失敗した場合、Route 53 はレイテンシーを測定できず、レイテンシーデータは、障害が起きた期間のグラフには表示されなくなります。

CloudWatch を使用したヘルスチェックのモニタリング

Route 53 ヘルスチェックは CloudWatch メトリクスと統合されており、次のことを実行できます。

- ヘルスチェックが適切に設定されているかどうかを確認できます。
- 指定した期間のヘルスチェックのステータスを確認できます。
- ヘルスチェックのステータスに不具合がある場合に Amazon SNS アラートを送信するように CloudWatch を設定できます。ただし、ヘルスチェックで不合格となってから、関連する SNS 通知が届くまでには、数分かかる場合があります。

詳細については、「Amazon Route 53 でヘルスチェックの正常性を判断する方法」を参照してください。

トピック

- ヘルスチェックのステータスを表示する
- ヘルスチェックアラームを表示する
- CloudWatch コンソールでヘルスチェックメトリクスを表示する
- SNS 通知を使用してアラームを作成する

ヘルスチェックのステータスを表示する

> **Note**
>
> Route 53 のヘルスチェックコンソールを更新中です。旧コンソールは移行期間中も引き続きご使用いただけます。

お使いのコンソールのタブを選択します。

- 新しいコンソール
- 旧コンソール

New console

ヘルスチェックのステータスを表示するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [ヘルスチェック] を選択します。
3. メトリクスを表示するヘルスチェックのリンクされた ID を選択します。
4. 下部のペインで、[メトリクス] タブを選択します。

   2 つのグラフに、1 分間隔で過去 1 時間のステータスが表示されます。

   ヘルスチェックステータス

   グラフには、エンドポイントの正常性に対する Route 53 の診断結果が (1は正常、0は異常として) 表示されます

   エンドポイントが正常であるとレポートするヘルスチェッカー (パーセント)

   エンドポイントのみをモニタリングするヘルスチェックについて、グラフには、選択されたエンドポイントを正常であると見なしている Route 53 ヘルスチェッカーの割合が示されます。

   ヘルスチェックが無効になっている場合、このメトリクスは使用できません。

   正常な子ヘルスチェックの数

   計算されたヘルスチェックについてのみ、グラフに正常である子ヘルスチェックの数が表示されます。
5. より大きなグラフを表示して異なる設定を指定するには、右上にある 3 つのドットを選択した後、[拡大] を選択します。以下の設定を指定することができます。

   Statistic

   CloudWatch がデータに対して実行する計算内容を変更します。

   時間範囲

   夜間、過去 1 週間など、期間ごとのヘルスチェックのステータスを表示します。

   Period

   グラフのデータポイントの間隔を変更します。

次の点に注意してください。

- ヘルスチェックを作成した直後は、グラフにデータが表示されたり、利用可能なメトリクスのリストにヘルスチェックのメトリクスが表示されたりするまでに数分かかる場合があります。
- グラフは自動的には更新されません。表示を更新するには、更新 () アイコンを選択します。

Old console

ヘルスチェックのステータスを表示するには (新しいコンソール)

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [Health Checks (ヘルスチェック)] を選択します。
3. 目的のヘルスチェックの行を選択します。
4. 下部のペインで、[Monitoring] タブを選択します。

   2 つのグラフに、1 分間隔で過去 1 時間のステータスが表示されます。i

   ヘルスチェックステータス

   グラフには、エンドポイントの正常性に対する Route 53 の診断結果が (1は正常、0は異常として) 表示されます

   エンドポイントが正常であるとレポートするヘルスチェッカー (パーセント)

   エンドポイントのみをモニタリングするヘルスチェックについて、グラフには、選択されたエンドポイントを正常であると見なしている Route 53 ヘルスチェッカーの割合が示されます。

   ヘルスチェックが無効になっている場合、このメトリクスは使用できません。

   正常な子ヘルスチェックの数

   計算されたヘルスチェックについてのみ、グラフに正常である子ヘルスチェックの数が表示されます。

> **Note**
>
> 複数のヘルスチェックを選択した場合、グラフには、各ヘルスチェックに対応する行が色分けして表示されます。

5. より大きなグラフを表示し、異なる設定を指定するには、グラフを選択します。以下の設定を指定することができます。

   Statistic

   CloudWatch がデータに対して実行する計算内容を変更します。

   時間範囲

   夜間、過去 1 週間など、期間ごとのヘルスチェックのステータスを表示します。

   Period

   グラフのデータポイントの間隔を変更します。

   次の点に注意してください。

   - ヘルスチェックを作成した直後は、グラフにデータが表示されたり、利用可能なメトリクスのリストにヘルスチェックのメトリクスが表示されたりするまでに数分かかる場合があります。
   - グラフは自動的には更新されません。表示を更新するには、更新 () アイコンを選択します。

ヘルスチェックアラームを表示する

> **Note**
>
> Route 53 のヘルスチェックコンソールを更新中です。旧コンソールは移行期間中も引き続きご使用いただけます。

お使いのコンソールのタブを選択します。

- 新しいコンソール
- 旧コンソール

New console

CloudWatch アラームのステータスを表示したり Amazon Route 53 のアラームを編集したりするには

1. Route 53 コンソールのナビゲーションペインで、[ヘルスチェック] を選択します。
2. アラームを表示するヘルスチェックのリンクされた ID を選択します。
3. 詳細ページのページ下部で、[アラーム] タブを選択します。

   [アラーム] リストには、選択したヘルスチェック用に作成したすべての Route 53 アラームが含まれます。

   [State] 列には、各アラームの最新のステータスが表示されます。

   OK

   Route 53 ヘルスチェックから、エンドポイントがアラームのしきい値を満たしていないと判断できるだけの統計が CloudWatch によって収集されました。

   データ不足

   エンドポイントがアラームのしきい値を満たしているかどうかを判断できるだけの統計が、まだ CloudWatch によって収集されていません。新しいアラームの初期状態はこれに該当します。また、CloudWatch メトリクスが使用できなくなった場合、あるいは関連付けられたアラームを削除せずにヘルスチェックを削除した場合は、アラームの状態が [INSUFFICIENT DATA] (データ不足) に変わります。

   アラーム

   Route 53 ヘルスチェックから CloudWatch によって、エンドポイントがアラームのしきい値を満たしていると判断でき、かつ指定された E メールアドレスに通知を送信できるだけの統計が収集されました。
4. CloudWatch コンソールでアラームを表示し、アラームに関するさらに詳しい情報 (アラームに対するアップデートの履歴、ステータスの変化など) を取得するには、アラームのリンクされた名前を選択します。CloudWatch コンソールでアラームを編集することもできます。

5. CloudWatch コンソールで新しい CloudWatch アラームを作成するには、[CloudWatch アラームを作成] を選択します。詳細については、「CloudWatch ユーザーガイド」の「推奨アラームを見つけて作成する」を参照してください。

Old console

CloudWatch アラームのステータスを表示したり Amazon Route 53 のアラームを編集したりするには

1. Route 53 コンソールのナビゲーションペインで、[Health Checks (ヘルスチェック)] を選択します。
2. ヘルスチェックの行を選択します。
3. 詳細ペイン ([x Health Checks Selected (x 個のヘルスチェックを選択)] の後) の右向きキャレット
( ) アイコンを選択します。

   CloudWatch アラームリストには、現在の AWS アカウントを使用して作成したすべての Route 53 アラームが含まれます。

   [State] 列には、各アラームの最新のステータスが表示されます。

   OK

   Route 53 ヘルスチェックから、エンドポイントがアラームのしきい値を満たしていないと判断できるだけの統計が CloudWatch によって収集されました。

   データ不足

   エンドポイントがアラームのしきい値を満たしているかどうかを判断できるだけの統計が、まだ CloudWatch によって収集されていません。新しいアラームの初期状態はこれに該当します。また、CloudWatch メトリクスが使用できなくなった場合、あるいは関連付けられたアラームを削除せずにヘルスチェックを削除した場合は、アラームの状態が [INSUFFICIENT DATA] (データ不足) に変わります。

   アラーム

   Route 53 ヘルスチェックから CloudWatch によって、エンドポイントがアラームのしきい値を満たしていると判断でき、かつ指定された E メールアドレスに通知を送信できるだけの統計が収集されました。

4. アラームの設定を表示したり編集したりするには、目的のアラームの名前を選択します。
5. CloudWatch コンソールでアラームを表示し、アラームに関するさらに詳しい情報 (アラームに対するアップデートの履歴、ステータスの変化など) を取得するには、アラームの [More Options (その他のオプション)] 列の [View (表示)] を選択します。
6. 他の AWS サービスのアラームなど、現在の AWS アカウントを使用して作成したすべての CloudWatch アラームを表示するには、すべての CloudWatch アラームを表示するを選択します。
7. 現在の AWS アカウントで現在使用されていないメトリクスなど、使用可能なすべての CloudWatch メトリクスを表示するには、すべての CloudWatch メトリクスを表示を選択します。

CloudWatch コンソールでヘルスチェックメトリクスを表示する

CloudWatch コンソールで Route 53 メトリクスを表示するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/cloudwatch/ で CloudWatch コンソールを開きます。
2. 現在のリージョンを米国東部 (バージニア北部) に変更します。それ以外のリージョンを現在のリージョンとして選択した場合、Route 53 のメトリクスは利用できません。
3. ナビゲーションペインで [Metrics (メトリクス)] を選択してください。
4. [All metrics] タブで、[Route 53] を選択します。
5. [Health Check Metrics] を選択します。
6. CloudWatch コンソールで SNS 通知を設定することもできます。詳細については、「CloudWatch ユーザーガイド」の「推奨アラームを作成」を参照してください。

SNS 通知を使用してアラームを作成する

> **Note**
>
> 以下の手順は、古いコンソールにのみ適用されます。新しいコンソールから CloudWatch コンソールに進み、アラームを作成します。詳細については、「CloudWatch ユーザーガイド」の「推奨アラームを見つけて作成する」を参照してください。

ヘルスチェックのステータスに不具合がある場合に Amazon SNS 通知を受け取るには (古いコンソール)

1. Route 53 コンソールのナビゲーションペインで、[Health Checks (ヘルスチェック)] を選択します。
2. 該当するヘルスチェックの行を選択します。
3. 下部のペインで、[Alarms] タブを選択します。

   テーブルには、このヘルスチェック用に作成したアラームが表示されます。
4. [Create Alarm] (アラームの作成) を選択します。
5. 次の値を指定します。

   アラーム名

   [Alarms (アラーム)] タブの [Name (名前)] 列に、Route 53 が表示する名前を入力します。

   Alarm Description

   (オプション) アラームの説明を入力します。この値は、CloudWatch コンソールに表示されます。

   Send Notification

   このヘルスチェックのステータスがアラームをトリガーした場合に、Route 53 から通知を送信するかどうかを選択します。

   Notification Target ([Send notification] が [Yes] の場合のみ)

   既存の SNS トピックに CloudWatch から通知を送信する場合は、リストからトピックを選択します。

   既存の SNS トピック以外に CloudWatch から通知を送信する場合は、次のいずれかを実行します。

   - CloudWatch からメール通知を送信する場合 – [New SNS topic] (新しい SNS トピック) を選択し、この手順を続行します。
   - 他の手段で CloudWatch から通知を送信する場合 – 新しいブラウザタブを開いて Amazon SNS コンソールに移動し、新しいトピックを作成します。その後 Route 53 コンソールに戻り、[Notification target (通知ターゲット)] のリストから新しいトピックの名前を選択し、この手順を続行します。

トピック名 (新しい Amazon SNS トピックを作成する場合のみ)

新しい Amazon SNS トピックの名前を入力します。

受信者の E メールアドレス (新しい Amazon SNS トピックを作成する場合のみ)

ヘルスチェックがアラームをトリガーした場合に、Route 53 から SNS 通知を送信する宛先の E メールアドレスを入力します。

Alarm Target

このヘルスチェックについて Route 53 に評価させる値を次から選択します。

- [Health check status (ヘルスチェックのステータス)] – Route 53 ヘルスチェッカーは、ヘルスチェック結果が正常か異常かをレポートします
- [Health checkers that report the endpoint healthy (%) (エンドポイントが正常であるとレポートするヘルスチェッカー)] (エンドポイントのみをモニタリングするヘルスチェック) – ヘルスチェックのステータスが正常であるとレポートする Route 53 ヘルスチェッカーの割合
- [Number of healthy child health checks] (正常な子ヘルスチェックの数) (計算されたヘルスチェックのみ) – ヘルスチェックのステータスが正常であることを報告する、計算されたヘルスチェックの子ヘルスチェックの数
- [TCP connection time (TCP 接続時間) (HTTP および TCP ヘルスチェックのみ)] – Route 53 ヘルスチェッカーがエンドポイントとの TCP 接続を確立するのにかかった時間 (ミリ秒)
- [Time to complete SSL handshake (SSL ハンドシェイクが完了する時間) (HTTPS ヘルスチェックのみ)] – Route 53 ヘルスチェッカーが SSL/TLS ハンドシェイクを完了するのにかかった時間 (ミリ秒)
- [Time to first byte (先頭バイトまでの時間) (HTTP および HTTPS ヘルスチェックのみ)] – Route 53 ヘルスチェッカーが HTTP および HTTPS リクエストの応答の先頭バイトを受信するのにかかった時間 (ミリ秒)

Alarm Target

レイテンシー (TCP 接続時間、SSL ハンドシェイクが完了する時間、先頭バイトまでの時間) に基づくアラームターゲットでは、CloudWatch がレイテンシーを計算する対象を、特定のリージョンの Route 53 ヘルスチェッカーにするか、すべてのリージョンのヘルスチェッカーにするかを選択します (グローバル)。

リージョンを選択した場合、Route 53 はレイテンシーを 1 分あたり 2 回のみ測定し、サンプル数はすべてのリージョンを選択した場合よりも小さくなることに注意してください。結果的に、極端な値になっている可能性があります。誤ったアラーム通知を防ぐには、CloudWatch が通知を送信する前にヘルスチェックの失敗を検知できるように、より多くの期間が連続する設定にすることをお勧めします。

Fulfill Condition

次の設定を使用して、CloudWatch によってアラームがトリガーされるタイミングを指定します。

Alarm Target	推奨状態	説明
ヘルスチェックステータス	最小 < 1	Route 53 ヘルスチェッカーは、いつエンドポイントに不具合が生じたかをレポートします。
エンドポイントが正常であるとレポートするヘルスチェッカー (パーセント)	平均 < 必要なパーセント	エンドポイントのみをモニタリングするヘルスチェック – ヘルスチェッカーの 18% 未満が、ステータスが正常であるとレポートしている場合には、Route 53 はヘルスチェックのステータスを異常と見なします。このメトリクスでは、[Sample Count (サンプル数)] を選択しないでください。Route 53 がさらに多くのヘルスチェックリージョンを追加する際に、サンプル数の範囲が変わる可能性があるためです。[平均] は、ヘルスチェックのステータスをレポートしているチェッカーの割合を常に正確に表します。
正常な子ヘルスチェックの数	最小 < 必要な正常な子ヘルスチェック数	最小の統計は、控えめな値を返し、最悪なシナリオ値を表します。

Alarm Target	推奨状態	説明
TCP 接続時間	平均 > 必要な時間 (ミリ秒)	平均は、他の統計よりも一貫性のある値です。
SSL ハンドシェイクが完了する時間	平均 > 必要な時間 (ミリ秒)	平均は、他の統計よりも一貫性のある値です。
先頭バイトまでの時間	平均 > 必要な時間 (ミリ秒)	平均は、他の統計よりも一貫性のある値です。

少なくとも ***x*** 回連続する ***y*** 分/時間/日の期間

指定した値が基準を満たした状態の期間が、連続して何回続いた場合に Route 53 から通知を送信するかを指定します。次に、期間の長さを指定します。

6. [Create] (作成) を選択した場合、新しい SNS トピックに関する情報を記載した E メールが Amazon SNS から送信されます。
7. E メールに記載されている [Confirm subscription] を選択します。ユーザーが CloudWatch 通知の受信を開始するには、サブスクリプションを完了する必要があります。

DNS ファイアウォールを使用してアウトバウンド DNS トラフィックをフィルタリングする

Resolver DNS Firewall を使用すると、仮想プライベートクラウド (VPC) のアウトバウンド DNS トラフィックをフィルタリングおよび規制できます。これを行うには、DNS Firewall のルールグループで再利用可能なフィルタリングルールのコレクションを作成し、そのルールグループを VPC に関連付けて、DNS Firewall のログとメトリクスのアクティビティを監視します。アクティビティに基づいて、DNS Firewall の動作を適宜調整できます。

DNS Firewall では、VPC からのアウトバウンド DNS リクエストを保護できます。これらのリクエストは、ドメイン名解決のために VPC Resolver を介してルーティングされます。DNS Firewall による保護の主な用途は、データの DNS 漏洩を防ぐことです。DNS 漏洩は、不正なアクターが VPC 内のアプリケーションインスタンスに侵入し、DNS ルックアップを使用して、VPC のデータを彼らが管理するドメインに送信する際に発生します。DNS Firewall を使用すると、アプリケーションでクエリできるドメインを監視および管理できます。不正であるとわかっているドメインへのアクセスを拒否し、他のすべてのクエリを許可できます。また、確実に信頼できるドメインを除くすべてのドメインへのアクセスを拒否することもできます。

DNS ファイアウォールは、VPC エンドポイント名など、プライベートのホストゾーン (共有またはローカル) 内のリソースに対する解決リクエストをブロックする場合にも使用できます。また、パブリックまたはプライベートの Amazon EC2 インスタンス名のリクエストをブロックすることもできます。

DNS Firewall は Route 53 VPC Resolver の機能であり、使用する追加の VPC Resolver のセットアップは必要ありません。

AWS Firewall Manager が DNS Firewall をサポート

Firewall Manager を使用すると、 AWS Organizationsのアカウント全体で VPC 向けの DNS Firewall ルールグループの関連付けを一元的に設定および管理できます。Firewall Manager では、Firewall Manager DNS Firewall ポリシーの対象となる VPC の関連付けが自動的に追加されます。詳細については、、、および デベロッパーガイドAWS Firewall Managerの「」を参照してください。 AWS WAF AWS Firewall Manager AWS Shield Advanced

DNS Firewall と の連携方法 AWS Network Firewall

DNS Firewall とNetwork Firewall は、どちらもドメイン名のフィルタリングを行いますが、トラフィックの種類は異なります。DNS Firewall とNetwork Firewall を組み合わせることで、2 つの異な

るネットワークパス上のアプリケーション層トラフィックに対してドメインベースのフィルタリングを設定できます。

- DNS Firewall は、VPC 内のアプリケーションから Route 53 VPC Resolver を通過するアウトバウンド DNS VPCs クエリのフィルタリングを提供します。また、ブロックしたドメイン名にクエリのカスタムレスポンスを送信するように DNS Firewall を設定できます。
- Network Firewall は、ネットワークレイヤートラフィックとアプリケーションレイヤートラフィックの両方をフィルタリングしますが、Route 53 VPC Resolver によって行われたクエリは可視化されません。

Network Firewall の詳細については、Network Firewall デベロッパーガイドを参照してください。

Resolver DNS Firewall の仕組み

Resolver DNS Firewall を使用すると、サイトへのアクセスを制御し、Route 53 VPC Resolver を介して VPC から送信される DNS クエリの DNS レベルの脅威をブロックできます。DNS Firewall では、VPC に関連付けるルールグループにドメイン名のフィルタリングルールを定義します。許可またはブロックするドメイン名のリスト、または DNS トンネリングとドメイン生成アルゴリズム (DGA) ベースの脅威から保護する Resolver DNS Firewall Advanced ルールを指定できます。ブロックする DNS クエリのレスポンスをカスタマイズできます。ドメインリストを含むルールの場合、ドメインリストをファインチューニングして、MX レコードなどの特定のクエリタイプを許可することもできます。

DNS Firewall は、ドメイン名のみをフィルタリングします。このドメイン名から、ブロックされる IP アドレスを調べることはできません。また、DNS ファイアウォールでは DNS トラフィックをフィルタリングできますが、HTTPS、SSH、TLS、FTP などの他のアプリケーションレイヤープロトコルはフィルタリングできません。

Resolver DNS Firewall のコンポーネントと設定

DNS Firewall は、次の中央にあるコンポーネントと設定で管理します。

DNS Firewall ルールグループ

DNS クエリをフィルタリングするために DNS Firewall ルールの再利用可能な名前付きコレクションを定義します。ルールグループにフィルタリングルールを設定し、ルールグループを 1 つ以上の VPC に関連付けます。ルールグループを VPC に関連付けると、VPC の DNS Firewall フィルタリングが有効になります。次に、VPC Resolver がルールグループが関連付けられてい

る VPC の DNS クエリを受信すると、VPC Resolver はフィルタリングのためにクエリを DNS Firewall に渡します。

複数のルールグループを 1 つの VPC に関連付ける場合は、各関連付けの優先度設定で処理する順序を指定します。DNS Firewall は、優先度が最も低い設定から VPC のルールグループを処理します。

詳細については、「DNS Firewall のルールグループとルール」を参照してください。

DNS Firewall ルール

DNS Firewall ルールグループ内の DNS クエリに対するフィルタリングルールを定義します。各ルールでは、それぞれドメインリスト、または DNS Firewall 保護を 1 つ指定します。また、ルール内のドメイン仕様に一致するドメインを持つ DNS クエリに対して実行するアクションを指定します。一致するクエリを許可 (ドメインリストのみを含むルール) 、ブロック、またはアラートできます。ドメインリストを持つルールでは、リスト内のドメインにクエリタイプを指定することもできます。例えば、特定のドメインの MX クエリタイプをブロックまたは許可できます。ブロックしたクエリのカスタムレスポンスも定義できます。

DNS Firewall ルールでは、一致するクエリに対してのみブロックまたはアラートを実行できます。

ルールグループの各ルールには、ルールグループ内で一意の優先度設定があります。DNS Firewall は、優先度が最も低い設定からルールグループ内のルールを処理します。

DNS Firewall ルールは、定義されているルールグループのコンテキストにのみ存在します。ルールを再利用したり、ルールグループから独立したルールを参照することはできません。

詳細については、「DNS Firewall のルールグループとルール」を参照してください

ドメインリスト

DNS フィルタリングで使用するドメイン仕様の再利用可能な名前付きコレクションを定義します。ルールグループの各ルールには、それぞれに 1 つのドメインリストが必要です。アクセスを許可するドメイン、アクセスを拒否するドメイン、またはその両方の組み合わせを指定できます。独自のドメインリストを作成し、 が AWS 管理するドメインリストを使用できます。

詳細については、「DNS ファイアウォールの基本ルール」を参照してください。

ドメインリダイレクト設定 (ドメインリストのみ)

ドメインリダイレクト設定を使用すると、DNS ファイアウォールルールを設定して、CNAME、DNAME など、DNS リダイレクトチェーン内のすべてのドメイン (デフォルト) ま

たは最初のドメインだけを検査して残りを信頼することができます。DNS リダイレクトチェーン全体を検査する場合は、ルールで ALLOW に設定されたドメインリストに後続のドメインを追加する必要があります。DNS リダイレクトチェーン全体を検査する場合は、後続のドメインをドメインリストに追加し、ルールが実行するアクション (ALLOW、BLOCK、ALERT のいずれか) に設定する必要があります。

> **Important**
>
> ドメインリダイレクト設定の信頼動作は、単一の DNS クエリトランザクション内にのみ適用されます。ホストの DNS クライアントが DNS リダイレクトチェーンに表示されるドメインに個別にクエリを実行する場合 (リダイレクトターゲットを直接クエリするなど)、DNS Firewall はそれを元のクエリからの信頼コンテキストのない独立したクエリとして評価します。このようなクエリを許可するには、リダイレクトターゲットドメインをドメインリストに追加します。

詳細については、「DNS Firewall のルール設定」を参照してください。

クエリタイプ (ドメインリストのみ)

クエリタイプ設定では、特定の DNS クエリタイプをフィルタリングするように DNS ファイアウォールルールを設定できます。クエリタイプを選択しない場合、ルールはすべての DNS クエリタイプに適用されます。例えば、特定のドメインのすべてのクエリタイプをブロックし、MX レコードを許可します。

詳細については、「DNS Firewall のルール設定」を参照してください。

DNS Firewall Advanced 保護

DNS クエリの既知の脅威署名に基づいて、疑わしい DNS クエリを検出します。ルールグループ内の各ルールには、単一の DNS Firewall Advanced 保護設定が必要です。保護は、以下から選択できます。

- ドメイン生成アルゴリズム (DGAs)

  DGAs は、攻撃者が多数のドメインを生成してマルウェア攻撃を開始するために使用されます。

- DNS トンネリング

  DNS トンネリングは、攻撃者がクライアントへのネットワーク接続を行わずに DNS トンネルを使用してクライアントからデータを抽出するために使用されます。

- ディクショナリ DGA

  ディクショナリ DGAs は、攻撃者がディクショナリ単語を使用してドメインを生成し、マルウェアcommand-and-control通信での検出を回避するために使用されます。

DNS Firewall Advanced ルールでは、脅威に一致するクエリをブロックするか、アラートするかを選択できます。脅威保護アルゴリズムは によって管理および更新されます AWS。

詳細については、「DNS ファイアウォールの詳細ルール」を参照してください。

信頼度しきい値 (DNS Firewall Advanced 保護のみ)

DNS 脅威保護の信頼度しきい値。DNS Firewall Advanced のルールを作成するときに、この値を指定する必要があります。信頼度の値は次のことを意味します。

- 高 – 誤検出率が低く、最も裏付けのある脅威のみを検出します。
- 中 – 脅威の検出と誤検出のバランスが取れています。
- 低 – 脅威の検出率が最も高いが、誤検出も増加します。

詳細については、「DNS Firewall のルール設定」を参照してください。

DNS Firewall ルールグループと VPC 間の関連付け

DNS Firewall ルールグループを使用して VPC の保護を定義し、VPC の VPC Resolver DNS Firewall 設定を有効にします。

複数のルールグループを 1 つの VPC に関連付ける場合は、関連付けの優先度設定で、それらを処理する順序を指定します。DNS Firewall は、優先度が最も低い設定から VPC のルールグループを処理します。

詳細については、「VPC のリゾルバー DNS ファイアウォール保護の有効化」を参照してください。

VPC の DNS ファイアウォール設定

VPC Resolver が VPC レベルで DNS Firewall 保護を処理する方法を指定します。この設定は、VPC に関連付けられた DNS Firewall ルールグループが少なくとも 1 つある場合に有効です。

この設定では、DNS Firewall がクエリのフィルタリングに失敗したときに Route 53 VPC Resolver がクエリを処理する方法を指定します。デフォルトでは、VPC Resolver がクエリの DNS Firewall からレスポンスを受信しない場合、閉じられてクエリがブロックされます。

詳細については、「DNS Firewall での VPC の設定」を参照してください。

DNS ファイアウォールアクションのモニタリング

Amazon CloudWatch を使用して、DNS ファイアウォールのルールグループでフィルタリングされた、DNS クエリ数をモニタリングできます。CloudWatch では、生データを収集し、ほぼリアルタイムの読み取り可能なメトリクスに加工します。

詳細については、「Amazon CloudWatch を使用した Resolver DNS Firewall ルールグループのモニタリング」を参照してください。

Amazon EventBridge は、イベントを使用してアプリケーションコンポーネント同士を接続するサーバーレスサービスです。これにより、スケーラブルなイベント駆動型アプリケーションを構築できます。

詳細については、「を使用したリゾルバー DNS ファイアウォールイベントの管理 Amazon EventBridge」を参照してください。

Resolver DNS Firewall が DNS クエリをフィルタリングする方法

DNS Firewall ルールグループが VPC の Route 53 VPC Resolver に関連付けられている場合、次のトラフィックはファイアウォールによってフィルタリングされます。

- その VPC 内で発信され、VPC DNS を通過する DNS クエリ。
- オンプレミスのリソースから、リゾルバーエンドポイントを通過して、リゾルバーに関連付けられた DNS ファイアウォールを持つ同じ VPC に渡される DNS クエリ。

DNS Firewall は、DNS クエリを受信すると、設定したルールグループ、ルール、およびその他の設定を使用してクエリをフィルタリングし、結果を VPC Resolver に送信します。

- DNS Firewall は、一致するものが見つかるまで、またはすべてのルールグループを使い果たすまで、VPC に関連付けられたルールグループを使用して DNS クエリの評価を行います。DNS Firewall は、関連付けで設定した優先度の順に、優先順位が最も低い設定からルールグループを評価します。詳細については、「DNS Firewall のルールグループとルール」および「VPC のリゾルバー DNS ファイアウォール保護の有効化」を参照してください。
- 各ルールグループ内で DNS Firewall は、一致するものが見つかるまで、またはすべてのルールを使い果たすまで、各ルールのドメインリストまたは DNS Firewall Advanced 保護に対する DNS クエリの評価を行います。DNS Firewall は、優先順位の順に、優先度が最も低い設定からルールを評価します。詳細については、「DNS Firewall のルールグループとルール」を参照してください。

- DNS Firewall は、ルールのドメインリスト、または DNS Firewall Advanced ルール保護によって識別された異常との一致を検出すると、クエリ評価を終了し、結果とともに VPC Resolver に応答します。アクションが の場合`alert`、DNS Firewall は設定された VPC Resolver ログにもアラートを送信します。詳細については、DNS Firewall でのルールアクション、DNS ファイアウォールの基本ルール、および DNS ファイアウォールの詳細ルール を参照してください。
- DNS Firewall が一致するものを見つけられずにすべてのルールグループを評価し終えた場合、通常どおりクエリに対して応答します。

VPC Resolver は、DNS Firewall からのレスポンスに従ってクエリをルーティングします。万一 DNS ファイアウォールが応答しない場合、VPC リゾルバーは VPC で設定された DNS ファイアウォールのフェイルモードを適用します。詳細については、「DNS Firewall での VPC の設定」を参照してください。

Resolver DNS Firewall を使用するための大まかな手順

Amazon Virtual Private Cloud VPC に Resolver DNS Firewall フィルタリングを実装するには、以下の大まかなステップを実行します。

- フィルタリングのアプローチ、ドメインリスト、DNS Firewall 保護を定義する — クエリをフィルタリングする方法を決定し、必要なドメイン仕様を特定して、クエリの評価に使用するロジックを定義します。例えば、既知の不正なドメインのリストにあるクエリを除くすべてのクエリを許可できます。または反対に、承認したリストのドメインを除くすべてのドメインをブロックすることもできます。これは、ウォールドガーデンアプローチとして知られています。承認済みまたはブロックされたドメイン仕様の独自のリストを作成および管理し、 が AWS 管理するドメインリストを使用できます。DNS Firewall 保護の場合、クエリをすべてブロックしてフィルタリングするか、脅威 (DGA、DNS トンネリング、ディクショナリ DGA) に関連する異常を含む可能性のあるドメインへの疑わしいクエリトラフィックをアラートして、DNS Firewall 設定をテストできます。詳細については、「DNS ファイアウォールの基本ルール」および「DNS ファイアウォールの詳細ルール」を参照してください。
- ファイアウォールルールグループの作成 — DNS Firewall で、VPC 向けの DNS クエリをフィルタリングするルールグループを作成します。ルールグループは、使用するリージョンごとに作成する必要があります。また、異なる VPC の複数のフィルタリングシナリオで再利用できるように、フィルタリング動作を複数のルールグループに分けることもできます。ルールグループについては、「DNS Firewall のルールグループとルール」を参照してください。
- ルールの追加と設定 — ルールグループで提供するドメインリストおよびフィルタリング動作ごとに、ルールグループにルールを追加します。ルールグループ内でルールが正しい順序で処理される

ように、ルールの優先度を設定します。最初に評価するルールの優先順位が最も低くなるようにします。ルールについては、「DNS Firewall のルールグループとルール」を参照してください。

- ルールグループを VPC に関連付ける — DNS Firewall ルールグループの使用を開始するには、VPC に関連付けます。VPC で複数のルールグループを使用している場合は、ルールグループが正しい順序で処理されるように、各関連付けの優先度を設定します。最初に評価するルールグループの優先順位が最も低くなるようにします。詳細については、「VPC と Resolver DNS Firewall ルールグループ間の関連付けの管理」を参照してください。
- (オプション) VPC のファイアウォール設定を変更する – DNS Firewall が応答を返さないときに Route 53 VPC Resolver でクエリをブロックする場合は、VPC Resolver で VPC の DNS Firewall 設定を変更します。詳細については、「DNS Firewall での VPC の設定」を参照してください。

複数のリージョンでの Resolver DNS Firewall ルールグループの使用

Resolver DNS Firewall はリージョンサービスであるため、1 つの AWS リージョンで作成したオブジェクトは、そのリージョンでのみ使用できます。同じルールグループを複数のリージョンで使用するには、リージョンごとにルールグループを作成する必要があります。

ルールグループを作成した AWS アカウントは、他の AWS アカウントと共有できます。詳細については、「Resolver DNS Firewall ルールグループを AWS アカウント間で共有する」を参照してください。

Resolver DNS Firewall のリージョンの可用性

DNS ファイアウォールは、以下で使用できます AWS リージョン。

- アフリカ (ケープタウン)
- アジアパシフィック (香港)
- アジアパシフィック (ハイデラバード)
- アジアパシフィック (ジャカルタ)
- アジアパシフィック (マレーシア)
- アジアパシフィック (メルボルン)
- アジアパシフィック (ムンバイ)
- アジアパシフィック (大阪) リージョン
- アジアパシフィック (ソウル)
- アジアパシフィック (シンガポール)

- アジアパシフィック (シドニー)
- アジアパシフィック (タイ)
- アジアパシフィック (東京)
- カナダ (中部) リージョン
- カナダ西部 (カルガリー)
- 欧州 (フランクフルト) リージョン
- 欧州 (アイルランド) リージョン
- 欧州 (ロンドン) リージョン
- 欧州 (ミラノ)
- 欧州 (パリ) リージョン
- 欧州 (スペイン)
- 欧州 (ストックホルム)
- 欧州 (チューリッヒ)
- イスラエル (テルアビブ)
- メキシコ (中部)
- 中東 (バーレーン)
- 中東 (アラブ首長国連邦)
- 南米 (サンパウロ)
- 米国東部 (バージニア北部)
- 米国東部 (オハイオ)
- 米国西部 (北カリフォルニア)
- 米国西部 (オレゴン)
- 中国 (北京)
- 中国 (寧夏)
- AWS GovCloud (US)

Resolver DNS Firewall の開始方法

DNS Firewall コンソールには、DNS Firewall の開始方法を次の手順で説明するウィザードが含まれています。

- 使用するルールセットごとにルールグループを作成します。

- ルールごとに、調査するドメインリストを設定します。独自のドメインリストを作成し、 AWS マネージドドメインリストを使用できます。
- 使用する VPC にルールグループを関連付けます。

Resolver DNS Firewall ウォールドガーデンの例

このチュートリアルでは、信頼できるドメインのうち選択されたグループを除くすべてのドメインをブロックするルールグループを作成します。これは、クローズドプラットフォーム、またはウォールドガーデンアプローチと呼ばれます。

コンソールウィザードを使用して DNS Firewall ルールグループを設定するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。

   ナビゲーションペインで、[DNS ファイアウォール] を選択し、Amazon VPC コンソールの [ルールグループ] ページで DNS ファイアウォールを開きます。ステップ 3 に進みます。

   - または -

   にサインイン AWS マネジメントコンソール して を開きます。

   https://console.aws.amazon.com/vpc/ から、Amazon VPC コンソールを開きます。
2. ナビゲーションペインで、[DNS ファイアウォール] の下にある [ルールグループ] を選択します。
3. ナビゲーションバーで、ルールグループのリージョンを選択します。
4. [ルールグループ] ページで、[ルールグループの追加] を選択します。
5. ルールグループ名に「**`WalledGardenExample`**」と入力します。

   [タグ] セクションで、タグのキーと値のペアをオプションで入力できます。タグは、 AWS リソースの整理と管理に役立ちます。詳細については、「Amazon Route 53 リソースのタグ付け」を参照してください。
6. [ルールグループを追加] を選択します。
7. WalledGardenExample の詳細ページで、[ルール] タブ、[ルールを追加] の順に選択します。
8. [ルールの詳細] ペインで、ルール名に「 **`BlockAll`**」と入力します。
9. [Domain list (ドメインリスト)] ペインで、[Add my own domain list (独自のドメインリストを追加)] を選択します。

10. [Choose or create a new domain list (新しいドメインリストを選択または作成)] で [Create new domain list (新しいドメインリストの作成)] を選択します。
11. ドメインリスト名 を入力し**AllDomains**、Enter one domain per line テキストボックスにアスタリスク を入力します*****。
12. [ドメインリダイレクト設定] では、デフォルトを受け入れ、[クエリの種類-オプション] は空のままにします。
13. [アクション] については、[BLOCK] を選択し、送信するレスポンスをデフォルト設定の [NODATA] のままにしておきます。
14. [ルールを追加] を選択してください。ルール BlockAll は、WalledGardenExample ページのルールタブに表示されます。
15. [WalledGardenExample] ページで、[ルールを追加] を選択して、ルールグループに 2 番目のルールを追加します。
16. [ルールの詳細] ペインで、ルール名に「 **AllowSelectDomains**」と入力します。
17. [Domain list (ドメインリスト)] ペインで、[Add my own domain list (独自のドメインリストを追加)] を選択します。
18. [Choose or create a new domain list (新しいドメインリストの選択または作成)]で、[Create new domain list (新しいドメインリストの作成)]を選択します。
19. ドメインリスト名に「**ExampleDomains**」と入力します。
20. [1 行につき 1 つのドメインを入力] テキストボックスの最初の行に「**example.com**」、2 行目に「**example.org**」と入力します。

    > **Note**
    >
    > ルールをサブドメインにも適用する場合は、それらのドメインもリストに追加する必要があります。例えば、example.com のすべてのサブドメインを追加するには、***.example.com** をリストに追加します。

21. [ドメインリダイレクト設定] では、デフォルトを受け入れ、[クエリの種類-オプション] は空のままにします。
22. [アクション] については、[ALLOW] を選択します。
23. [ルールを追加] を選択してください。ルールは両方とも、WalledGardenExample ページのルールタブに表示されます。
24. [WalledGardenExample] ページの [ルール] タブで、[優先度] 列にリストされている番号を選択し、新しい番号を入力して、ルールグループ内のルールの評価順序を調整できます。DNS ファ

イアウォールは、最も優先度が低い設定から順にルールを評価するため、最も優先度が低いルールが最初に評価されます。この例では、最初に DNS Firewall でドメインの選択リストの DNS クエリを特定して許可し、残りのクエリをすべてブロックします。

[AllowSelectDomains] の優先度が低くなるようにルールの優先度を調整します。

これで、特定のドメインクエリのみを許可するルールグループができました。使用を開始するには、フィルタリング動作を使用する VPC にルールグループを関連付けます。詳細については、「VPC と Resolver DNS Firewall ルールグループ間の関連付けの管理」を参照してください。

Resolver DNS Firewall ブロックリストの例

このチュートリアルでは、悪意のあるドメインであることがわかっているドメインをブロックするルールグループを作成します。ブロックされたリストのドメインに許可される DNS クエリタイプも追加します。ルールグループは、VPC リゾルバーを介した他のすべてのアウトバウンド DNS リクエストを許可します。

コンソールウィザードを使用して DNS ファイアウォールブロックリストを設定するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。

   ナビゲーションペインで、[DNS ファイアウォール] を選択し、Amazon VPC コンソールの [ルールグループ] ページで DNS ファイアウォールを開きます。ステップ 3 に進みます。

   - または -

   にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/vpc/ で Amazon VPC コンソールを開きます。
2. ナビゲーションペインで、[DNS ファイアウォール] の下にある [ルールグループ] を選択します。
3. ナビゲーションバーで、ルールグループのリージョンを選択します。
4. [ルールグループ] ページで、[ルールグループの追加] を選択します。
5. ルールグループ名に「**`BlockListExample`**」と入力します。

   [タグ] セクションで、タグのキーと値のペアをオプションで入力できます。タグは、 AWS リソースの整理と管理に役立ちます。詳細については、「Amazon Route 53 リソースのタグ付け」を参照してください。

6. BlockListExample の詳細ページで、ルールタブを選択し、ルールを追加します。
7. [ルールの詳細] ペインで、ルール名に「 **`BlockList`**」と入力します。
8. [Domain list (ドメインリスト)] ペインで、[Add my own domain list (独自のドメインリストを追加)] を選択します。
9. [Choose or create a new domain list (新しいドメインリストの選択または作成)]で、[Create new domain list (新しいドメインリストの作成)] を選択します。
10. ドメインリスト名 **`MaliciousDomains`** を入力し、次にテキストボックスにブロックするドメインを入力します。例えば、 **`example.org`**。1 行に 1 つドメインを入力します。

    > **Note**
    >
    > ルールをサブドメインにも適用する場合は、それらのドメインもリストに追加する必要があります。例えば、example.org のすべてのサブドメインを追加するには、**`*.example.org`** をリストに追加します。

11. [ドメインリダイレクト設定] では、デフォルトを受け入れ、[クエリの種類-オプション] は空のままにします。
12. アクションについては、BLOCK を選択し、送信するレスポンスをデフォルト設定の NODATA のままにしておきます。
13. [ルールを追加] を選択してください。ルールが BlockListExample ページのルールタブに表示されます。
14. [BlockedListExample] ページの [ルール] タブで、[優先度] 列にリストされている番号を選択し、新しい番号を入力して、ルールグループ内のルールの評価順序を調整できます。DNS ファイアウォールは、最も優先度が低い設定から順にルールを評価するため、最も優先度が低いルールが最初に評価されます。

    ルールの優先度を選択して、[ブロックリスト] の他のルールの前または後に評価されるようルールの優先度を調整します。ほとんどの場合、既知の悪意のあるドメインを最初にブロックしてください。つまり、これらに関連付けられているルールは、最も小さい優先順位番号にする必要があります。
15. BlockList ドメインの MX レコードを許可するルールを追加するには、ルールタブの BlockedListExample の詳細ページで、ルールの追加を選択します。
16. [ルールの詳細] ペインで、ルール名に「 **`BlockList-allowMX`**」と入力します。
17. [Domain list (ドメインリスト)] ペインで、[Add my own domain list (独自のドメインリストを追加)] を選択します。

18. [新しいドメインリストを選択または作成] で、[**MaliciousDomains**] を選択します。
19. [ドメインリダイレクト設定] では、デフォルトを受け入れます。
20. [DNS クエリタイプ] リストで、[MX: メールサーバーを指定する] を選択します。
21. アクションについては、[ALLOW] を選択します。
22. [ルールを追加] を選択してください。
23. [BlockedListExample] ページの [ルール] タブで、[優先度] 列にリストされている番号を選択し、新しい番号を入力して、ルールグループ内のルールの評価順序を調整できます。DNS ファイアウォールは、最も優先度が低い設定から順にルールを評価するため、最も優先度が低いルールが最初に評価されます。

    ルールの優先度を選択して、[BlockList-allowMX] は、他のルールの前または後に評価されるようルールの優先度を調整します。MX クエリを許可するため、[BlockList -allowMX] ルールが [ブラックリスト] よりも優先度が低いことを確認してください。

これで、特定の悪意のあるドメインクエリをブロックするルールグループができましたが、特定の DNS クエリタイプが許可されます。使用を開始するには、フィルタリング動作を使用する VPC にルールグループを関連付けます。詳細については、「VPC と Resolver DNS Firewall ルールグループ間の関連付けの管理」を参照してください。

DNS Firewall のルールグループとルール

このセクションでは、VPC 向けの DNS Firewall の動作を定義するために DNS Firewall のルールグループおよびルールに対して行える設定について説明します。また、ルールおよびルールグループを設定する方法についても説明します。

ルールグループを希望どおりに設定したら、それらをそのまま使用して、アカウント間や AWS Organizations内の組織全体で共有および管理することができます。

- ルールグループを複数の VPC に関連付けて、組織全体で一貫した動作を行えます。詳細については、「VPC と Resolver DNS Firewall ルールグループ間の関連付けの管理」を参照してください。
- アカウント間でルールグループを共有し、組織全体で一貫して DNS クエリを管理できます。詳細については、「Resolver DNS Firewall ルールグループを AWS アカウント間で共有する」を参照してください。
- AWS Firewall Manager ポリシーで管理 AWS Organizations することで、 で組織全体のルールグループを使用できます。Firewall Manager の詳細については、の「」、および デベロッパーガイ

ドAWS Firewall Managerの「」を参照してください。 AWS WAF AWS Firewall Manager AWS Shield Advanced

DNS Firewall のルールグループ設定

DNS Firewall ルールグループを作成または編集する場合、次の値を指定します。

名前

わかりやすい名前にすると、ダッシュボードでルールグループを見つけやすくなります。

(オプション) 説明

ルールグループのコンテキストについての簡単な説明。

リージョン

ルールグループの作成時に選択する AWS リージョン。1 つのリージョンで作成したルールグループは、そのリージョンでのみ使用できます。同じルールグループを複数のリージョンで使用するには、リージョンごとにルールグループを作成する必要があります。

ルール

ルールグループのフィルタリング動作は、そのルールに含まれています。詳細については、次のセクションを参照してください。

タグ

1 つ以上のキーと対応する値を指定します。例えば、[Key (キー)] に Cost center を、[Value (値)] には 456 を指定します。

これらは、 が請求書を整理するために AWS Billing and Cost Management 提供するタグです AWS 。タグを使ったコスト配分の詳細については、AWS Billing ユーザーガイドのコスト配分タグの使用を参照してください。

DNS Firewall のルール設定

DNS Firewall ルールグループを作成または編集する場合、次の値を指定します。

名前

ルールグループ内のルールの一意の識別子。

(オプション) 説明

ルールの詳細についての簡単な説明。

ドメインリスト

ルールが調査するドメインのリスト。独自のドメインリストを作成して管理したり、 AWS が管理するドメインリストをサブスクライブできます。詳細については、「DNS ファイアウォールの基本ルール」を参照してください。

ルールには、ドメインリストまたは DNS Firewall Advanced 保護を含めることができますが、両方を含めることはできません。

ドメインリダイレクト設定 (ドメインリストのみ)

DNS ファイアウォールルールでは、CNAME、DNAME など、DNS リダイレクトチェーン内の最初のドメインのみまたはすべて (デフォルト) のドメインのみを検査するように選択できます。すべてのドメインを検査することを選択した場合、DNS リダイレクトチェーン内の後続のドメインをドメインリストに追加し、ルールが実行するアクション (ALLOW、BLOCK、ALERT のいずれか) に設定する必要があります。詳細については、「Resolver DNS Firewall のコンポーネントと設定」を参照してください。

> **Important**
>
> ドメインリダイレクト設定の信頼動作は、単一の DNS クエリトランザクション内にのみ適用されます。ホストの DNS クライアントが DNS リダイレクトチェーンに表示されるドメインに個別にクエリを実行する場合 (リダイレクトターゲットを直接クエリするなど) 、DNS Firewall はそれを元のクエリからの信頼コンテキストのない独立したクエリとして評価します。このようなクエリを許可するには、リダイレクトターゲットドメインをドメインリストに追加します。

クエリタイプ (ドメインリストのみ)

ルールが検査する DNS クエリタイプのリスト。有効な値を次に示します。

- A: IPv4 アドレスを返します。
- AAAA: Ipv6 アドレスを返します。
- CAA: ドメインの SSL/TLS 証明書を作成できる CA を制限します。
- CNAME: 別のドメイン名を返します。
- DS: 委任ゾーンの DNSSEC 署名キーを識別するレコード。

- MX: メールサーバーを指定します。
- NAPTR: ドメイン名の正規表現ベースの書き換え。
- NS: 権威ネームサーバー。
- PTR: IP アドレスをドメイン名にマッピングします。
- SOA: ゾーンの管理情報の始点レコード。
- SPF: ドメインから E メールを送信する権限を持つサーバーを一覧表示します。
- SRV: サーバーを識別するアプリケーション固有の値。
- TXT: E メール送信者とアプリケーション固有の値を検証します。
- DNS タイプ ID を使用して定義するクエリタイプ (例えば、AAAA の場合は 28)。値は TYPE *NUMBER* として定義する必要があります。*NUMBER* は 1 ~ 65334 です。たとえば、TYPE28 です。詳細については、「DNS レコードタイプの一覧」を参照してください。

  ルールごとに 1 つのクエリタイプを作成できます。

  > **Note**
  >
  > クエリタイプが AAAA に等しいアクション NXDOMAIN でファイアウォールの BLOCK ルールを設定すると、DNS64 が有効になっているときに生成される合成 IPv6 アドレスにはこのアクションは適用されません。

DNS Firewall Advanced 保護

DNS クエリの既知の脅威署名に基づいて、疑わしい DNS クエリを検出します。保護は、以下から選択できます。

- ドメイン生成アルゴリズム (DGAs)

  DGAs は、攻撃者が多数のドメインを生成してマルウェア攻撃を開始するために使用されます。

- DNS トンネリング

  DNS トンネリングは、攻撃者がクライアントへのネットワーク接続を行わずに DNS トンネルを使用してクライアントからデータを抽出するために使用されます。

- ディクショナリ DGA

  ディクショナリ DGAs は、攻撃者がディクショナリ単語を使用してドメインを生成し、マルウェアcommand-and-control通信での検出を回避するために使用されます。

DNS Firewall Advanced ルールでは、脅威に一致するクエリをブロックするか、アラートするかを選択できます。

詳細については、DNS ファイアウォールの詳細ルール を参照してください。

ルールには、DNS Firewall Advanced 保護またはドメインリストを含めることができますが、両方を含めることはできません。

信頼度のしきい値 (DNS Firewall Advanced のみ)。

DNS Firewall Advanced の信頼度のしきい値。DNS Firewall Advanced のルールを作成するときに、この値を指定する必要があります。信頼度の値は次のことを意味します。

- 高 – 誤検出率が低く、最も裏付けのある脅威のみを検出します。
- 中 – 脅威の検出と誤検出のバランスが取れています。
- 低 – 脅威の検出率が最も高いが、誤検出も増加します。

詳細については、「DNS Firewall のルール設定」を参照してください。

アクション

DNS Firewall で、ルールのドメインリストの仕様と一致するドメイン名を持つ DNS クエリを処理する方法 詳細については、「DNS Firewall でのルールアクション」を参照してください

優先度

ルールグループ内のルールの一意の自然数の設定。これにより、処理順序が決定されます。DNS Firewall は、ルールグループのルールに対する DNS クエリを調査します。優先度が最も低い設定で始まり、上がっていきます。ルールの優先度はいつでも変更できます。例えば、処理の順序を変更したり、他のルールのためのスペースを確保できます。

DNS Firewall でのルールアクション

DNS Firewallでは、DNS クエリとルールのドメイン仕様の間で一致が検出されると、ルールで指定されたアクションがクエリに適用されます。

作成する各ルールで、次のオプションのいずれかを指定する必要があります：

- Allow – クエリの検査を停止し、実行を許可します。DNS Firewall Advanced では使用できません。
- Alert – クエリの検査を停止して通過を許可し、Route 53 VPC Resolver ログにクエリのアラートを記録します。

- Block – クエリの検査を中止し、目的の宛先へのクエリのブロックアクションを Route 53 VPC Resolver ログに記録します。

  次のように、設定されたブロックレスポンスで応答します。

  - NODATA – クエリが成功したが、応答がないことを示す応答。
  - NXDOMAIN – クエリのドメイン名が存在しないことを示す応答。
  - OVERRIDE – レスポンスにカスタムオーバーライドを指定します。このオプションには、次の設定が必要です。
    - Record value – クエリに応答して返送するカスタム DNS レコード。
    - Record type – DNS レコードのタイプ。これによりレコード値の形式が決定します。これは、CNAME である必要があります。
    - Time to live in seconds – DNS リゾルバーまたはウェブブラウザがオーバーライドレコードをキャッシュし、再度受信された場合にこのクエリへの応答に使用するのに推奨される時間。デフォルトではこの値はゼロであり、レコードはキャッシュされません。

クエリログの設定と内容の詳細については、「リゾルバーでのクエリの log 記録」および「VPC Resolver クエリログに表示される値」を参照してください。

Alert を使用してブロックルールをテストする

ブロックルールを初めて作成する際は、アクションを Alert に設定して、ブロックルールをテストします。次に、ルールが警告するクエリの数を調べて、アクションを Block に設定した場合にブロックされるクエリの数を確認します。

DNS Firewall でのルールグループおよびルールの管理

コンソールでルールグループとルールを管理するには、このセクションのガイダンスに従います。

ルールやドメインリストなどの DNS Firewall エンティティに変更を加えると、DNS Firewall はエンティティが格納および使用されるすべての場所に変更を伝播します。変更は数秒以内に適用されますが、変更がある場所に到着し、他の場所には到着していない場合、一時的な不一致が生じる可能性があります。そのため、例えばブロックルールによって参照されるドメインリストにドメインを追加すると、新しいドメインは VPC のあるエリアで一時的にブロックされ、別のエリアでは許可されます。この一時的な不一致は、ルールグループと VPC の関連付けを初めて行う際、既存の設定を変更する際に発生する可能性があります。ほとんどの場合、このタイプの不一致は数秒で解決します。

ルールグループおよびルールの作成

ルールグループを作成してルールを追加するには、この手順のステップに従います。

ルールグループとそのルールを作成するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。

   ナビゲーションペインで、[DNS ファイアウォール] を選択し、Amazon VPC コンソールの [ルールグループ] ページで DNS ファイアウォールを開きます。ステップ 3 に進みます。

   - または -

   AWS マネジメントコンソール にサインインして、

   https://console.aws.amazon.com/vpc/ から、Amazon VPC コンソールを開きます。
2. ナビゲーションペインで、[DNS ファイアウォール] の下にある [ルールグループ] を選択します。
3. ナビゲーションバーで、ルールグループのリージョンを選択します。
4. [Add rule group (ルールグループの追加)] を選択し、ウィザードのガイダンスに従ってルールグループとルール設定を指定します。

   ルールグループにルールを追加するときは、まずルールタイプとして Foundation または Advanced を選択します。

   - Foundation – ルール保護を選択して、独自のカスタムドメインリストまたは AWS 重要なマネージドドメインリストでルールを作成します。

     カスタムドメインリストの詳細については、「」を参照してください独自のドメインリストの管理。

     マネージドドメインリストの詳細については、「」を参照してくださいマネージドドメインリスト。
   - 詳細 – 1 つ以上の高度なマネージドドメインリスト (脅威カテゴリとコンテンツカテゴリ) または高度な保護 (ドメイン生成アルゴリズム、ディクショナリ DGA、または DNS トンネリング) を選択します。

     高度なマネージドドメインリストの詳細については、「」を参照してください高度なマネージドドメインリスト。

高度な保護の詳細については、「」を参照してください高度な DNS 保護。

5. ルールごとに、1 つ以上のルール設定を選択できます。

   ルールグループの値の詳細については、「DNS Firewall のルールグループ設定」を参照してください。

   ルールの値の詳細については、「DNS Firewall のルール設定」を参照してください。

ルールグループおよびルールの表示と更新

ルールグループとそのグループに割り当てられたルールを表示するには、次の手順に従います。ルールグループとルール設定を更新することもできます。

ルールとグループを表示および更新するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。

   ナビゲーションペインで、[DNS ファイアウォール] を選択し、Amazon VPC コンソールの [ルールグループ] ページで DNS ファイアウォールを開きます。ステップ 3 に進みます。

   - または -

   AWS マネジメントコンソール にサインインして、

   https://console.aws.amazon.com/vpc/ から、Amazon VPC コンソールを開きます。
2. ナビゲーションペインで、[DNS ファイアウォール] の下にある [ルールグループ] を選択します。
3. ナビゲーションバーで、ルールグループのリージョンを選択します。
4. 表示または編集するルールグループを選択し、[View details (詳細を表示)] を選択します。
5. ルールグループのページで、設定を表示および編集できます。

   ルールグループの値の詳細については、「DNS Firewall のルールグループ設定」を参照してください。

   ルールの値の詳細については、「DNS Firewall のルール設定」を参照してください。

ルールグループの削除

ルールグループの削除は、次の手順を実行します。

> **Important**
>
> VPC に関連付けられているルールグループを削除すると、DNS Firewall は関連付けを削除し、ルールグループが VPC に行っていた保護を停止します。

DNS Firewall エンティティの削除

DNS Firewall で使用できるエンティティ (ルールグループで使用中のドメインリストや VPC に関連付けられている可能性があるルールグループなど) を削除すると、DNS Firewall ではそのエンティティが現在使用されているかどうかの確認が行われます。使用中であることが判明した場合、DNS Firewall からアラートが表示されます。DNS Firewall では、ほとんどの場合エンティティが使用中かどうかを判別できます。ただし、まれに判別できないことがあります。エンティティが現在使用中でないことを確認する必要があるときは、DNS Firewall 設定で確認してください。エンティティが参照されているドメインリストである場合は、ルールグループでエンティティが使用されていないことを確認してください。エンティティがルールグループである場合は、どの VPC にも関連付けられていないことを確認してください。

ルールグループを削除するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。

   ナビゲーションペインで、[DNS ファイアウォール] を選択し、Amazon VPC コンソールの [ルールグループ] ページで DNS ファイアウォールを開きます。ステップ 3 に進みます。

   - または -

   AWS マネジメントコンソール にサインインして、

   https://console.aws.amazon.com/vpc/ から、Amazon VPC コンソールを開きます。
2. ナビゲーションペインで、[DNS ファイアウォール] の下にある [ルールグループ] を選択します。
3. ナビゲーションバーで、ルールグループのリージョンを選択します。
4. 削除するルールグループを選択し、削除を選択して削除を確定します。

DNS ファイアウォールの基本ルール

DNS Firewall Foundational ルールは、DNS Firewall の使用を開始するのに役立つ基本的な DNS 保護を提供します。次の 2 種類の基本ルールがあります。

- マネージドドメインリストは、自動的に AWS 作成および維持されます。
- お客様が作成し管理を行う独自のドメインリスト。1 つのドメインリストを複数のルールで使用でき、ドメインリストに加えた更新は、それを使用するすべてのルールに自動的に影響します。

ドメインリストは、ルールグループ内の DNS Firewall ルールで使用する、再利用可能なドメイン仕様のセットです。ルールグループを VPC に関連付けると、DNS Firewall はルールで使用されているドメインリストとDNS クエリを比較します。一致が見つかった場合は、一致したルールのアクションに従って DNS クエリを処理します。ルールグループおよびルールに関する詳細は、「DNS Firewall のルールグループとルール」を参照してください。

マネージドドメインリスト

マネージドドメインリストには、悪意のあるアクティビティやその他の潜在的な脅威に関連するドメイン名が含まれています。Route 53 VPC Resolver のお客様は、DNS Firewall の使用時にアウトバウンド DNS クエリを無料でチェックできるように、これらのリスト AWS を維持します。

絶えず変化する脅威の状況に遅れずについていくには、時間とコストがかかることがあります。マネージドドメインリストを使用すると、DNS Firewall を実装して使用する時間を節約できます。は、新しい脆弱性や脅威が発生したときにリスト AWS を自動的に更新します。 AWS は、一般に公開される前に新しい脆弱性の通知を受け取ることが多いため、DNS Firewall は、新しい脅威が広く知られる前に緩和策を頻繁にデプロイできます。

マネージドドメインリストは、一般的なウェブの脅威からユーザーを保護するためのサポートを提供するように設計されており、アプリケーションに別のセキュリティレイヤーを追加します。 AWS Managed Domain Lists は、内部 AWS ソースと RecordedFuture の両方からデータを取得し、継続的に更新されます。ただし、 AWS マネージドドメインリストは、選択した AWS リソースによって決定される Amazon GuardDutyなどの他のセキュリティコントロールに代わるものではありません。

ベストプラクティスとして、本番稼働環境でマネージドドメインリストを使用する前に、ルールアクションを `Alert` に設定して、非本稼働環境でテストを行います。Amazon CloudWatch メトリクスと Resolver DNS Firewall のサンプルリクエストまたは DNS Firewall ログを組み合わせてルールを評価します。ルールが希望通りであることを確認したら、必要に応じてアクション設定を変更します。

利用可能な AWS マネージドドメインリスト

このセクションでは、DNS Firewall Foundational ルールで現在利用可能なマネージドドメインリストについて説明します。これらのリストがサポートされているリージョンにいる場合、ドメインリストの管理やルールのドメインリストの指定を行う際、コンソールに表示されます。ログでは、ドメインリストは `firewall_domain_list_id`フィールド内に記録されます。

AWS は、Resolver DNS Firewall のすべてのユーザーに対して、利用可能なリージョンの Foundational ルールタイプで次の Managed Domain Lists を提供します。

マネージドドメインリスト

脅威タイプ	説明
Malware	マルウェアの送信、マルウェアのホスティング、またはマルウェアの配布に関連するドメイン。
ボットネット/コマンドとコントロール	スパムマルウェアに感染したコンピュータのネットワークの制御に関連するドメイン。
脅威リストの集約	マルウェア、ランサムウェア、ボットネット、スパイウェア、DNS トンネリングなど、複数の DNS 脅威カテゴリに関連付けられているドメインは、複数のタイプの脅威をブロックするのに役立ちます。集約脅威リストには、ここにリストされている他の AWS マネージドドメインリストのすべてのドメインが含まれます。
Amazon GuardDuty 脅威リスト	Amazon GuardDuty DNS セキュリティ検出結果に関連付けられたドメイン。ドメインは GuardDuty の脅威インテリジェンスシステムのみから取得されており、外部のサードパーティーのソースから取得されたドメインは含まれません。より具体的には、現在、このリストは内部的に生成され、GuardDuty で次の検出に使用される次のドメインのみをブロックします: Impact:EC2/AbusedDomainRequest.Reputation、Impact:EC2/B

脅威タイプ	説明
	itcoinDomainRequest.Reputation、Impact:EC2/MaliciousDomainRequest.Reputation、Impact:Runtime/AbusedDomainRequest.Reputation、Impact:Runtime/BitcoinDomainRequest.Reputation、Impact:Runtime/MaliciousDomainRequest.Reputation。詳細については、「Amazon GuardDuty ユーザーガイド」の「検出結果タイプ」を参照してください。

AWS マネージドドメインリストはダウンロードまたは参照できません。知的財産を保護するために、 AWS マネージドドメインリスト内の個々のドメイン仕様を表示または編集することはできません。この制限はまた、悪意のあるユーザーが具体的に公開されているリストを避けて脅威を作り出すことを防ぐのにも役立ちます。

マネージドドメインリストをテストするには

マネージドドメインリストのテスト用に、以下のドメインセットが用意されています。

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 および
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

これらのドメインは、ブロックされなければ 1.2.3.4 に解決されます。マネージドドメインリストを VPC で使用すると、これらのドメインをクエリしたとき、(例えば NODATA で) ルール内のブロックアクションが設定されているレスポンスが返されます。

マネージドドメインリストの詳細については、AWS サポート センターにお問い合わせください。

次の表に、 AWS マネージドドメインリストのリージョンの可用性を示します。

利用可能なマネージドドメインリストのリージョン

リージョン	マネージドドメインリストを利用できますか?
アフリカ (ケープタウン)	はい
アジアパシフィック (香港)	はい
アジアパシフィック (ハイデラバード)	はい
アジアパシフィック (ジャカルタ)	はい
アジアパシフィック (マレーシア)	はい
アジアパシフィック (メルボルン)	はい
アジアパシフィック (ムンバイ)	はい
アジアパシフィック (大阪) リージョン	はい
アジアパシフィック (ソウル)	あり
アジアパシフィック (シンガポール)	あり

リージョン	マネージドドメインリストを利用できますか?
アジアパシフィック (シドニー)	はい
アジアパシフィック (タイ)	はい
アジアパシフィック (東京)	はい
Canada (Central) Region	はい
カナダ西部 (カルガリー)	はい
Europe (Frankfurt) Region	はい
欧州 (アイルランド) リージョン	はい
Europe (London) Region	はい
欧州 (ミラノ)	はい
欧州 (パリ) リージョン	はい
欧州 (スペイン)	はい
欧州 (ストックホルム)	はい
欧州 (チューリッヒ)	はい
イスラエル (テルアビブ)	はい
中東 (バーレーン)	はい

リージョン	マネージドドメインリストを利用できますか?
中東 (アラブ首長国連邦)	はい
南米 (サンパウロ)	はい
米国東部 (バージニア北部)	あり
米国東部 (オハイオ)	あり
米国西部 (北カリフォルニア)	あり
米国西部 (オレゴン)	はい
中国 (北京)	はい
中国 (寧夏)	はい
AWS GovCloud (US)	はい

セキュリティに関するその他の考慮事項

AWS マネージドドメインリストは、一般的なウェブ脅威からユーザーを保護するように設計されています。ドキュメントに従って使用した場合、これらのリストはアプリケーションに別のセキュリティレイヤーを追加します。ただし、マネージドドメインリストは、選択した AWS リソースに伴うセキュリティコントロールに代わるものではありません。のリソースが適切に保護されていることを確認するには、 AWS 「 責任共有モデル」のガイダンスを参照してください。

誤検出シナリオの軽減

マネージドドメインリストを使用してクエリをブロックするルールで誤検出のシナリオが発生した場合は、次の手順を実行します。

1. VPC Resolver ログで、誤検出の原因となっているルールグループとマネージドドメインリストを特定します。これを行うには、DNS Firewall がブロックしているが、通過を許可するクエリのログを見つけます。ログレコードには、ルールグループ、ルールアクション、マネージドリストが一覧表示されます。ログの詳細については、「VPC Resolver クエリログに表示される値」を参照してください。
2. ブロックしたクエリを明示的に許可するルールグループに新しいルールを作成します。ルールを作成するときに、許可するドメイン仕様のみを使用して、独自のドメインリストを定義できます。ルールグループおよびルールの作成 のルールグループおよびルールの管理に関するガイダンスに従ってください。
3. ルールグループ内で新しいルールの優先度を設定して、そのルールをマネージドリストを使用しているルールの前に実行できるようにします。これを行うには、新しいルールの優先順位の数値を小さく設定します。

ルールグループを更新すると、ブロックルールが実行される前に、許可するドメイン名が新しいルールによって明示的に示されます。

独自のドメインリストの管理

独自のドメインリストを作成すると、マネージドドメインリストのサービスに見つからないドメインカテゴリや、自分で処理したいドメインカテゴリを指定できます。

このセクションで説明する手順に加えて、 コンソールでは、ルールを作成または更新するときに、Resolver DNS Firewall ルール管理のコンテキストでドメインリストを作成できます。

ドメインリストの各ドメイン仕様は、次の要件を満たす必要があります。

- オプションで * (アスタリスク) から始めます。
- オプションの先頭のアスタリスクとピリオドを除き、ラベル間の区切り文字として、、A-Z、0-9、 - (ハイフン) a-zのみを含める必要があります。
- 長さは 1～255 文字にする必要があります。

ルールやドメインリストなどの DNS Firewall エンティティに変更を加えると、DNS Firewall はエンティティが格納および使用されるすべての場所に変更を伝播します。変更は数秒以内に適用されますが、変更がある場所に到着し、他の場所には到着していない場合、一時的な不一致が生じる可能性があります。そのため、例えばブロックルールによって参照されるドメインリストにドメインを追加すると、新しいドメインは VPC のあるエリアで一時的にブロックされ、別のエリアでは許可されま

す。この一時的な不一致は、ルールグループと VPC の関連付けを初めて行う際、既存の設定を変更する際に発生する可能性があります。ほとんどの場合、このタイプの不一致は数秒で解決します。

本番稼働環境で使用する前にドメインリストをテストする

ベストプラクティスとして、本番稼働環境でドメインリストを使用する前に、ルールアクションを `Alert` に設定して、非本稼働環境でテストを行います。Amazon CloudWatch メトリクスと VPC Resolver ログを使用してルールを評価します。ログには、すべてのアラートとブロックアクションのドメインリスト名が表示されます。ドメインリストが DNS クエリに希望どおりに一致していることを確認したら、必要に応じてルールのアクション設定を変更します。CloudWatch メトリクスとクエリログの詳細については、「Amazon CloudWatch を使用した Resolver DNS Firewall ルールグループのモニタリング」、「VPC Resolver クエリログに表示される値」および「Resolver のクエリログ記録の設定の管理」を参照してください。

ドメインリストを追加するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。

   ナビゲーションペインで、[DNS ファイアウォール] を選択し、Amazon VPC コンソールの [ルールグループ] ページで DNS ファイアウォールを開きます。ステップ 2 に進みます。

   - または -

   AWS マネジメントコンソール にサインインして、

   https://console.aws.amazon.com/vpc/ から、Amazon VPC コンソールを開きます。
2. ナビゲーションペインで、[DNS ファイアウォール] の下にある [ドメインリスト] を選択します。[ドメインリスト] ページで、既存のドメインリストを選択および編集したり、独自のドメインリストを追加することができます。
3. ドメインリストを追加するには、[ドメインリストの追加] を選択します。
4. ドメインリスト名を入力し、テキストボックスにドメイン指定を 1 行に 1 つずつ入力します。

   [Switch to bulk upload (一括アップロードに切り替える)] をオンにスライドして、ドメインリストを作成した Amazon S3 バケットの URI を入力します。このドメインリストには、1 行につき 1 つのドメイン名が必要です。

> **Note**
>
> ドメイン名が重複していると、一括インポートが失敗します。

5. [ドメインリストの追加] を選択します。[ドメインリスト] ページには、新しいドメインリストが一覧表示されます。

ドメインリストを作成したら、DNS Firewall ルールから名前を指定して参照できます。

DNS Firewall エンティティの削除

DNS Firewall で使用できるエンティティ (ルールグループで使用中のドメインリストや VPC に関連付けられている可能性があるルールグループなど) を削除すると、DNS Firewall ではそのエンティティが現在使用されているかどうかの確認が行われます。使用中であることが判明した場合、DNS Firewall からアラートが表示されます。DNS Firewall では、ほとんどの場合エンティティが使用中かどうかを判別できます。ただし、まれに判別できないことがあります。エンティティが現在使用中でないことを確認する必要があるときは、DNS Firewall 設定で確認してください。エンティティが参照されているドメインリストである場合は、ルールグループでエンティティが使用されていないことを確認してください。エンティティがルールグループである場合は、どの VPC にも関連付けられていないことを確認してください。

ドメインリストを削除するには

1. ナビゲーションペインで、[ドメインリスト] を選択します。
2. ナビゲーションバーで、ドメインリストのリージョンを選択します。
3. 削除するドメインリストを選択し、削除を選択して削除を確定します。

DNS ファイアウォールの詳細ルール

DNS Firewall Advanced Rule 階層は、より高度な DNS 脅威 (ドメイン生成アルゴリズム (DGA) や DNS トンネリングなど) を検出してモニタリングするのに役立つ保護、または脅威とウェブコンテンツ (ギャンブル、ソーシャルネットワーキングなど) に基づくより詳細な保護を提供します。

アドバンストルールには主に 3 つのタイプがあります。

- DNS クエリの既知の脅威シグネチャ (DGA など) に基づいて疑わしい DNS クエリを検出するのに役立つ高度な保護。

- DNS 脅威のタイプ (スパム、フィッシングなど) またはウェブコンテンツ (アダルトコンテンツ、ソーシャルネットワーキング、ギャンブルサイトなど) に基づいて DNS クエリをブロックするより詳細な制御を提供する高度な DNS 脅威とコンテンツカテゴリ。
- Palo Alto Networks Advanced DNS Security からのパートナーマネージド DNS 保護 (AWS Marketplace サブスクリプションが必要) 。

高度な DNS 保護

DNS Firewall Advanced は、DNS クエリの既知の脅威シグネチャに基づいて、疑わしい DNS クエリを検出します。ルールグループ内で、DNS Firewall ルールで使用するルールで脅威タイプを指定できます。ルールグループを VPC に関連付けると、DNS Firewall はルールでフラグが付いているドメインと DNS クエリを比較します。一致が見つかった場合は、一致したルールのアクションに従って DNS クエリを処理します。

DNS Firewall Advanced は、リクエストのタイムスタンプ、リクエストとレスポンスの頻度、DNS クエリ文字列、アウトバウンドとインバウンドの両方の DNS クエリの長さ、タイプ、サイズなど、DNS ペイロード内のキー識別子の範囲を調べることで、疑わしい DNS 脅威シグネチャを識別します。脅威署名のタイプに基づいて、ブロックするか、単にクエリをログに記録して警告するようにポリシーを設定できます。拡張された脅威識別子のセットを使用することで、より広範なセキュリティコミュニティによって維持されている脅威インテリジェンスフィードによってまだ分類されていないドメインソースからの DNS 脅威から保護できます。

現在、DNS Firewall Advanced は以下からの保護を提供しています。

- ドメイン生成アルゴリズム (DGAs)

  DGAs は、攻撃者が多数のドメインを生成してマルウェア攻撃を開始するために使用されます。
- DNS トンネリング

  DNS トンネリングは、攻撃者がクライアントへのネットワーク接続を行わずに DNS トンネルを使用してクライアントからデータを抽出するために使用されます。
- ディクショナリ DGA

  ディクショナリ DGAs は、攻撃者がディクショナリ単語を使用してドメインを生成し、マルウェアcommand-and-control通信での検出を回避するために使用されます。

ルールを作成する方法については、「ルールグループおよびルールの作成」および「DNS Firewall のルール設定」を参照してください。

誤検出シナリオの軽減

DNS Firewall Advanced 保護を使用してクエリをブロックするルールで誤検出のシナリオが発生した場合は、次の手順を実行します。

1. VPC Resolver ログで、誤検出の原因となっているルールグループと DNS Firewall Advanced 保護を特定します。これを行うには、DNS Firewall がブロックしているが、通過を許可するクエリのログを見つけます。ログレコードには、ルールグループ、ルールアクション、DNS Firewall Advanced 保護が一覧表示されます。ログの詳細については、「VPC Resolver クエリログに表示される値」を参照してください。
2. ブロックしたクエリを明示的に許可するルールグループに新しいルールを作成します。ルールを作成するときに、許可するドメイン仕様のみを使用して、独自のドメインリストを定義できます。ルールグループおよびルールの作成 のルールグループおよびルールの管理に関するガイダンスに従ってください。
3. ルールグループ内で新しいルールの優先度を設定して、そのルールをマネージドリストを使用しているルールの前に実行できるようにします。これを行うには、新しいルールの優先順位の数値を小さく設定します。

ルールグループを更新すると、ブロックルールが実行される前に、許可するドメイン名が新しいルールによって明示的に示されます。

高度なマネージドドメインリスト

アドバンストマネージドドメインリストには、悪意のあるアクティビティやその他のnot-safe-for-work用ドメインに関連付けられているドメイン名が含まれています。アドバンストマネージドドメインリストは脅威カテゴリとコンテンツカテゴリに分類され、一般的なウェブ脅威から保護し、safe-for-workでないドメインへのクエリ解決をブロックするように設計されています。

ベストプラクティスとして、本番稼働環境でマネージドドメインリストを使用する前に、ルールアクションを `Alert` に設定して、非本稼働環境でテストを行います。Amazon CloudWatch メトリクスと DNS Firewall ログを組み合わせてルールを評価します。ルールが希望通りであることを確認したら、必要に応じてアクション設定を変更します。

利用可能なアドバンストマネージドドメインリスト

このセクションでは、アドバンストルール階層で DNS ファイアウォールで現在利用可能なアドバンストマネージドドメインリストについて説明します。 は、脅威またはコンテンツタイプ別に分類された以下のマネージドドメインリスト AWS を提供します。

脅威カテゴリ

脅威
スパム
フィッシング

コンテンツカテゴリ

コンテンツ
暴力とヘイトスピーチ
子供向け
オンライン広告
サイエンス
家族と子育て
Pets
キャリアとジョブの検索
宗教
Lifestyle
ホームとガーデン
犯罪および違法行為
スポーツと娯楽
車両
金融サービス
不動産

コンテンツ
趣味と興味
Travel
料理とレストラン
政府と法律
教育
ファッショナリ
健康
ショッピング
アダルトコンテンツと成熟コンテンツ
テクノロジーとインターネット
ビジネスと経済
ニュース
検索エンジンとポータル
アートと文化
エンターテインメント
軍事
ソーシャルネットワーキング
プロキシ回避
リダイレクト
E メール

コンテンツ
[Translation] (変換)
児童虐待
中止
ギャンブル
ハッキング
マリファナ
Cryptocurrency
日付
人工知能とMachine Learning
パークされたドメイン
プライベート IP アドレス

DNS Firewall での Palo Alto Networks でのパートナーマネージド DNS 脅威保護の使用

このトピックでは、Amazon Route 53 Resolver DNS Firewall ルールグループ内の Palo Alto Networks (PANW) DNS 脅威保護ルールをサブスクライブ、設定、管理する方法について説明します。

Palo Alto Networks Advanced DNS Security for Route 53 は、Palo Alto Networks 脅威インテリジェンスを DNS Firewall に直接統合することで、Amazon Virtual Private Cloud インスタンスにクラウドネイティブな DNS 脅威保護を提供します。この統合により、個別のファイアウォールをデプロイしたり、Amazon VPC ルーティング設定を管理したり、DNS トラフィックを外部検査ポイントに転送したりする必要がなくなります。Palo Alto Networks DNS 保護は、DNS セキュリティの管理に既に使用しているものと同じ DNS Firewall ルールとルールグループを通じて適用します AWS。

統合は、次の 2 つの主要な方法で役立ちます。

1. Palo Alto Networks Advanced DNS Security から 30 以上の DNS 脅威検出へのアクセスを提供します。例としては、高速フラックス検出、DNS ハイジャック、ドメイン生成アルゴリズム (DGA) 検出、新しく登録されたドメインの識別などがあります。
2. これにより、DNS 検査のみを目的として、複数の VPCsとアカウントに Palo Alto Networks ファイアウォールをデプロイするインフラストラクチャのオーバーヘッドがなくなります。これにより、同じ脅威の有効性を維持しながら、コストと運用の複雑さの両方を減らすことができます。

> **可用性**
>
> Palo Alto Networks によるパートナーマネージド DNS 脅威保護は、DNS Firewall AWS リージョン が利用可能なすべての商用 で一般利用可能です。

前提条件

Palo Alto Networks でパートナーマネージド DNS 脅威保護を使用する前に、次のものが必要です。

- DNS Firewall と AWS Marketplace の適切な IAM アクセス許可を持つ AWS アカウント。
- DNS Firewall ルールグループが既に作成されている (またはワークフロー中に作成されている)。
- ルールグループに選択されたアドバンストプランの料金オプション (パートナーマネージド DNS 脅威保護に必要)。これは、DNS Firewall ルールの作成時に選択できます。

Palo Alto Networks Advanced DNS Security をサブスクライブする

Palo Alto Networks Advanced DNS Security は、ルール作成フロー中に DNS Firewall コンソールから直接、または AWS Marketplace からサブスクライブできます。サブスクライブすると、 が DNS クエリメタデータ AWS を Palo Alto Networks と共有することを許可します。

DNS Firewall コンソールを使用してサブスクライブする (推奨)

コンソールからサブスクライブするには、次の手順に従います。

1. AWS マネジメントコンソールにサインインし、Amazon Virtual Private Cloud コンソールを開きます。
2. ナビゲーションペインで、[DNS ファイアウォール] の下にある [ルールグループ] を選択します。
3. パートナーマネージド DNS 保護を追加するルールグループを選択します。

4. [ルールを追加] を選択してください。
5. ルールの詳細に、ルールの名前を入力します (例: `PAN Threat Protection Rule`)。有効な文字: A ~ Z、a ~ z、0 ~ 9、ハイフン (-)、アンダースコア (_)。最大 64 文字。アドバンスト料金オプションを選択します。
6. ルール設定 > ルールタイプで、パートナーマネージド DNS 脅威保護を選択します。
7. Vendor で、Palo Alto Networks を選択します。

まだサブスクライブしていない場合は、 AWS Marketplace for Palo Alto Networks を通じてサブスクリプションが必要であることを示すバナーが表示されます。

1. サブスクリプションオプションの表示 を選択します。利用可能なオファー、料金詳細、法的条件を示すサブスクリプションダイアログが表示されます。
2. 利用規約と料金を確認し、サブスクライブを選択します。
3. サブスクリプションが処理されるまで待ちます。ステータスバナーは、 AWS Marketplace サブスクリプションが処理中であることを示します。サブスクリプションがアクティブになると、フォームは自動的に更新されます。
4. サブスクリプションが成功すると、DNS セキュリティカテゴリドロップダウンが利用可能になり、ルール作成の脅威リストフィードを選択できます。

AWS Marketplace でサブスクライブする

Marketplace からサブスクライブするには、次の手順に従います。

1. AWS Marketplace コンソールを開きます。
2. Amazon Route 53 の「Palo Alto Networks Advanced DNS Security for Amazon Route 53」製品を検索します。
3. 製品の出品、料金、条件を確認します。
4. [サブスクライブ] を選択します。
5. サブスクライブしたら、DNS Firewall コンソールに戻り、パートナーマネージドルールタイプを使用してルールを作成します。

> **Note**
>
> Marketplace コンソールからサブスクライブすると、販売者のホームページにリダイレクトされます。DNS Firewall コンソールからサブスクライブした場合、リダイレクトされませ

ん。必要な登録の詳細を入力するには、販売者のホームページに個別にアクセスすることをお勧めします。

Palo Alto Networks のサブスクリプションを解除する

> **Important**
>
> サブスクリプション料金を停止するには、 AWS Marketplace からのサブスクリプション解除に加えて、DNS Firewall ルールグループからすべての PANW ルールを削除する必要があります。サブスクリプションを解除してもルールグループ内にルールを残した場合、ルールを削除するまで料金は継続されます。

すべてのルールグループから PANW ルールを削除する

PANW ルールを削除するには、次の手順に従います。

1. Amazon Virtual Private Cloud コンソールを開きます。
2. ナビゲーションペインで、DNS ファイアウォールを選択し、ルールグループを選択します。
3. Palo Alto Networks ルールを含むルールグループごとに、パートナーマネージドルールを選択し、削除を選択します。
4. 削除を確定します。

Marketplace サブスクリプションをキャンセルする

サブスクリプションをキャンセルするには、次の手順に従います。

1. AWS Marketplace コンソールを開きます。
2. [サブスクリプションを管理する] を選択します。
3. [配信方法] リストを開き、[SaaS] を選択します。
4. 契約で、アクションリストを開き、Palo Alto Networks 製品の横にあるサブスクリプションをキャンセルを選択します。
5. [サブスクリプションをキャンセル] ダイアログボックスで、**`confirm`** と入力し、[はい、サブスクリプションをキャンセルします] を選択します。

> **Note**
>
> サブスクリプションを解除してもルールグループ内にルールを残した場合、ルールを削除するまで料金は継続されます。

DNS Firewall ルールグループに Palo Alto Networks ルールを追加する

サブスクライブ後、任意の DNS Firewall ルールグループ内で Palo Alto Networks 脅威フィードを使用して 1 つ以上のルールを作成できます。

Palo Alto Networks ルールを追加するには

ルールを追加するには、次の手順に従います。

1. Amazon Virtual Private Cloud コンソールを開き、ナビゲーションペインで DNS ファイアウォールを選択し、ルールグループを選択します。
2. ターゲットルールグループを選択します。
3. [ルールを追加] を選択してください。
4. ルールの詳細で、名前を入力し、詳細プランの料金オプションを選択します。
5. ルール設定 > ルールタイプで、パートナーマネージド DNS 脅威保護を選択します。
6. Vendor で、Palo Alto Networks が選択されていることを確認します。
7. DNS セキュリティカテゴリで、ドロップダウンから脅威リストフィードを 1 つ以上選択します。使用可能なカテゴリの詳細については、次の表を参照してください。
8. アクション で、アクション ALERT (ログは許可されます) または BLOCK (クエリをブロックします) を選択します。
9. [ルールを追加] を選択してください。成功バナーはルールの作成を確認します。

使用可能な DNS セキュリティカテゴリ

次の表は、Palo Alto Networks から利用できる DNS セキュリティカテゴリを示しています。

DNS セキュリティカテゴリ

Category	説明
Palo Alto Networks - 動的 DNS ホストドメイン	IP アドレスの迅速な変更を許可する動的 DNS プロバイダーを使用するドメイン。IP ベースのブロックを回避するために脅威アクターによって頻繁に悪用されます。
Palo Alto Networks - パークドドメイン	プレースホルダーまたは「販売用」コンテンツを表示するドメイン。攻撃者はこれらを取得して、残された評判を活用し、訪問者を悪意のあるコンテンツにリダイレクトする可能性があります。
Palo Alto Networks - プロキシ回避と匿名化	ウェブプロキシ、VPN サービス、匿名化ネットワークなど、ネットワークセキュリティコントロールをバイパスするサービスを提供するドメイン。
Palo Alto Networks - 広告追跡ドメイン	広告ネットワークとサードパーティートラッカーがユーザーアクティビティをモニタリングするために使用するドメイン。これらは、悪意のあるキャンペーンのベクトルとして機能します。
Palo Alto Networks - 新しく登録されたドメイン	過去 32 日以内に登録されたドメイン。攻撃者は評価履歴がないため、新しいドメインを使用するため、検出が困難になります。
Palo Alto Networks - グレーウェアドメイン	過剰な追跡、未承諾広告、ブラウザハイジャックなどの望ましくない動作を示すアプリケーションに関連付けられたドメイン。
Palo Alto Networks - フィッシングドメイン	タイプクォータ、ホモグラフ攻撃、またはドメインシャドウを通じて認証情報や個人情報を盗む正当な組織を偽装するドメイン。
Palo Alto Networks - Malware ドメイン	エクスプロイトキット、ランサムウェアのドロッパー、トロイの木馬配信ネットワークなど、悪意のあるソフトウェアをホストまたは配布するドメイン。

Category	説明
Palo Alto Networks - コマンドドメインとコントロールドメイン	マルウェアが命令、データ流出、ペイロード配信のために攻撃者が管理するインフラストラクチャと通信するために使用するドメイン。

> **Tip**
>
> 選択したセキュリティカテゴリごとに、ルールグループ内に個別のルールエントリが作成されます。4 つのカテゴリを選択すると、4 つのルールが順番に優先順位を付けて作成されます。

Palo Alto Networks からマネージドルールを表示する

コンソール、API、または CLI を使用して、使用可能な PANW マネージドルールグループとその現在の状態を表示できます。

コンソールを使用して マネージドルールを表示するには

ルールを表示するには、次の手順に従います。

1. Amazon Virtual Private Cloud コンソールを開きます。
2. ナビゲーションペインで、DNS ファイアウォールを選択し、ルールグループを選択します。
3. PANW ルールを含むルールグループを選択します。
4. ルールタブで、名前、アクション、優先度、ルールタイプ、リソース値、クエリタイプ、ドメインリダイレクト設定、ステータスの列を含むルールを表示します。

Palo Alto Networks ルールのルール状態

DNS Firewall の PANW ルールは、ステータスを示す異なる同期状態を持つことができます。

ルールの同期状態

同期状態	説明	推奨されるアクション
CREATED	ルールが正常に作成され、正常に適用されています。	アクションは不要です。

同期状態	説明	推奨されるアクション
CREATING	ルールは現在作成中であり、使用権限チェックを保留しています。PANW 製品をサブスクライブしている場合、ルールは最終的に に移行しますCREATED。	アクションは不要です。
CREATION_FAILED	PANW 製品をサブスクライブしていないため、ルールの作成に失敗しました。	サブスクライブ後にルールの作成を再試行するには、ルールグループからルールを削除し、ルールを再度作成する必要があります。

コンソールでルールのステータスを確認するには、DNS Firewall ルールグループに移動し、ルールテーブルのステータス列を確認します。

Palo Alto Networks パートナーマネージドルールのベストプラクティス

Palo Alto Networks パートナーマネージド DNS 脅威保護を使用する場合は、次のベストプラクティスをお勧めします。

- 本番稼働前のテスト: 本番稼働環境にデプロイする前に、 ALERT モードを使用してドライランを実行します。アラートログを確認してから、検証BLOCK後に に切り替えます。
- カテゴリごとに複数のルール: セキュリティカテゴリごとに個別のルールが作成されます。異なるカテゴリに異なるアクションを割り当てることができます。
- Amazon VPC の関連付け: ルールを追加したら、ルールグループが Amazon VPC に関連付けられていることを確認し、ルールを有効にします。
- AWS Firewall Manager 統合: AWS Firewall Manager ポリシーに関連付けるオプションを使用して、組織全体にルールグループを適用します。

DNS Firewall でのログ記録の設定

Amazon CloudWatch メトリクスと Resolver のクエリログを使用して、DNS Firewall のルールを評価できます。ログには、すべてのアラートとブロックアクションのドメインリスト名が表示されます。Amazon CloudWatch の詳細については、「Amazon CloudWatch を使用した Resolver DNS Firewall ルールグループのモニタリング」を参照してください。

DNS Firewall を有効にして、VPC に関連付けログ記録を有効にした場合、`firewall_rule_group_id`、`firewall_rule_action`、 `firewall_domain_list_id` は、ログ内に提供される DNS Firewall 特有のフィールドです。

> **Note**
>
> クエリログには、DNS ファイアウォールルールによってブロックされたクエリの追加の DNS ファイアウォールフィールドのみが表示されます。

VPC から発信される DNS Firewall のルールによってフィルタリングされた DNS クエリのログ記録を開始するには、Amazon Route 53 コンソールで次のタスクを実行します。

DNS Firewall で Resolver のクエリログ記録を設定するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. Route 53 コンソールのメニューを展開します。コンソールの左上隅にある 3 本の水平バー (☰) アイコンを選択します。
3. Resolver メニューから、[Query logging (クエリログ記録)] を選択します。
4. リージョンセレクターで、クエリログ記録設定を作成する AWS リージョンを選択します。

   これは、クエリをログに記録する DNS Firewall に関連付けた VPC を作成したリージョンと同じリージョンである必要があります。VPC が複数のリージョンに存在する場合は、リージョンごとにクエリログ記録の設定を少なくとも 1 つ作成する必要があります。
5. [クエリログ記録の設定] を選択します。
6. 次の値を指定します。

   クエリログ記録設定の名前

   クエリログ記録の設定に使用する名前を入力します。この名前は、コンソールのクエリログ記録の設定リストに表示されます。この設定では、後で検索する際に便利な名前を入力します。

クエリログの保存先

VPC Resolver がクエリログを送信する AWS リソースのタイプを選択します。各オプション (CloudWatch Logs ロググループ、S3 バケット、および Firehose 配信ストリーム) から選択する方法については、「AWS VPC Resolver クエリログを送信できる リソース」を参照してください。

リソースのタイプを選択したら、そのタイプの別のリソースを作成するか、現在の AWS アカウントによって作成された既存のリソースを選択できます。

> **Note**
>
> ステップ 4 で選択した AWS リージョン (クエリログ記録の設定を作成するリージョン) で作成されたリソースのみを選択できます。新しいリソースを作成することを選択した場合、そのリソースは同じリージョンに作成されます。

クエリを ログに記録する VPC

このクエリログ記録の設定では、選択した VPC で発生した DNS クエリがログに記録されます。VPC Resolver がクエリをログに記録する現在のリージョンの各 VPC のチェックボックスをオンにし、選択を選択します。

> **Note**
>
> VPC ログの配信は、特定の送信先タイプに対して 1 回だけ有効にすることができます。ログは、同じタイプの複数の送信先に配信することはできません。例えば、VPC ログを 2 つの Amazon S3 の送信先に配信することはできません。

7. [クエリログ記録の設定] を選択します。

> **Note**
>
> クエリログ記録の設定が正常に作成されてから数分以内に、VPC 内のリソースによって作成された DNS クエリがログ内に表示されるようになります。

Resolver DNS Firewall ルールグループを AWS アカウント間で共有する

AWS アカウント間で DNS Firewall ルールグループを共有できます。ルールグループを共有するには、 AWS Resource Access Manager () を使用しますAWS RAM。DNS Firewall コンソールは AWS RAM コンソールと統合されます。詳細については AWS RAM、「 Resource Access Manager ユーザーガイド」を参照してください。

次の点に注意してください。

VPC と共有ルールグループの関連付け

別の AWS アカウントが自分のアカウントとルールグループを共有している場合は、作成したルールグループを関連付けるのと同じ方法で VPCs に関連付けることができます。詳細については、「VPC と Resolver DNS Firewall ルールグループ間の関連付けの管理」を参照してください。

ルールグループの削除または共有解除

他のアカウントと共有しているルールグループまたはその共有を解除すると、DNS Firewall では他のアカウントがルールグループと VPC の間に作成したすべての関連付けが削除されます。

ルールグループおよび関連付けの最大設定

共有ルールグループと VPC との関連付けの数は、ルールグループを共有するアカウントの総数に含まれます。

現在の DNS Firewall のクォータについては「Resolver DNS ファイアウォールのクォータ」を参照してください。

アクセス許可

ルールグループを別の AWS アカウントと共有するには、PutFirewallRuleGroupPolicy アクションを使用するアクセス許可が必要です。

ルールグループが共有されている AWS アカウントの制限

ルールグループが共有されているアカウントが、ルールグループを変更または削除することはできません。

タグ付け

ルールグループを作成したアカウントだけが、ルールグループのタグを追加、削除、または表示できます。

ルールグループの現在の共有ステータス (ルールグループを共有したアカウントやルールグループが共有されているアカウントを含む) を確認し、別のアカウントとルールグループを共有するには、次の手順を実行します。

共有ステータスを表示し、ルールグループを別の AWS アカウントと共有するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで、[Rule groups] (ルールグループ) を選択します。
3. ナビゲーションバーで、ルールグループを作成したリージョンを選択します。

   [Sharing status (共有ステータス)] 列に、現在のアカウントで作成されたルールグループまたは現在のアカウントと共有されているルールグループの現在の共有ステータスが表示されます。

   - Not shared: 現在の AWS アカウントがルールグループを作成し、ルールグループは他のアカウントと共有されません。
   - Shared by me (自分が共有): 現在のアカウントがルールグループを作成し、1 つ以上の他のアカウントと共有しています。
   - Shared with me (自分と共有): 別のアカウントがルールグループを作成し、現在のアカウントと共有しています。
4. 共有情報を表示するルールグループまたは別のアカウントと共有するルールグループの名前を選択します。

   Rule group: ***rule group name*** ページで、[Owner (所有者)] の値として、ルールグループを作成したアカウントの ID が表示されます。これは現在のアカウントです。ただし、[Sharing status (共有ステータス)] の値が [Shared with me (自分と共有)] である場合を除きます。この場合、所有者はルールグループを作成し、現在のアカウントと共有したアカウントです。
5. [Share (共有)] を選択し、追加情報を表示するか、別のアカウントとルールグループを共有します。共有ステータスの値に応じて、 AWS RAM コンソールにページが表示されます。

   - Not shared (未共有): [Create resource share (リソース共有の作成)] ページが表示されます。別のアカウントと、あるいは組織単位 (OU) や組織でルールグループを共有する方法については、この後の手順を参照してください。
   - Shared by me (自分が共有): [Shared resources (共有リソース)] ページに、現在のアカウントが所有し、他のアカウントと共有しているルールグループと他のリソースが表示されます。
   - Shared with me (自分と共有): Shared resources (共有リソース) ページに、他のアカウントが所有し、現在のアカウントと共有しているルールグループと他のリソースが表示されます。

6. ルールグループを別の AWS アカウント、OU、または組織と共有するには、次の値を指定します。

> **Note**
>
> 共有設定を更新することはできません。次のいずれかの設定を変更する場合は、新しい設定を使用してルールグループを共有し直し、古い共有設定を削除する必要があります。

説明

ルールグループを共有した理由についての簡単な説明を入力します。

リソース

共有するルールグループのチェックボックスをオンにします。

プリンシパル

AWS アカウント番号、OU 名、または組織名を入力します。

タグ

1 つ以上のキーと対応する値を指定します。たとえば、キーにコストセンターを指定し、値に 456 を指定することができます。

これらは、 が AWS 請求書を整理するために AWS Billing and Cost Management 提供するタグです。他の目的でタグを使用することもできます。タグを使ったコスト配分の詳細については、AWS Billing ユーザーガイドのコスト配分タグの使用を参照してください。

VPC のリゾルバー DNS ファイアウォール保護の有効化

VPC 向けの DNS Firewall による保護を有効にするには、1 つ以上のルールグループを VPC に関連付けます。VPC が DNS Firewall ルールグループに関連付けられている場合、Route 53 VPC Resolver は次の DNS Firewall 保護を提供します。

- VPC Resolver は VPC のアウトバウンド DNS クエリを DNS Firewall 経由でルーティングし、DNS Firewall は関連するルールグループを使用してクエリをフィルタリングします。
- VPC リゾルバーは、VPC の DNS ファイアウォール設定の設定を適用します。

DNS Firewall による保護を VPC に提供するには、次の操作を行います。

- DNS Firewall ルールグループと VPC 間の関連付けを作成および管理します。ルールグループについては、「DNS Firewall のルールグループとルール」を参照してください。
- DNS ファイアウォールが DNS クエリの応答を提供しない場合など、障害発生時に VPC の DNS クエリを VPC リゾルバーが処理する方法を設定します。

VPC と Resolver DNS Firewall ルールグループ間の関連付けの管理

ルールグループでの VPC の関連付けを表示するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。

   ナビゲーションペインで、[DNS ファイアウォール] を選択し、Amazon VPC コンソールの [ルールグループ] ページで DNS ファイアウォールを開きます。

   - または -

   AWS マネジメントコンソール にサインインして、

   https://console.aws.amazon.com/vpc/ から、Amazon VPC コンソールを開きます。
2. ナビゲーションペインで、[DNS ファイアウォール] の下にある [ルールグループ] を選択します。
3. ナビゲーションバーで、ルールグループのリージョンを選択します。
4. 関連付けるルールグループを選択します。
5. [詳細を表示] を選択します。ルールグループのページが表示されます。
6. 下部には、ルールと関連する VPC を含むタブ付きの詳細エリアが表示されます。[関連付けられた VPC] タブを選択します。

ルールグループを VPC に関連付けるには

1. ルールグループでの VPC の関連付けを確認するには、前述の手順「ルールグループの VPC の関連付けを表示するには」を実行します。
2. [関連付けられた VPC] タブで、[VPC を関連付け] を選択します。
3. ドロップダウンで、ルールグループに関連付ける VPC を見つけます。それを選択し、[Associate (関連付け)] をクリックします。

ルールグループのページでは、[関連付けられた VPC] タブに VPC が表示されます。最初は、関連付けのステータスに更新中と表示されます。関連付けが完了すると、ステータスは 完了に変わります。

ルールグループと VPC 間の関連付けを削除するには

1. ルールグループでの VPC の関連付けを確認するには、前述の手順「ルールグループの VPC の関連付けを表示するには」を実行します。
2. リストから削除する VPC を選択し、関連付け解除を選択します。検証し、アクションを確認します。

ルールグループのページでは、[関連付けを解除中] のステータスで [関連付けられた VPC] タブに VPC が表示されます。操作が完了すると、DNS Firewall がリストを更新して VPC が削除されます。

DNS Firewall での VPC の設定

VPC の DNS ファイアウォール設定は、DNS ファイアウォールに障害が発生したとき、応答しないとき、またはゾーンで使用できないときなど、障害発生時に Route 53 VPC Resolver がクエリを許可またはブロックするかどうかを決定します。VPC Resolver は、VPC に関連付けられた 1 つ以上の DNS Firewall ルールグループがあるたびに、VPC のファイアウォール設定を適用します。

フェールオープンまたはフェールクローズするように VPC を設定できます。

- デフォルトでは、障害モードは閉じられます。つまり、VPC Resolver は DNS Firewall から応答を受信しないクエリをブロックし、DNS `SERVFAIL` 応答を送信します。このアプローチでは、可用性よりもセキュリティが優先されます。
- フェイルオープンを有効にすると、VPC Resolver は DNS Firewall から応答を受信しない場合にクエリを許可します。このアプローチでは、セキュリティよりも可用性が優先されます。

VPC の DNS Firewall 設定を変更するには (コンソール)

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53resolver/ で VPC Resolver コンソールを開きます。
2. リゾルバーのナビゲーションペインで、VPCsを選択します。
3. [VPC] ページで VPC を特定し、編集します。必要に応じて、DNS Firewall 設定をフェールオープンまたはフェールクローズに変更します。

VPC (API) 向けの DNS Firewall の動作を変更するには

- UpdateFirewallConfig を呼び出し、 を有効または無効にして、VPC ファイアウォール設定を更新します `FirewallFailOpen`。

ListFirewallConfigs を呼び出すことで、API を通じて VPC ファイアウォール設定のリストを取得できます。

Amazon Route 53 プロファイルとは

Route 53 プロファイルを使用すると、DNS 関連の Route 53 設定を多くの VPCs や異なる に適用および管理できます AWS アカウント。プロファイルにより、多くの VPC の DNS 設定の管理は、単一の VPC の管理と同じくらい簡単になり、プロファイルを更新すると、その設定はプロファイルに関連付けられたすべての VPC に伝達されます。を使用して、同じリージョン AWS アカウント の とプロファイルを共有することもできます AWS RAM。プロファイルに関連付けることができる、現在 Route 53 でサポートされているリソースは次のとおりです。

- プライベートホストゾーンとそのゾーンで指定された設定。プライベートホストゾーンの使用について詳しくは「プライベートホストゾーンの使用」を参照してください。
- 転送とシステムの両方のリゾルバールール。Resolver ルールの詳細については、「転送ルールの管理」を参照してください。
- DNS ファイアウォールルールグループ。DNS ファイアウォールルールグループの詳細については「DNS Firewall のルールグループとルール」を参照してください。
- インターフェイス VPC エンドポイント。インターフェイス VPC エンドポイントについて詳しくは、「Amazon VPC ユーザーガイド」の「インターフェイス VPC エンドポイント 」を参照してください。
- VPC Resolver クエリのログ記録設定。VPC Resolver クエリのログ記録の詳細については、「」を参照してくださいリゾルバーでのクエリのログ記録。

一部の VPC 設定は、プロファイルで直接管理されます。設定は次のとおりです。

- リゾルバールールの逆 DNS ルックアップ設定。
- DNS ファイアウォール障害モード設定。
- DNSSEC 検証設定。

例えば、プロファイルが関連付けられているすべての VPC で DNS ファイアウォール障害モード設定を有効にできますが、VPC の既存の DNSSEC 検証設定は維持できます。

> **Important**
>
> 上記の設定のプロファイル設定を有効にし、プロファイルを VPC に関連付けると、プロファイル設定がすぐに有効になります。

を使用して CloudFormation 、新しくプロビジョニングされた VPCs の一貫した DNS 設定を設定することもできます。

VPC ごとに 1 つのプロファイルを関連付けることができます。関連付けることができるリソースの数はプロファイルごとに異なります。詳細については、「Route 53 プロファイルのクォータ」を参照してください。

Route 53 プロファイル設定の優先順位付け方法

ローカル DNS 設定と関連付けを、移行やその他のテスト目的でプロファイルに設定することができます。DNS クエリが VPC に直接関連付けられているプライベートホストゾーンのリゾルバールールと、プロファイルに関連付けられているプライベートホストゾーンのリゾルバールールの両方に一致する場合、ローカル DNS 設定が優先されます。競合するドメイン名に対して DNS クエリが行われると、最も具体的なドメイン名が優先されます。次の表には、評価順序の例が含まれています。

DNS 評価順序の例

DNS クエリ	プロファイルルール	VPC ルール	評価されたルール
example.com	example.com	example.com	ローカル VPC
test.example.com	test.example.com	example.com	プロファイル
marketing.example.com	なし	marketing.example.com	ローカル VPC

Route 53 プロファイルリージョンの可用性

リージョンの可用性とエンドポイントを確認するには、「AWS 一般リファレンスガイド」の「Route 53 のサービスエンドポイント」を参照してください。

Route 53 プロファイルを使用する手順の概要

Amazon Virtual Private Cloud VPC で Amazon Route 53 プロファイルを実装するには、次の大まかなステップを実行します。

1. 空のプロファイルを作成する – 最初のステップは、DNS リソースを関連付けることができる空のプロファイルを作成することです。詳細については、「Route 53 プロファイルの作成」を参照してください。
2. DNS リソースをプロファイルに関連付ける – 現在プロファイルに関連付けることができるリソースは、プライベートホストゾーン、リゾルバールール、転送とシステムの両方、DNS Firewall ルールグループ、VPC Resolver クエリログ記録設定、インターフェイス VPC エンドポイントです。詳細については、「DNS ファイアウォールルールグループを Route 53 プロファイルに関連付ける」、「プライベートホストゾーンを Route 53 プロファイルに関連付ける」、「リゾルバールールを Route 53 プロファイルに関連付ける」、「VPC Resolver クエリログ設定を Route 53 プロファイルに関連付ける」、「インターフェイス VPC エンドポイントを Route 53 プロファイルに関連付ける」を参照してください。
3. プロファイルの VPC 設定の一部を設定する – プロファイルに関連付けられたホストゾーンなどの DNS 設定の一部は、VPC にすぐに適用されます。DNSSEC 検証、リゾルバーのリバース DNS ルックアップ、および DNS ファイアウォール障害モード設定では、次のいずれかのオプションを選択できます。
   - DNSSEC 検証では、ローカル VPC 設定 (デフォルト) を使用するか、検証を有効にするか、プロファイルに関連付けられているすべての VPC の検証を無効にするかを選択できます。
   - リゾルバーのリバース DNS ルックアップ設定では、有効にするか、無効にするか、VPC にローカルで定義された自動定義されたルールを使用できます (デフォルト)。
   - DNS ファイアウォール障害モード設定では、有効にするか、無効にするか、VPC にローカルで定義された障害モード設定を使用できます (デフォルト)。

   詳細については、「Route 53 プロファイル設定を編集する」を参照してください。
4. プロファイルを 1 つ以上の VPC に関連付ける – プロファイルの使用を開始するには、1 つ以上の VPC に関連付けます。詳細については、「Route 53 プロファイルを VPC に関連付ける」を参照してください。

Route 53 プロファイルの作成

Route 53 プロファイルを作成するには、このトピックのガイダンスに従います。Route 53 コンソールまたは を使用して Route 53 プロファイルを作成するタブを選択します AWS CLI。

- コンソール
- CLI

Console

Route 53 プロファイルを作成するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [プロファイル] を選択します。
3. ナビゲーションバーで、プロファイルを作成するリージョンを選択します。
4. プロファイルの名前を入力し、オプションでタグを追加し、[プロファイルの作成] を選択します。

   これにより、リソースを関連付けることができるデフォルト設定で空のプロファイルが作成されます。リソースをプロファイルに関連付けると、複数の VPC に関連付けて、リゾルバー設定の一部が VPC にどのように適用されるかを編集できます。

CLI

プロファイルを作成するには、次のような AWS CLI コマンドを実行し、 に独自の値を使用しますname。

```
aws route53profiles create-profile --name test
```

以下は、コマンド実行後の出力例を次に示します。

```
{
    "Profile": {
        "Arn": "arn:aws:route53profiles:us-east-1:123456789012:profile/
rp-6ffe47d5example",
        "ClientToken": "2ca1a304-32b3-4f5f-bc4c-EXAMPLE11111",
        "CreationTime": 1710850903.578,
        "Id": "rp-6ffe47d5example",
        "ModificationTime": 1710850903.578,
        "Name": "test",
        "OwnerId": "123456789012",
        "ShareStatus": "NOT_SHARED",
        "Status": "COMPLETE",
        "StatusMessage": "Created Profile"
    }
}
```

プロファイルを異なるリソースに関連付け、プロファイルの VPC 設定を編集するには、以下の手順を参照してください。

トピック

- DNS ファイアウォールルールグループを Route 53 プロファイルに関連付ける
- プライベートホストゾーンを Route 53 プロファイルに関連付ける
- リゾルバールールを Route 53 プロファイルに関連付ける
- インターフェイス VPC エンドポイントを Route 53 プロファイルに関連付ける
- VPC Resolver クエリログ設定を Route 53 プロファイルに関連付ける
- Route 53 プロファイル設定を編集する
- Route 53 プロファイルを VPC に関連付ける

DNS ファイアウォールルールグループを Route 53 プロファイルに関連付ける

ルールグループを作成する手順については「ルールグループおよびルールの作成」を参照し、Route 53 コンソールまたは AWS CLIを使用して DNS Firewall ルールグループを Route 53 プロファイルに関連付けるタブを選択します。

- コンソール
- CLI

Console

DNS ファイアウォールルールグループを関連付けるには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションバーで、プロファイルを作成したリージョンを選択します。
3. ナビゲーションペインで [プロファイル] を選択し、[プロファイル] テーブルで、操作するプロファイルのリンクされた名前を選択します。
4. [<プロファイル名>] ページで、[DNS ファイアウォールルールグループ] タブ、[関連付ける] の順に選択します。

5. [DNS ファイアウォールルールグループ] セクションでは、以前に作成したルールグループを最大 10 個選択できます。10 を超えるルールグループを関連付ける場合は、API を使用します。詳細については、「AssociateResourceToProfile」を参照してください。

   新しいルールグループを作成するには、「ルールグループおよびルールの作成」を参照してください。
6. [次へ] を選択します。
7. [優先度を定義] ページで、事前に割り当てられた優先度番号をクリックし、新しい番号を入力して、ルールグループが処理される順序を設定できます。優先度の許容値は、100～9900です。

   ルールグループは、最も低い数値の優先度設定から順に評価されます。ルールグループの優先度はいつでも変更できます。例えば、処理の順序を変更したり、他のルールグループのためのスペースを確保できます。

   [Submit] を選択してください。
8. 関連付けの進行状況は、[DNS ファイアウォール] ルールグループダイアログボックスの [ステータス] 列に表示されます。

CLI

ルールグループをプロファイルに関連付けるには、次のような AWS CLI コマンドを実行しprofile-id、name、resource-arn、および に独自の値を使用しますpriority。

```
aws route53profiles associate-resource-to-profile --name test-
resource-association --profile-id rp-4987774726example --resource-arn
arn:aws:route53resolver:us-east-1:123456789012:firewall-rule-group/
rslvr-frg-cfe7f72example --resource-properties "{\"priority\": 102}"
```

以下は、コマンド実行後の出力例を次に示します。

```
{
    "ProfileResourceAssociation": {
        "CreationTime": 1710851216.613,
        "Id": "rpr-001913120a7example",
        "ModificationTime": 1710851216.613,
        "Name": "test-resource-association",
        "OwnerId": "123456789012",
        "ProfileId": "rp-4987774726example",
```

```
        "ResourceArn": "arn:aws:route53resolver:us-east-1:123456789012:firewall-
rule-group/rslvr-frg-cfe7f72example",
        "ResourceProperties": "{\"priority\":102}",
        "ResourceType": "FIREWALL_RULE_GROUP",
        "Status": "UPDATING",
        "StatusMessage": "Updating the Profile to DNS Firewall rule group
 association"
    }
}
```

プライベートホストゾーンを Route 53 プロファイルに関連付ける

プライベートホストゾーンの作成方法の解釈については「プライベートホストゾーンの作成」を参照してから、この手順の手順に従ってプライベートホストゾーンをプロファイルに関連付けます。

プライベートホストゾーンを関連付けるには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションバーで、プロファイルを作成したリージョンを選択します。
3. ナビゲーションペインで [プロファイル] を選択し、[プロファイル] テーブルで、操作するプロファイルのリンクされた名前を選択します。
4. [<プロファイル名>] ページで、[プライベートホストゾーン] タブ、[関連付ける] の順に選択します。
5. [プライベートホストゾーンを関連付ける] ページで、以前に作成したプライベートホストゾーンを最大 10 個選択できます。10 を超えるプライベートホストゾーンを関連付ける場合は、API を使用します。詳細については、「AssociateResourceToProfile」を参照してください。

   プライベートホストゾーンを作成するには、「プライベートホストゾーンの作成」を参照してください。
6. [関連付ける] を選択します。
7. 関連付けの進行状況は、[プライベートホストゾーン] ページの [ステータス] 列に表示されます。

リゾルバールールを Route 53 プロファイルに関連付ける

Resolver ルールを作成する手順については、「転送ルールの作成」を参照してから、この手順の手順に従って Resolver ルールをプロファイルに関連付けます。

VPC リゾルバールールを関連付けるには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションバーで、プロファイルを作成したリージョンを選択します。
3. [<プロファイル名>] ページで、[リゾルバールール] タブ、[関連付ける] の順に選択します。
4. [リゾルバールールを関連付ける] ページの [リゾルバールール] テーブルで、以前に作成したリゾルバールールを最大 10 個選択できます。10 を超えるリゾルバールールを関連付けるには、API を使用します。詳細については、「AssociateResourceToProfile」を参照してください。

   リゾルバールールを作成するには、「転送ルールの作成」を参照してください。
5. [関連付ける] を選択します。
6. 関連付けの進行状況は、[Resolver ルール] ページの [ステータス] タブに表示されます。

インターフェイス VPC エンドポイントを Route 53 プロファイルに関連付ける

インターフェイス VPC エンドポイントを作成する方法については、「VPC ユーザーガイド」の「VPC エンドポイントを作成する」を参照してください。次に、この手順の手順に従って VPC エンドポイントをプロファイルに関連付けます。

VPC エンドポイントを関連付けるには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションバーで、プロファイルを作成したリージョンを選択します。
3. [<プロファイル名>] ページで、[VPC エンドポイント] タブ、[関連付ける] の順に選択します。
4. [VPC エンドポイントの関連付け] ページで、VPC エンドポイントテーブルで、以前に作成したエンドポイントを最大 10 個選択できます。10 個を超えるエンドポイントを関連付ける場合は、API を使用します。詳細については、「AssociateResourceToProfile」を参照してください。

   リゾルバールールを作成するには、「転送ルールの作成」を参照してください。
5. [関連付ける] を選択します。
6. 関連付けの進行状況は [VPC エンドポイント] タブの [ステータス] 列に表示されます。

VPC Resolver クエリログ設定を Route 53 プロファイルに関連付ける

VPC Resolver クエリログ記録設定を作成する方法については、「」を参照してからの設定 (VPC Resolver クエリログ記録)、Route 53 コンソールまたは を使用して VPC Resolver 設定を Route 53 プロファイルに関連付けるタブを選択します AWS CLI。

- コンソール
- CLI

Console

クエリログ設定を関連付けるには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションバーで、プロファイルを作成したリージョンを選択します。
3. プロファイル名ページで、リゾルバーのクエリログ設定タブを選択し、関連付けます。
4. クエリログ記録設定の関連付けページで、Resolver クエリログ設定テーブルで、以前に作成した設定を最大 3 つ選択できます。3 つ以上のクエリログ設定を関連付ける場合は、 API を使用します。詳細については、「AssociateResourceToProfile」を参照してください。
5. 新しい VPC Resolver クエリログ記録設定を作成するには、「」を参照してくださいの設定 (VPC Resolver クエリログ記録)。
6. [関連付ける] を選択します。
7. 関連付けの進行状況は、リゾルバーのクエリログ設定タブのステータス列に表示されます。

CLI

次のような AWS CLI コマンドを実行し、 と に独自の値を使用して、クエリログ設定をプロファイルに関連付けることができますnameprofile-idresource-arn。

```
aws route53profiles associate-resource-to-profile --name test-
resource-association --profile-id rp-4987774726example --resource-
arn arn:aws:route53resolver:us-east-1:123456789012:resolver-query-log-
config/rqlc-cfe7f72example
```

以下は、コマンド実行後の出力例を次に示します。

```
{
    "ProfileResourceAssociation": {
        "CreationTime": 1710851226.613,
        "Id": "rpr-001913120b8example",
        "ModificationTime": 1710851226.613,
        "Name": "test-resource-association",
        "OwnerId": "123456789012",
        "ProfileId": "rp-4987774726example",
        "ResourceArn": "arn:aws:route53resolver:us-east-1:123456789012:resolver-
query-log-config/rqlc-cfe7f72example",
        "ResourceType": "RESOLVER_QUERY_LOG_CONFIG",
        "Status": "CREATING",
        "StatusMessage": "Creating rp-4987774726example to rqlc-cfe7f72example
 association"
    }
}
```

Route 53 プロファイル設定を編集する

リソースをプロファイルに関連付けると、デフォルトの VPC 設定を編集して VPC に適用される方法を決定できます。

プロファイル設定を編集するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションバーで、プロファイルを作成したリージョンを選択します。
3. ナビゲーションペインで [プロファイル] を選択し、[プロファイル] テーブルで、操作するプロファイルのリンクされた名前を選択します。
4. [<プロファイル名>] ページで、[設定] タブ、[編集] の順に選択します。
5. [設定を編集] ページで、VPC DNSSEC 設定、リゾルバーのリバース DNS ルックアップ設定、および DNS ファイアウォール障害モード設定の値のいずれかを選択します。

   値の詳細については、「Route 53 プロファイルの設定」を参照してください。
6. [更新] を選択します。

Route 53 プロファイルの設定

Route 53 プロファイル設定を編集するときは、次の値を指定します。

DNSSEC 設定

次のいずれかの値を選択します。

- ローカル VPC DNSSEC 設定を使用 - デフォルト

  このプロファイルに関連付けられているすべての VPC でローカル DNSSEC 検証設定を保持する場合は、このオプションを選択します。

- DNSSEC 検証を有効にする

  このプロファイルに関連付けられているすべての VPC で DNSSEC 検証を有効にする場合は、このオプションを選択します。

- DNSSEC 検証を無効にする

  このプロファイルに関連付けられているすべての VPC で DNSSEC 検証を無効にする場合は、このオプションを選択します。

リゾルバーのリバース DNS ルックアップ設定

次のいずれかの値を選択します。

- 有効化

  関連付けられたすべての VPC でリバース DNS ルックアップの自動定義ルールを作成する場合は、このオプションを選択します。

- 有効になっていません

  関連付けられているすべての VPC でリバース DNS ルックアップの自動定義ルールを作成しない場合は、このオプションを選択します。

- ローカルの自動定義ルールを使用する - デフォルト

  関連付けられた VPC のリバース DNS ルックアップにローカル VPC 設定を使用する場合は、このオプションを選択します。

DNS ファイアウォール障害モード設定

次のいずれかの値を選択します。

- 無効化

関連付けられた VPC の DNS ファイアウォール障害モードを閉じる場合は、このオプションを選択します。このオプションを使用すると、DNS ファイアウォールは適切に評価できないすべてのクエリをブロックします。

- 有効

  関連付けられているすべての VPC で DNS ファイアウォール障害モードを開いたままにする場合は、このオプションを選択します。このオプションを使用すると、DNS ファイアウォールはクエリを適切に評価できない場合にクエリの続行を許可します。

- ローカル障害モード設定を使用する - デフォルト

  ローカル VPC DNS ファイアウォール障害モード設定を使用する場合は、このオプションを選択します。

設定の詳細については、次を参照してください。

- Amazon Route 53 での DNSSEC 検証の有効化
- VPC Resolver でのリバース DNS クエリの転送ルール
- DNS Firewall での VPC の設定

Route 53 プロファイルを VPC に関連付ける

Route 53 プロファイルを VPC に関連付けるには、このトピックのガイダンスに従います。Route 53 コンソールまたは を使用して、Route 53 プロファイルを VPC に関連付けるタブを選択します AWS CLI。

- コンソール
- CLI

Console

VPC を関連付けるには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションバーで、プロファイルを作成したリージョンを選択します。
3. [<プロファイル名>] ページで、[VPC] タブ、[関連付ける] の順に選択します。

4. [VPC を関連付ける] ページで、以前に作成した VPC を最大 10 個選択できます。10 個を超える VPC を関連付ける場合は、API を使用します。詳細については、[AssociateProfile] を参照してください。
5. [関連付ける] を選択します。
6. 関連付けの進行状況は [VPC] ページの [ステータス] 列に表示されます。

CLI

プロファイルを一覧表示するには、次のような AWS CLI コマンドを実行しname、、profile-id、および に独自の値を使用しますresource-id。

```
aws route53profiles associate-profile --name test-association --profile-id rp-4987774726example --resource-id vpc-0af3b96b3example
```

以下は、コマンド実行後の出力例を次に示します。

```
{
    "ProfileResourceAssociation": {
        "CreationTime": 1710851216.613,
        "Id": "rpr-001913120a7example",
        "ModificationTime": 1710851216.613,
        "Name": "test-resource-association",
        "OwnerId": "123456789012",
        "ProfileId": "rp-4987774726example",
        "ResourceArn": "arn:aws:route53resolver:us-east-1:123456789012:firewall-rule-group/rslvr-frg-cfe7f72example",
        "ResourceProperties": "{\"priority\":102}",
        "ResourceType": "FIREWALL_RULE_GROUP",
        "Status": "UPDATING",
        "StatusMessage": "Updating the Profile to DNS Firewall rule group association"
    }
}
```

Amazon Route 53 プロファイルの表示と更新

Route 53 プロファイルを表示および編集するには、コンソールタブを選択します。所有している、共有されている、または共有されているプロファイルを一覧表示 AWS CLI するために使用する CLI タブを選択します。

- コンソール
- CLI

Console

Route 53 プロファイルの表示と更新

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [プロファイル] を選択します。
3. 表示または編集するプロファイルの名前の横にあるボタンを選択します。
4. [<プロファイル名>] ページで、現在関連付けられている DNS リソースを表示し、新しいリソースを関連付け、タグと VPC 設定を編集できます。

CLI

プロファイルを一覧表示するには、次のような AWS CLI コマンドを実行します。

```
aws route53profiles list-profiles
```

以下は、コマンド実行後の出力例を次に示します。

```
{
    "ProfileSummaries": [
        {
            "Arn": "arn:aws:route53profiles:us-east-1:123456789012:profile/
rp-4987774726example",
            "Id": "rp-4987774726example",
            "Name": "test",
            "ShareStatus": "NOT_SHARED"
        }
    ]
}
```

プロファイルが関連付けられている特定の VPS に関する情報を取得するには、次のような AWS CLI コマンドを実行し、profile-association-id に独自の値を使用します。

```
aws route53profiles get-profile-association --profile-association-id
rpassoc-489ce212fexample
```

以下は、コマンド実行後の出力例を次に示します。

```
   "ProfileAssociation": {
        "CreationTime": 1709338817.148,
        "Id": "rrpassoc-489ce212fexample",
        "ModificationTime": 1709338974.772,
        "Name": "test-association",
        "OwnerId": "123456789012",
        "ProfileId": "rp-4987774726example",
        "ResourceId": "vpc-0af3b96b3example",
        "Status": "COMPLETE",
        "StatusMessage": "Created Profile Association"
    }   ]
}
```

Amazon Route 53 プロファイルの削除

Route 53 コンソールを使用して Route 53 プロファイルを削除するタブ、または を選択します AWS CLI。

- コンソール
- CLI

Console

Route 53 プロファイルを削除するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [プロファイル] を選択します。
3. 削除するプロファイル名の横にあるボタンを選択して、[削除] を選択します。

> **Important**
>
> VPC に関連付けられているプロファイルは削除できません。さらに、プロファイルが別の と共有されている場合 AWS アカウント、プロファイル設定が関連付けられている VPCs はそれらの設定を失います。

4. [<プロファイル名> を削除] ダイアログに「**confirm**」と入力し、[削除] を選択します。

CLI

> **Important**
>
> VPC に関連付けられているプロファイルは削除できません。さらに、プロファイルが別の と共有されている場合 AWS アカウント、プロファイル設定が関連付けられている VPCs はそれらの設定を失います。

プロファイルを削除するには、次のような AWS CLI コマンドを実行し、 に独自の値を使用しますprofile-id。

```
aws route53profiles delete-profile --profile-id rp-6ffe47d5example
```

以下は、コマンド実行後の出力例を次に示します。

```
{
    "Profile": {
        "Arn": "arn:aws:route53profiles:us-east-1:123456789012:profile/
rp-6ffe47d5example",
        "ClientToken": "0a15fec0-05d9-4f78-bec0-EXAMPLE11111",
        "CreationTime": 1710850903.578,
        "Id": "rp-6ffe47d5example",
        "ModificationTime": 1710850903.578,
        "Name": "test",
        "OwnerId": "123456789012",
        "ShareStatus": "NOT_SHARED",
        "Status": "DELETED",
        "StatusMessage": "Deleted Profile"
    }
}
```

Amazon Route 53 プロファイルに関連付けられた Route 53 リソースの表示と更新

コンソールタブを選択して Route 53 プロファイルリソースの関連付けを表示し、オプションで DNS ファイアウォールルールグループの優先度を編集します。リソースの関連付けを一覧表示 AWS CLI

し、DNS Firewall ルールグループの優先度の更新例を表示するには、使用する CLI タブを選択します。

- コンソール
- CLI

Console

プロファイルに関連付けられたリソースを表示および更新するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [プロファイル] を選択します。
3. ナビゲーションバーで、プロファイルを作成したリージョンを選択します。
4. リソースの関連付けを表示または編集するプロファイルの名前の横にあるボタンを選択します。
5. [<プロファイル名>] ページで、[DNS ファイアウォールルールグループ]、[プライベートホストゾーン]、または [Resolver ルール]、または [VPC エンドポイント] のいずれかを表示または編集するリソースのタブを選択します。
6. リソースのタブページで、関連するリソースの名前、ARN、ステータスを表示できます。歯車アイコンを選択して、リソーステーブルに表示される内容を調整することもできます。

   [DNS ファイアウォールルールグループ] タブページで、ルールグループの優先度エントリを選択し、それをより小さい数または大きい数に編集することもできます。ルールグループは、数が最も小さい優先度番号から数が最も大きい優先度番号までの順序で評価されます。

CLI

プロファイルに関連付けられたリソースを一覧表示するには、次のような AWS CLI コマンドを実行し、 に独自の値を使用しますprofile-id。

```
aws route53profiles list-profile-resource-associations --profile-id
rp-4987774726example
```

以下は、コマンド実行後の出力例を次に示します。

```
{
    "ProfileResourceAssociations": [
```

```
        {
            "CreationTime": 1710851216.613,
            "Id": "rpr-001913120a7example",
            "ModificationTime": 1710851216.613,
            "Name": "test-resource-association",
            "OwnerId": "123456789012",
            "ProfileId": "rp-4987774726example",
            "ResourceArn": "arn:aws:route53resolver:us-east-1:123456789012:firewall-
rule-group/rslvr-frg-cfe7f72example",
            "ResourceProperties": "{\"priority\":102}",
            "ResourceType": "FIREWALL_RULE_GROUP",
            "Status": "COMPLETE",
            "StatusMessage": "Completed creation of Profile to DNS Firewall rule
 group association"
        }
    ]
}
```

プロファイルに関連付けられた DNS Firewall ルールグループの優先度を更新するには、次のような AWS CLI コマンドを実行し、 に独自の値を使用し、 profile-resource-association-idと に独自の値を使用します--resource-properties。

```
aws route53profiles update-profile-resource-association --profile-
resource-association-id rpr-001913120a7example --resource-properties
"{\"priority\": 105}"
```

以下は、コマンド実行後の出力例を次に示します。

```
{
    "ProfileResourceAssociation": {
        "CreationTime": 1710851216.613,
        "Id": "rpr-001913120a7example",
        "ModificationTime": 1710852303.798,
        "Name": "test-resource-association",
        "OwnerId": "123456789012",
        "ProfileId": "rp-4987774726example",
        "ResourceArn": "arn:aws:route53resolver:us-east-1:123456789012:firewall-
rule-group/rslvr-frg-cfe7f72example",
        "ResourceProperties": "{\"priority\":105}",
        "ResourceType": "FIREWALL_RULE_GROUP",
        "Status": "UPDATING",
        "StatusMessage": "Updating the Profile to DNS Firewall rule group
 association"
```

```
    }
}
```

Amazon Route 53 プロファイルからのリソースの関連付け解除

プロファイルを削除する前に、プロファイルからすべてのリソースの関連付けを解除する必要があります。

Route 53 プロファイルに関連付けられたリソースの関連付けを解除するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [プロファイル] を選択します。
3. ナビゲーションバーで、リソースの関連付けを解除するプロファイルが作成されたリージョンを選択します。
4. リソースの関連付けを解除するプロファイルの名前の横にあるボタンを選択します。
5. プロファイル名ページで、削除するリソースのタブを選択します。、DNS Firewall ルールグループ、プライベートホストゾーン、リゾルバークエリログ記録、リゾルバールール、または VPC エンドポイントのいずれかです。
6. リソースのタブページで、関連付けを解除するリソースを選択し、[関連付けを解除] を選択します。
7. [リソースの関連付けを解除] ダイアログに「**confirm**」と入力し、[関連付けを解除] を選択します。

Amazon Route 53 プロファイルに関連付けられた VPC の表示

コンソールタブを選択して、Route 53 プロファイルと VPC の関連付けを表示および編集します。プロファイルから VPC への関連付けを一覧表示したり、特定の関連付けに関する情報を取得 AWS CLI するために使用する CLI タブを選択します。

- コンソール
- CLI

Console

プロファイルに関連付けられた VPC を表示するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [プロファイル] を選択します。
3. ナビゲーションバーで、プロファイルを作成したリージョンを選択します。
4. 関連付けられた VPC を表示するプロファイルの名前の横にあるボタンを選択します。
5. [<プロファイル名>] ページで [VPC] タブを選択します。
6. VPC のタブページで、関連する VPC の名前、ARN、ステータスを表示できます。

CLI

プロファイルが関連付けられている VPCs を一覧表示するには、次のような AWS CLI コマンドを実行します。

```
aws route53profiles list-profile-associations
```

以下は、コマンド実行後の出力例を次に示します。

```
{
    "ProfileAssociations": [
        {
            "CreationTime": 1709338817.148,
            "Id": "rpassoc-489ce212fexample",{
    "ProfileAssociations": [
        {
            "CreationTime": 1709338817.148,
            "Id": "rpassoc-489ce212fexample",
            "ModificationTime": 1709338974.772,
            "Name": "test-association",
            "OwnerId": "123456789012",
            "ProfileId": "rp-4987774726example",
            "ResourceId": "vpc-0af3b96b3example",
            "Status": "COMPLETE",
            "StatusMessage": "Created Profile Association"
        }
    ]
}
```

```
            "ModificationTime": 1709338974.772,
            "Name": "test-association",
            "OwnerId": "123456789012",
            "ProfileId": "rp-4987774726example",
            "ResourceId": "vpc-0af3b96b3example",
            "Status": "COMPLETE",
            "StatusMessage": "Created Profile Association"
        }
    ]
}
```

プロファイルが関連付けられている特定の VPS に関する情報を取得するには、次のような AWS CLI コマンドを実行し、profile-association-id に独自の値を使用します。

```
aws route53profiles get-profile-association --profile-association-id
rpassoc-489ce212fexample
```

以下は、コマンド実行後の出力例を次に示します。

```
   "ProfileAssociation": {
        "CreationTime": 1709338817.148,
        "Id": "rrpassoc-489ce212fexample",
        "ModificationTime": 1709338974.772,
        "Name": "test-association",
        "OwnerId": "123456789012",
        "ProfileId": "rp-4987774726example",
        "ResourceId": "vpc-0af3b96b3example",
        "Status": "COMPLETE",
        "StatusMessage": "Created Profile Association"
    }   ]
}
```

Amazon Route 53 プロファイルからの VPC の関連付け解除

Route 53 コンソールまたは を使用して、VPC から Route 53 プロファイルの関連付けを解除するタブを選択します AWS CLI。

- コンソール
- CLI

Console

Route 53 プロファイルに関連付けられた VPC の関連付けを解除するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [プロファイル] を選択します。
3. ナビゲーションバーで、VPC の関連付けを解除するプロファイルが作成されたリージョンを選択します。
4. VPC の関連付けを解除するプロファイルの名前の横にあるボタンを選択します。
5. [<プロファイル名>] ページで [VPC] タブを選択します。
6. リソースの VPC タブページで、関連付けを解除する VPC を選択し、[関連付けを解除] を選択します。
7. [リソースの関連付けを解除] ダイアログに「**confirm**」と入力し、[関連付けを解除] を選択します。

CLI

プロファイルと VPC の関連付けを解除するには、次のような AWS CLI コマンドを実行し、`profile-id`と に独自の値を使用します`--resource-id`。

```
aws route53profiles disassociate-profile --profile-id
rp-4987774726example --resource-id vpc-0af3b96b3example
```

以下は、コマンド実行後の出力例を次に示します。

```
"ProfileAssociation": {
        "CreationTime": 1710851336.527,
        "Id": "rpassoc-489ce212fexample",
        "ModificationTime": 1710851401.362,
        "Name": "test-association",
        "OwnerId": "123456789012",
        "ProfileId": "rp-4987774726example",
        "ResourceId": "vpc-0af3b96b3example",
        "Status": "DELETING",
        "StatusMessage": "Deleting Profile Association"
    }
```

共有 Route 53 プロファイルの使用

プロファイルは、次の方法で他のアカウントと共有できます。

- 読み取り専用アクセス許可を付与します。つまり、他のアカウントはプロファイルを VPC に関連付けることができます。この場合、すべての DNS リソースと設定は、関連付けられた VPC で有効になります。
- 管理者アクセス許可の付与。この場合、共有プロファイルを持つアカウントはプロファイルを変更し、VPC に関連付けることができます。所有者は、コンシューマーアカウントで実行できるアクションを指定するために使用できる、カスタマー管理アクセス許可を作成することもできます。詳細については、「AWS RAM ユーザーガイド」の「カスタマー管理アクセス許可」を参照してください。

Amazon Route 53 Profile は AWS Resource Access Manager (AWS RAM) と統合してリソース共有を有効にします。 AWS RAM は、一部の Route 53 リソースを他の AWS アカウント または と共有できるようにするサービスです AWS Organizations。では AWS RAM、リソース共有を作成して、所有しているリソースを共有します。リソース共有は、共有するリソースと、それらを共有するコンシューマーを指定します。コンシューマーには以下が含まれます。

- 固有 AWS アカウント
- の組織内の組織単位 AWS Organizations
- の組織全体 AWS Organizations

詳細については AWS RAM、AWS RAM 「 ユーザーガイド」を参照してください。

このトピックでは、所有しているリソースの共有方法と、共有されているリソースの使用方法を説明します。

内容

- Route 53 プロファイルを共有するためのアクセス許可の付与
- Route 53 プロファイルを共有するための前提条件
- Route 53 プロファイルの共有
- 共有 Route 53 プロファイルの共有解除
- 共有 Route 53 プロファイルの特定
- 共有 Route 53 プロファイルの責任とアクセス許可

- 請求と使用量測定
- インスタンスクォータ

Route 53 プロファイルを共有するためのアクセス許可の付与

IAM プリンシパルがプロファイルを共有するには、最小限のアクセス許可のセットが必要です。AmazonRoute53ProfilesFullAccess マネージド IAM ポリシーを使用して、IAM プリンシパルが共有プロファイルを共有して使用するために必要なアクセス許可を持っていることを確認することをお勧めします。

カスタム IAM ポリシーを使用する場合は、route53profiles:GetProfilePolicy および route53profiles:PutProfilePolicy アクションが必要です。これらはアクセス許可のみの IAM アクションです。IAM プリンシパルにこれらのアクセス許可が付与されていない場合、 AWS RAM サービスを使用してプロファイルを共有しようとするとエラーが発生します。

Route 53 プロファイルを共有するための前提条件

- Route 53 プロファイルを共有するには、 で所有する必要があります AWS アカウント。つまり、自分のアカウントにそのリソースが割り当てられているか、プロビジョニングされている必要があります。自身が共有を受けている Route 53 プロファイルは共有できません。
- AWS Organizationsの組織や組織単位と Route 53 プロファイルを共有するには、 AWS Organizationsとの共有を有効にする必要があります。詳細については、「AWS RAM ユーザーガイド」の「Enable Sharing with AWS Organizations」を参照してください。

Route 53 プロファイルの共有

所有しているプロファイルを別のプロファイルと共有すると AWS アカウント、プロファイルの DNS 関連の設定を VPCs に適用できるようになります。これにより、管理オーバーヘッドを最小限に抑えながら、数千の VPC に均一な DNS 設定を簡単に適用できます。

Route 53 プロファイルを共有するには、リソース共有に追加する必要があります。リソース共有とは、 AWS アカウント間で自身のリソースを共有するための AWS RAM リソースです。リソース共有では、共有対象のリソースと、共有先のコンシューマーを指定します。Route 53 コンソールを使用して Route 53 プロファイルを共有すると、既存のリソース共有に追加されます。Route 53 プロファイルを新しいリソース共有に追加するには、まず AWS RAM コンソールを使用してリソース共有を作成する必要があります。

の組織に属 AWS Organizations していて、組織内での共有が有効になっている場合、組織内のコンシューマーには共有 Route 53 プロファイルへのアクセスが自動的に付与されます。それ以外の場合、コンシューマーはリソース共有への参加の招待を受け取り、その招待を受け入れた後で、共有 Route 53 プロファイルへのアクセス許可が付与されます。

Route 53 コンソールで所有している Route 53 プロファイルの共有を開始し、 AWS RAM コンソールで続行できます。

Route 53 コンソールを使用して、自身が所有する Route 53 プロファイルを共有するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [プロファイル] を選択します。
3. 共有するプロファイルを選択し、[プロファイルの詳細] ページで [プロファイルの共有] を選択します。
4. AWS RAM コンソールに移動し、「 AWS RAM ユーザーガイド」の「リソース共有の作成」のステップを実行できます。
5. プロファイルが共有されている場合、[プロファイル] テーブルにはテキストの [自分と共有] が含まれます。

   プロファイルを共有すると、[プロファイル] テーブルに [共有] として一覧表示されます。

AWS RAM コンソールを使用して所有している Route 53 プロファイルを共有するには

「AWS RAM ユーザーガイド」の「リソース共有の作成」を参照してください。

を使用して所有している Route 53 プロファイルを共有するには AWS CLI

create-resource-share コマンドを使用します。

共有 Route 53 プロファイルの共有解除

プロファイルを共有解除すると、そのプロファイルの設定が関連付けられている VPC は失われ、デフォルトで VPC 固有の設定になります。

自身が所有する共有 Route 53 プロファイルを共有解除するには、それをリソース共有から削除する必要があります。この操作は、Route 53 コンソール、 AWS RAM コンソール、または AWS CLIを使用して行うことができます。

Route 53 コンソールを使用して、自身が所有する共有 Route 53 プロファイルを共有解除するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [プロファイル] を選択します。
3. 共有解除するプロファイルのリンク名を選択し、[<プロファイル名>] ページで [共有の管理] を選択します。
4. AWS RAM コンソールに移動し、「 AWS RAM ユーザーガイド」の「リソース共有の更新」の手順を実行できます。

AWS RAM コンソールを使用して、所有している共有 Route 53 プロファイルの共有を解除するには

「AWS RAM ユーザーガイド」の「リソース共有の更新」を参照してください。

を使用して、所有している共有 Route 53 プロファイルの共有を解除するには AWS CLI

disassociate-resource-share コマンドを使用します。

共有 Route 53 プロファイルの特定

所有者とコンシューマーは、Route 53 コンソールまたは AWS CLIを使用して、共有 Route 53 プロファイルを特定できます。

Route 53 コンソールを使用して共有、Route 53 プロファイルを識別するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [プロファイル] を選択します。
3. プロファイルが共有されている場合、[プロファイル] テーブルにはテキストの [自分と共有] が含まれます。

   プロファイルを共有すると、[プロファイル] テーブルに [共有] として一覧表示されます。

を使用して共有 Route 53 プロファイルを識別するには AWS CLI

get-profile コマンドまたは list-profile コマンドを使用します。コマンドは、自身が所有する Route 53 プロファイルと Route 53 プロファイルの共有ステータスに関する情報を返します。

共有 Route 53 プロファイルの責任とアクセス許可

所有者のアクセス許可

プロファイル所有者は、コンシューマーアカウントによって行われたリソースの関連付けを含むプロファイルリソースの関連付けを表示、管理、削除できます。所有者は、所有する VPC 関連付けを表示および削除することができます。さらに、プロファイル所有者のみが自身が所有するプロファイルを削除できます。これにより、プロファイルのすべてのリソース関連付けも自動的に削除されます。

> **Note**
>
> プロファイルが共有されているアカウントのリソースを関連付けるには、デフォルトのアクセス許可に加えて `route53profiles:AssociateResourceToProfile` アクションを含むカスタム管理アクセス許可を作成する必要があります。これは、デフォルトのポリシー `AWSRAMPermissionRoute53ProfileAllowAssociation` には含まれていないためです。

コンシューマーのアクセス許可

共有プロファイルのコンシューマーに対するデフォルトのアクセス許可は、読み取り専用です。読み取り専用アクセス許可では、関連付けられたリソースを表示して VPC に関連付けることはできますが、リソースの関連付けを管理することはできません。

所有者は、 AWS RAM コンソールでカスタマー管理アクセス許可を作成することもできます。詳細については、「AWS RAM ユーザーガイド」の「Creating and using customer managed permission」を参照してください。

請求と使用量測定

Route 53 プロファイルは、VPC 関連付けの数に基づいて請求されます。プロファイル所有者は、お客様ごとの VPC 関連付けの請求を担当します。

インスタンスクォータ

プロファイル所有者とコンシューマーは同じクォータを共有します。リージョンのアカウントあたりの Route 53 プロファイルの数は除きます。詳細については、Route 53 プロファイルのクォータ を参照してください。

Amazon Route 53 on Outposts とは

AWS Outposts は、 AWS インフラストラクチャ、サービス、APIs、ツールをお客様の施設に拡張するフルマネージドサービスです。を使用すると AWS Outposts、 と同じプログラミングインターフェイスを使用して、オンプレミスのワークロードで AWS サービスを実行できます AWS リージョン。詳細については、「 とは」を参照してください AWS Outposts。 AWS Outposts ユーザーガイドの「」を参照してください。

Route 53 on Outposts には 2 つの機能があります。

- からのすべての DNS クエリをキャッシュする VPC リゾルバー AWS Outposts。
- インバウンドおよびアウトバウンドエンドポイントをデプロイする際の Outpost とオンプレミス DNS リゾルバーの間のハイブリッド接続。

詳細については、「Route 53 VPC Resolver とは」を参照してください。

さらに、Outposts の Route 53 の「VPC リゾルバー」は、最も近い にラウンドトリップするのではなく、Outpost 内でクエリを解決できるようにすることで、ネットワークのレイテンシーを軽減します AWS リージョン。

> **Note**
>
> Route 53 on Outposts と互換性のないバージョンの AWS Outposts ラックがある場合、AWS アカウントチームに通知され、アップグレードについて連絡します AWS Outposts。

アーキテクチャの概要

Route 53 on Outposts は分散 DNS アーキテクチャを実装します。

- DNS レコードとホストゾーンは、 AWS リージョンの Amazon Route 53 で管理されたままになります。
- リゾルバー機能はローカルクエリ処理のためにラックに拡張されます AWS Outposts

この設計は、一元化された DNS レコード管理を維持しながら、クエリのパフォーマンスと可用性を最適化します。DNS レコードは、 AWS Outposts ラックのローカルではなく、 AWS リージョンに引き続き保存されます。

Amazon Route 53 on Outposts の機能

次の表はRoute 53 on Outposts 機能と Amazon Route 53 の機能の違いを示しています。

Route 53 on Outposts と Route 53 の比較

Route 53 の機能	第 1 世代の Route 53 AWS Outposts	第 2 世代の Route 53 AWS Outposts
VPC リゾルバー	サポート - VPC Resolver は、Outpost ラック、 のピア接続された VPC、 AWS リージョンおよびパブリックにアクセス可能なホスト名でホストされているアプリケーションのレコードのローカルキャッシュを維持します。	サポート - VPC Resolver は、Outpost ラック、 のピア接続された VPC、 AWS リージョンおよびパブリックにアクセス可能なホスト名でホストされているアプリケーションのレコードのローカルキャッシュを維持します。
ヘルスチェック	サポートされていない - ヘルスチェックは から計算され、報告されます AWS リージョン。Outpost がクラウドから切断されると、エンドポイントはフェールオープンになり、バックアップにフェイルオーバーできなくなります。	サポートされていない - ヘルスチェックは から計算され、報告されます AWS リージョン。Outpost がクラウドから切断されると、エンドポイントはフェールオープンになり、バックアップにフェイルオーバーできなくなります。
Resolver エンドポイント	サポート - Outpost ラックのリゾルバーエンドポイントにより、DNS クエリをオンプレミスの DNS サーバーに転送および受信できます。 エンドポイントで使用できるのは IPv4 エンドポイントタイプだけです。	サポート外。
リゾルバー DNS ファイアウォール	サポート外。	サポート外。
トラフィックフロー	サポート外。	サポート外。

AWS Outposts が VPC から切断された場合の VPC リゾルバーの動作

AWS Outposts が から切断されている場合 AWS リージョン、Resolver on Outpost は次のように動作します。

- コントロールプレーンは変更できません。
- ヘルスチェックと DNS フェイルオーバー機能は使用できません。
- Outposts でローカルにホストされているリソースへの DNS クエリは解決されますが、Outpost が切断状態のときにリソースの IP アドレスが更新されると応答が古くなることがあります。
- リージョン内の VPC でホストされているリソースの DNS クエリは解決可能です。ただし、 AWS リージョン への Outpost 接続が回復するまでリソースにはアクセスできません。
- パブリック DNS リソースの DNS クエリは、Outpost の VPC Resolver キャッシュで使用可能な場合に解決できます。

での VPC Resolver の開始方法 AWS Outposts

AWS Outposts ラックを注文して配送したら、ガイドの「 を作成する AWS Outposts」の説明に従ってAWS Outposts 、Outpost でリゾルバーを設定できます。

第 2 世代 AWS Outposts

第 2 世代の場合 AWS Outposts、VPC Resolver はデフォルトで有効になっており、それを使用するためのアクションを実行する必要はありません。VPC Resolver にオプトインまたはオプトアウトするには、 にお問い合わせくださいAWS サポート。

第 1 世代 AWS Outposts

> **Important**
>
> Outpost のリゾルバーは、 AWS Outposts ラックを所有する AWS アカウントによってのみ作成できます。 AWS Outposts ラックが他のアカウントと共有されている場合、それらのアカウントは共有ラックに Outpost でリゾルバーを作成できません。

API を使用して Route 53 on Outposts を管理することもできます。詳細については、「Resolver on Outpost のアクション」を参照してください。

> **Important**
>
> で VPC Resolver キャッシュを作成するまでに最大 30 ~ 150 分かかる場合があります AWS Outposts。

AWS Outposts ラックを配送したら、Route 53 on Outposts にオプトインできます。

Resolver on Outpost を設定するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. 左側のナビゲーションペインで [Resolver] を展開し、[Outposts] にナビゲートします。
3. ナビゲーションバーで、 AWS Outposts があるリージョンを選択します。
4. Outpost のリゾルバーページで、VPC リゾルバーの作成を選択します。
5. VPC リゾルバーの作成ページで、次の操作を行います。
   - VPC リゾルバー AWS Outposts を作成する AWS Outpostsを選択します。
   - VPC Resolver 名テキストボックスに VPC Resolver の名前を入力します。
   - VPC Resolver の推奨インスタンスタイプに Amazon EC2 インスタンスを入力したら、いずれかを選択します。

     インスタンスタイプの詳細については、「第 1 世代の Resolver のクォータ AWS Outposts」を参照してください。
   - インスタンス数 で、VPC VPC リゾルバーの Elastic Interface インスタンスの数を選択します。デフォルト値は 4 です。

     に VPC Resolver をサポートするインスタンスタイプ AWS Outposts がない場合、VPC Resolver を作成することはできません。
6. VPC リゾルバーの作成を選択します。

   VPC リゾルバーの作成は、Outpost のリゾルバーページでモニタリングできます。

インバウンドエンドポイントの作成 (第 1 世代 AWS Outposts のみ)

> **Note**
>
> このコンテンツは第 1 世代 AWS Outposts にのみ適用されます。第 2 世代には適用されません AWS Outposts。

Resolver on Outpost を作成した後、インバウンドエンドポイントとアウトバウンドエンドポイントの両方を追加して、オンプレミスネットワークと送受信される DNS クエリを解決できます。

Resolver on Outpost のインバウンドエンドポイントを設定するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. 左側のナビゲーションペインで [Resolver] を展開し、[Outposts] にナビゲートします。
3. ナビゲーションバーで、 AWS Outposts があるリージョンを選択します。
4. 運用状態にある VPC リゾルバーの横にあるチェックボックスをオンにし、詳細の表示を選択します。
5. [インバウンドエンドポイント] テーブルで [インバウンドエンドポイントを作成] を選択します。
6. [インバウンドエンドポイントの作成] ページで、適切な値を入力します。詳細については、「Outpost のインバウンドエンドポイントを作成または編集するときに指定する値」を参照してください。
7. エンドポイントの作成 を選択します。

Outpost のインバウンドエンドポイントを作成または編集するときに指定する値

インバウンドエンドポイントを作成または編集する場合、以下の値を指定します。

Outpost ID

AWS Outposts VPC で VPC リゾルバーのエンドポイントを作成する場合、これは AWS Outposts ID です。

エンドポイント名

わかりやすい名前にすると、ダッシュボードでインバウンドエンドポイントを見つけやすくなります。

region-name リージョンの VPC

ネットワークからのすべてのインバウンド DNS クエリは、VPC リゾルバーへの途中でこの VPC を通過します。

このエンドポイントのセキュリティグループ

このインバウンドエンドポイントへのアクセスを制御するために使用する 1 つ以上のセキュリティグループの ID です。指定したセキュリティグループには、1 つ以上のインバウンドルールを含める必要があります。インバウンドルールでは、ポート 53 での TCP および UDP アクセスを許可する必要があります。エンドポイントの作成が完了した後は、この値を変更できません。

詳細については、Amazon VPC ユーザーガイドの「VPC のセキュリティグループ」を参照してください。

IP アドレス

インバウンドエンドポイントに割り当てる IP アドレス。冗長性を確保するため、少なくとも 2 つの IP アドレスを指定する必要があります。次の点に注意してください。

IP アドレスと Amazon VPC Elastic Network Interface

指定したアベイラビリティーゾーン、サブネット、IP アドレスの組み合わせごとに、VPC Resolver は Amazon VPC Elastic Network Interface を作成します。エンドポイントの IP アドレスあたりの 1 秒あたりの DNS クエリの現在の最大数については、「Route 53 VPC リゾルバーのクォータ」を参照してください。各 Elastic Network Interface の料金については、Amazon Route 53 料金ページの「Amazon Route 53」を参照してください。

> **Note**
>
> Resolver エンドポイントはプライベート IP アドレスを持ちます。これらの IP アドレスは、エンドポイントの存続期間中に変更されることはありません。

IP アドレスごとに、以下の値を指定します。各 IP アドレスは、[VPC in the region-name Region (region-name リージョンの VPC)] で指定した VPC のアベイラビリティーゾーンに存在する必要があります。

アベイラビリティーゾーン

VPC に向かう途中で DNS クエリを通過させるアベイラビリティーゾーンです。指定したアベイラビリティーゾーンには、サブネットが設定されている必要があります。

サブネット

DNS クエリの転送先となる IP アドレスを含むサブネット。サブネットには利用可能な IP アドレスが必要です。

IPv4 アドレスのサブネットを指定します。IPv6 はサポートされていません。

IP アドレス

DNS クエリの転送先となる IP アドレス。

VPC Resolver で、指定したサブネットで使用可能な IP アドレスの中から IP アドレスを選択するか、自分で IP アドレスを指定するかを選択します。

IP アドレスを自分で指定する場合は、IPv4 アドレスを入力します。IPv6 はサポートされていません。

タグ

1 つ以上のキーと対応する値を指定します。例えば、[Key (キー)] に Cost center を、[Value (値)] には 456 を指定します。

これらは、 が請求書を整理するために AWS Billing and Cost Management 提供するタグです AWS 。タグは他の目的でも使用できます。タグを使ったコスト配分の詳細については、AWS Billing ユーザーガイドのコスト配分タグの使用を参照してください。

アウトバウンドエンドポイントの作成 (第 1 世代 AWS Outposts のみ)

> **Note**
>
> このコンテンツは第 1 世代 AWS Outposts にのみ適用されます。第 2 世代には適用されません AWS Outposts。

VPC Resolver をオプトインして設定したら、インバウンドエンドポイントとアウトバウンドエンドポイントの両方を追加して、DNS クエリをオンプレミスネットワークに解決することもできます。

> **Note**
>
> アウトバウンドエンドポイントを設定すると、VPC Resolver は DNS レスポンスをキャッシュするため、Outpost がリージョンから切断された場合でもクエリを解決できます。このキャッシュを維持すると、オンプレミスリゾルバーへの DNS リクエストが増加する可能性があります。

Resolver on Outpost のアウトバウンドエンドポイントを設定するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. 左側のナビゲーションペインで [Resolver] を展開し、[Outposts] にナビゲートします。
3. ナビゲーションバーで、 AWS Outposts があるリージョンを選択します。
4. 運用状態にある VPC リゾルバーの横にあるチェックマークを選択し、詳細の表示を選択します。
5. [アウトバウンドエンドポイント] テーブルで [アウトバウンドエンドポイントを作成] を選択します。
6. [アウトバウンドエンドポイントの作成] ページで、適切な値を入力します。詳細については、「でアウトバウンドエンドポイントを作成または編集するときに指定する値 AWS Outposts」を参照してください。
7. エンドポイントの作成 を選択します。

でアウトバウンドエンドポイントを作成または編集するときに指定する値 AWS Outposts

アウトバウンドエンドポイントを作成または編集する場合、以下の値を指定します。

Outpost ID

AWS Outposts VPC で VPC リゾルバーのエンドポイントを作成する場合、これは AWS Outposts ID です。

エンドポイント名

わかりやすい名前にすると、ダッシュボードでアウトバウンドエンドポイントを見つけやすくなります。

region-name リージョンの VPC

VPC からのすべてのアウトバウンド DNS クエリは、ネットワークに向かう途中でこの VPC を通過します。

このエンドポイントのセキュリティグループ

この VPC へのアクセスを制御するために使用する 1 つ以上のセキュリティグループの ID です。指定したセキュリティグループには、1 つ以上のアウトバウンドルールを含める必要があります。アウトバウンドルールでは、ネットワークで DNS クエリに使用するポートで TCP および UDP アクセスを許可する必要があります。エンドポイントの作成が完了した後は、この値を変更できません。

詳細については、Amazon VPC ユーザーガイドの「VPC のセキュリティグループ」を参照してください。

IP アドレス

アウトバウンドエンドポイントに割り当てる IP アドレス。冗長性を確保するため、少なくとも 2 つの IP アドレスを指定する必要があります。次の点に注意してください。

IP アドレスと Amazon VPC Elastic Network Interface

指定したアベイラビリティーゾーン、サブネット、IP アドレスの組み合わせごとに、VPC Resolver は Amazon VPC Elastic Network Interface を作成します。エンドポイントの IP アドレスあたりの 1 秒あたりの DNS クエリの現在の最大数については、「Route 53 VPC リゾルバーのクォータ」を参照してください。各 Elastic Network Interface の料金については、Amazon Route 53 料金ページの「Amazon Route 53」を参照してください。

> **Note**
>
> Resolver エンドポイントはプライベート IP アドレスを持ちます。これらの IP アドレスは、エンドポイントの存続期間中に変更されることはありません。

IP アドレスごとに、以下の値を指定します。各 IP アドレスは、[VPC in the region-name Region (region-name リージョンの VPC)] で指定した VPC のアベイラビリティーゾーンに存在する必要があります。

アベイラビリティーゾーン

VPC からの途中で DNS クエリを通過させるアベイラビリティーゾーンです。指定するアベイラビリティーゾーンにはサブネットを設定する必要があります。

サブネット

DNS クエリの転送元となる IP アドレスを含むサブネット。サブネットには使用可能な IP アドレスが必要です。

IPv4 アドレスのサブネットを指定します。IPv6 はサポートされていません。

IP アドレス

アウトバウンドエンドポイントに割り当てる IP アドレス。

VPC Resolver で、指定したサブネットで使用可能な IP アドレスの中から IP アドレスを選択するか、自分で IP アドレスを指定するかを選択します。

IP アドレスを自分で指定する場合は、IPv4 アドレスを入力します。IPv6 はサポートされていません。

タグ

1 つ以上のキーと対応する値を指定します。例えば、[Key (キー)] に Cost center を、[Value (値)] には 456 を指定します。

これらは、 が請求書を整理するために AWS Billing and Cost Management 提供するタグです AWS 。他の目的でタグを使用することもできます。タグを使ったコスト配分の詳細については、AWS Billing ユーザーガイドのコスト配分タグの使用を参照してください。

アウトバウンドエンドポイントの転送ルールの作成

アウトバウンドエンドポイントの転送ルールを作成することもできます。詳細については、転送ルールを作成して 1 つ以上の VPC に関連付けるには を参照してください。

Resolver on Outpost の管理

Resolver on Outpost の管理方法は、 AWS Outposts 世代によって異なります。

- 第 1 世代 AWS Outpostsでは、リゾルバーを編集、表示、削除できます。
- 第 2 世代では AWS Outposts、Resolver を編集または削除することはできません。表示のみ可能です。
- 第 2 世代のリゾルバーを使用しない場合は AWS Outposts、 AWS サポート に連絡してオプトアウトする必要があります。

- Resolver が第 2 世代で失敗した場合 AWS Outposts、 は問題を解決するためにお客様 AWS に連絡します。

トピック

- Outpost でのリゾルバーの編集 (第 1 世代 AWS Outposts のみ)
- Resolver on Outpost ステータスの表示
- Outpost でのリゾルバーの削除 (第 1 世代 AWS Outposts のみ)

Outpost でのリゾルバーの編集 (第 1 世代 AWS Outposts のみ)

Resolver on Outpost を編集するには、次の手順を実行します。

Resolver on Outpost を編集するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. 左側のナビゲーションペインで [Resolver] を展開し、[Outposts] にナビゲートします。
3. ナビゲーションバーで、 AWS Outposts があるリージョンを選択します。
4. 運用状態にある VPC リゾルバーの横にあるチェックマークを選択し、編集を選択します。
5. 編集できる情報は次のとおりです。
   - VPC リゾルバー名
   - インスタンスタイプ
   - インスタンスの数
6. 編集が終わったら、[変更を保存] を選択します。

Resolver on Outpost ステータスの表示

Resolver on Outpost のステータスを表示するには、次の手順を実行します。

インバウンドエンドポイントのステータスを表示するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. 左側のナビゲーションペインで [Resolver] を展開し、[Outposts] にナビゲートします。

3. ナビゲーションバーで、 AWS Outposts があるリージョンを選択します。
4. 動作状態にある VPC リゾルバーの横にあるチェックマークを選択し、詳細の表示を選択します。
5. [Resolver on Outpost] ページの [ステータス] 列には、次のいずれかの値が含まれています。

   作成

   Resolver on Outpost は作成中です。

   運用中

   Resolver on Outpost は正しく設定されています。

   [更新中]

   Resolver on Outpost がインスタンスタイプを更新しています。

   Action needed (アクションが必要)

   この VPC リゾルバーは異常であり、自動的に復旧することはできません。この問題を解決するには、インスタンスが Resolver on Outpost AWS Outposts をサポートできることを確認することをお勧めします。

   削除

   Resolver on Outpost は削除中です。

   作成に失敗

   Resolver on Outpost の作成が失敗しました。

   削除に失敗

   Resolver on Outpost の削除が失敗しました。この問題を解決するには、数分後にもう一度試してください。

Outpost でのリゾルバーの削除 (第 1 世代 AWS Outposts のみ)

> **Note**
>
> Resolver on Outpost を削除する前に、削除する Resolver on Outpost に関連付けられているすべてのエンドポイントを削除する必要があります。

Resolver on Outpost を削除するには、次の手順を実行します。

Resolver on Outpost を削除するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. 左側のナビゲーションペインで [Resolver] を展開し、[Outposts] にナビゲートします。
3. ナビゲーションバーで、 AWS Outposts があるリージョンを選択します。
4. 動作状態にある VPC リゾルバーの横にあるチェックボックスをオンにし、削除を選択します。
5. VPC リゾルバーの削除ダイアログボックスで、テキストボックス**delete**に「」と入力し、「削除」を選択します。

Resolver on Outpost でのインバウンドエンドポイントの管理 (第 1 世代 AWS Outposts のみ)

> **Note**
>
> このコンテンツは第 1 世代 AWS Outposts にのみ適用されます。第 2 世代には適用されません AWS Outposts。

Resolver on Outpost 上のインバウンドエンドポイントを管理するには、該当する手順を実行します。

トピック

- インバウンドエンドポイントの表示と編集
- インバウンドエンドポイントのステータスの表示
- インバウンドエンドポイントの削除

インバウンドエンドポイントの表示と編集

インバウンドエンドポイントの設定を表示および編集するには、次の手順を実行します。

インバウンドエンドポイントの設定を表示および編集するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. 左側のナビゲーションペインで [Resolver] を展開し、[Outposts] にナビゲートします。
3. ナビゲーションバーで、 AWS Outposts があるリージョンを選択します。
4. 運用状態にある VPC リゾルバーの横にあるチェックボックスをオンにし、詳細の表示を選択します。
5. [インバウンドエンドポイント] リストで、設定を表示または編集するエンドポイントのオプションを選択します。
6. [View details (詳細の表示)] または [Edit (編集)] を選択します。

   インバウンドエンドポイントの値の詳細については、「でアウトバウンドエンドポイントを作成または編集するときに指定する値 AWS Outposts」を参照してください。
7. [Edit (編集)] を選択した場合は、該当する値を入力し、[Save (保存)] を選択します。

インバウンドエンドポイントのステータスの表示

インバウンドエンドポイントのステータスを表示するには、次の手順を実行します。

インバウンドエンドポイントのステータスを表示するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. 左側のナビゲーションペインで [Resolver] を展開し、[Outposts] にナビゲートします。
3. ナビゲーションバーで、 AWS Outposts があるリージョンを選択します。
4. オペレーション状態にある VPC リゾルバーの横にあるチェックボックスをオンにし、詳細の表示を選択します。
5. [インバウンドエンドポイント] リストの [ステータス] 列には、次のいずれかの値が表示されます。

   作成

   VPC Resolver は、このエンドポイントの 1 つ以上の Amazon VPC ネットワークインターフェイスを作成および設定しています。

運用中

このエンドポイントの Amazon VPC ネットワークインターフェイスが正しく設定されており、ネットワークと VPC Resolver 間でインバウンドまたはアウトバウンドの DNS クエリを渡すことができます。

更新中

Resolver はこのエンドポイントと 1 つまたは複数のネットワークインターフェイスを関連付けるか関連付けを解除しています。

自動復旧中

VPC Resolver は、このエンドポイントに関連付けられている 1 つ以上のネットワークインターフェイスを復旧しようとしています。復旧プロセス中は、IP アドレスごと (ネットワークインターフェイスごと) の DNS クエリの数の制限により、エンドポイントは容量が制限された状態で機能します。現在の制限については、「Route 53 VPC リゾルバーのクォータ」を参照してください。

Action needed (アクションが必要)

このエンドポイントは異常であり、VPC Resolver は自動的に復旧できません。この問題を解決するには、エンドポイントに関連付けした各 IP アドレスを確認することをお勧めします。使用できない IP アドレスごとに別の IP アドレスを追加して、使用できない IP アドレスを削除します。エンドポイントには常に少なくとも 2 つの IP アドレスが含まれている必要があります。[必要なアクション] のステータスにはさまざまな原因が考えられます。一般的な 2 つの原因を以下に示します。

- エンドポイントに関連付けられている、1 つまたは複数のネットワークインターフェイスが、Amazon VPC を使用して削除されました。
- VPC Resolver のコントロール外にある何らかの理由により、ネットワークインターフェイスを作成できませんでした。

削除

Resolver が、このエンドポイントおよび関連するネットワークインターフェイスを削除しています。

インバウンドエンドポイントの削除

インバウンドエンドポイントを削除するには、次の手順を実行します。

> **Important**
>
> インバウンドエンドポイントを削除すると、ネットワークからの DNS クエリは、エンドポイントで指定した VPC の VPC リゾルバーに転送されなくなります。

インバウンドエンドポイントを削除するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. 左側のナビゲーションペインで [Resolver] を展開し、[Outposts] にナビゲートします。
3. ナビゲーションバーで、 AWS Outposts があるリージョンを選択します。
4. オペレーション状態にある VPC リゾルバーの横にあるチェックボックスをオンにし、詳細の表示を選択します。
5. 削除するエンドポイントの横にあるチェックボックスをオンにします。
6. [削除] を選択します。
7. エンドポイントの削除を確定するには、エンドポイントの名前を入力し、[Submit (送信)] を選択します。

Resolver on Outpost でのアウトバウンドエンドポイントの管理 (第 1 世代 AWS Outposts のみ)

> **Note**
>
> このコンテンツは第 1 世代 AWS Outposts にのみ適用されます。第 2 世代には適用されません AWS Outposts。

Resolver on Outpost 上のアウトバウンドエンドポイントを管理するには、該当する手順を実行します。

トピック

- アウトバウンドエンドポイントの表示と編集
- アウトバウンドエンドポイントのステータスの表示
- アウトバウンドエンドポイントの削除

アウトバウンドエンドポイントの表示と編集

アウトバウンドエンドポイントの設定を表示および編集するには、次の手順を実行します。

アウトバウンドエンドポイントの設定を表示および編集するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. 左側のナビゲーションペインで [Resolver] を展開し、[Outposts] にナビゲートします。
3. ナビゲーションバーで、 AWS Outposts があるリージョンを選択します。
4. オペレーション状態にある VPC リゾルバーの横にあるチェックボックスをオンにし、詳細の表示を選択します。
5. [アウトバウンドエンドポイント] リストで、設定を表示または編集するエンドポイントのチェックボックスを選択します。
6. [View details (詳細の表示)] または [Edit (編集)] を選択します。

   アウトバウンドエンドポイントの値の詳細については、「でアウトバウンドエンドポイントを作成または編集するときに指定する値 AWS Outposts」を参照してください。
7. [Edit (編集)] を選択した場合は、該当する値を入力し、[Save (保存)] を選択します。

アウトバウンドエンドポイントのステータスの表示

アウトバウンドエンドポイントのステータスを表示するには、次の手順を実行します。

アウトバウンドエンドポイントのステータスを表示するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. 左側のナビゲーションペインで [Resolver] を展開し、[Outposts] にナビゲートします。
3. ナビゲーションバーで、 AWS Outposts があるリージョンを選択します。
4. オペレーション状態にある VPC リゾルバーの横にあるチェックボックスをオンにし、詳細の表示を選択します。
5. [アウトバウンドエンドポイント] リストの [ステータス] 列には、次のいずれかの値が表示されます。

作成

VPC Resolver は、このエンドポイントの 1 つ以上の Amazon VPC ネットワークインターフェイスを作成および設定しています。

運用中

このエンドポイントの Amazon VPC ネットワークインターフェイスが正しく設定されており、ネットワークと VPC Resolver 間でインバウンドまたはアウトバウンドの DNS クエリを渡すことができます。

更新中

Resolver はこのエンドポイントと 1 つまたは複数のネットワークインターフェイスを関連付けるか関連付けを解除しています。

自動復旧中

VPC Resolver は、このエンドポイントに関連付けられている 1 つ以上のネットワークインターフェイスを復旧しようとしています。復旧プロセス中は、IP アドレスごと (ネットワークインターフェイスごと) の DNS クエリの数の制限により、エンドポイントは容量が制限された状態で機能します。現在の制限については、「Route 53 VPC リゾルバーのクォータ」を参照してください。

Action needed (アクションが必要)

このエンドポイントは異常であり、VPC Resolver は自動的に復旧できません。この問題を解決するには、エンドポイントに関連付けした各 IP アドレスを確認することをお勧めします。使用できない IP アドレスごとに別の IP アドレスを追加して、使用できない IP アドレスを削除します。(エンドポイントには常に少なくとも 2 つの IP アドレスが含まれている必要があります。) [必要なアクション] のステータスにはさまざまな原因が考えられます。一般的な 2 つの原因を以下に示します。

- エンドポイントに関連付けられている、1 つまたは複数のネットワークインターフェイスが、Amazon VPC を使用して削除されました。
- VPC Resolver のコントロール外にある何らかの理由により、ネットワークインターフェイスを作成できませんでした。

削除

Resolver が、このエンドポイントおよび関連するネットワークインターフェイスを削除しています。

アウトバウンドエンドポイントの削除

エンドポイントを削除する前に、VPC に関連付けられているルールをすべて削除する必要があります。

アウトバウンドエンドポイントを削除するには、次の手順を実行します。

> **Important**
>
> アウトバウンドエンドポイントを削除すると、VPC Resolver は、削除されたアウトバウンドエンドポイントを指定するルールについて、VPC からネットワークへの DNS クエリの転送を停止します。

アウトバウンドエンドポイントを削除するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. 左側のナビゲーションペインで [Resolver] を展開し、[Outposts] にナビゲートします。
3. オペレーション状態にある VPC リゾルバーの横にあるチェックボックスをオンにし、詳細の表示を選択します。
4. [アウトバウンドエンドポイント] リストで、削除するエンドポイントのオプションを選択します。
5. [削除] を選択します。
6. エンドポイントの削除を確定するには、エンドポイントの名前を入力し、[Submit (送信)] を選択します。

Route 53 Global Resolver とは

Route 53 Global Resolver は、インターネットにアクセスできる DNS リゾルバーであり、リモートロケーション、ブランチオフィス、オンプレミス環境にわたって、組織内の認可されたクライアントに簡単、安全、信頼性の高い DNS 解決を提供します。Amazon Route 53 プライベートホストゾーンでホストされているドメインまたはインターネット上のパブリックドメインのクエリを解決しながら、グローバルエニーキャストアーキテクチャを通じて高可用性を維持できます。Route 53 Global Resolver は、潜在的に悪意のあるドメインにクエリをフィルタリングすることで、DNS ベースのデータ流出攻撃からクライアントを保護するのに役立ちます。

Route 53 Global Resolver は、DNS クエリをソースクエリの場所に最も近い AWS リージョンに自動的にルーティングするエニーキャスト IP アドレスを使用して、最適なレイテンシーと可用性を実現します。グローバルリゾルバーが認可されたクライアントに対して DNS 解決を提供するリージョンを選択し、プライベートドメインとパブリックドメインの解決のためにクライアントに対して異なるビューを設定し、悪意のあるドメインをフィルタリングし、組織全体の DNS アクティビティをモニタリングできます。

トピック

- Route 53 Global Resolver を使用する理由
- Route 53 Global Resolver の主な概念とコンポーネント
- Route 53 Global Resolver の仕組み
- Route 53 Global Resolver の DNS セキュリティと分割期間ユースケース
- AWS Route 53 Global Resolver と統合して DNS セキュリティを強化する サービス
- AWS インターフェイスを介して Route 53 Global Resolver にアクセスして管理する方法
- サポートされている AWS リージョン
- Route 53 Global Resolver のオプトインリージョンに関する考慮事項
- Route 53 Global Resolver のアカウントアクセスの設定
- チュートリアル: 最初の Route 53 Global Resolver を作成する
- Route 53 Global Resolver による DNS ビューの管理
- Route 53 Global Resolver でのアクセスソースとトークンを使用したアクセスコントロールの管理
- Route 53 Global Resolver を使用したクライアントの DNS の保護
- Route 53 Global Resolver とのプライベートホストゾーンの関連付けの設定
- AWS アカウント間の Route 53 Global Resolver DNS ビューの共有

- Route 53 Global Resolver による DNS アクティビティとパフォーマンスのモニタリング
- Route 53 Global Resolver の DNS 問題のトラブルシューティング
- Route 53 Global Resolver のクォータ

Route 53 Global Resolver を使用する理由

Route 53 Global Resolver は、複数の口ケーションにわたるリモートおよびハイブリッドのクライアントとワークロードに対して、一元化された DNS セキュリティとフィルタリングを提供します。ワークロード、アプリケーション、ユーザーの場所に関係なく、Route 53 Global Resolver は複雑なオンプレミスインフラストラクチャを必要とせずに一貫した DNS 保護を実現します。

リモート環境とハイブリッド環境の主な利点:

- 管理の簡素化 - 複数のオンプレミス DNS サーバーを管理する代わりに、単一のソリューションを使用してプライベートドメインとパブリックドメインの解決を設定する
- 統合 DNS セキュリティ - すべてのリモートクライアントとハイブリッドワークロードに一貫したフィルタリングポリシーを適用する
- スケーラブルな保護 - 拡大するリモートワークフォースとクラウドワークロードからの DNS クエリを処理するように自動的にスケーリングします
- インフラストラクチャの削減 - 各リモート口ケーションでの DNS セキュリティアプライアンスの必要性を最小限に抑える

開始するには、以下を参照してください。

- the section called “概念と用語” - DNS セキュリティデプロイの主要な概念
- the section called “仕組み” - Route 53 Global Resolver がリモート環境とハイブリッド環境を保護する方法
- the section called “チュートリアル: 最初の Route 53 Global Resolver を作成する” - 最初の DNS フィルタリング設定のチュートリアル

Route 53 Global Resolver の主な概念とコンポーネント

Route 53 Global Resolver は、複数の主要コンポーネントを連携させて、分割トラフィックの DNS 解決、グローバルエニーキャストアーキテクチャによる高可用性、包括的な DNS セキュリティを組織に提供します。これらの Route 53 Global Resolver の概念を理解することで、プライベートリソー

スとパブリックリソースの両方へのシームレスなアクセスを可能にし、複数のリージョンにわたるサービスの継続性を確保し、DNS ベースの脅威から保護するソリューションを設計およびデプロイできます。

オンプレミスおよびリモートロケーションのクライアント用の DNS リゾルバー

分散ワークロード、お客様のロケーション、ユーザーに Route 53 Global Resolver をデプロイするには、以下の主要なコンポーネントを設定します。

グローバルリゾルバー

複数の AWS リージョンにわたる組織の DNS 解決とフィルタリングを提供するメインサービスインスタンス。グローバルリゾルバーは、エニーキャストテクノロジーを使用して DNS クエリを最も近い利用可能なリージョンに自動的にルーティングするため、場所に関係なくすべてのクライアントの応答時間が短縮されます。

エニーキャスト IP アドレス

クライアントデバイスとネットワーク機器で設定するグローバルリゾルバーに割り当てられた 2 つの一意の IPv4 アドレスまたは IPv6 アドレス。これらのエニーキャスト IP アドレスはグローバルに同じであるため、すべてのロケーションで DNS 設定が簡素化されます。エニーキャスト IP アドレス指定により、最も近いグローバルリゾルバーへの DNS リクエストの自動ルーティングが可能になり、応答時間を最適化し、サービスの信頼性が向上します。

DNS ビュー

ネットワーク内の異なるクライアントのグループに異なる DNS ポリシーを適用できる設定テンプレート。DNS ビューを使用して分割期間 DNS を実装します。たとえば、IP ベースのアクセスとブランチオフィスのさまざまなセキュリティポリシーを使用しながら、リモートロケーションに厳密なフィルタリングとトークン認証を適用します。

DNS クライアント認証

デプロイに最適な認証方法を選択します。

トークンベースの認証

DNS-over-HTTPS (DoH) および DNS-over-TLS (DoT) の暗号化されたトークンを使用して DNS 接続を保護します。 DoH DoT 個々のクライアントまたはデバイスグループに一意のアクセストークンを生成し、有効期限を設定し、必要に応じてトークンを取り消すことができます。

ソースベースの認証にアクセスする

IP アドレスと CIDR 範囲の許可リストを使用してアクセスを制御します。ブランチオフィスのパブリック IP アドレスまたはネットワーク範囲を設定し、セキュリティ要件に基づいて各ロケーションで使用できる DNS プロトコル (DNS-over-port-53、DoT、または DoH) を指定できます。

DNS プロトコルの選択

セキュリティと互換性のニーズに基づいて、適切な DNS プロトコルを選択します。

- DNS-over-port-53 (Do53) - 既存のネットワークインフラストラクチャとの互換性を最大化するために使用します
- DNS-over-TLS (DoT) - ネットワークモニタリング専用ポート分離で暗号化された DNS が必要な場合に使用します。
- DNS-over-HTTPS (DoH) - トラフィックが通常の HTTPS として表示されるため、ネットワーク制限をバイパスする必要がある場合に使用します。

トラフィック分割 DNS 解決

Route 53 Global Resolver を使用すると、組織は任意の場所からプライベートドメインとパブリックドメインの両方をシームレスに解決できるため、複雑な VPN 設定やリージョン固有の DNS 設定が不要になります。

ハイブリッド DNS 解決

ハイブリッド DNS 解決により、Route 53 Global Resolver はオンプレミスのユーザーとアプリケーションからプライベートアプリケーションへのクエリを同時に解決できます AWS。

グローバルプライベートゾーンアクセス

グローバルプライベートゾーンアクセスは、VPC 境界を超えて Amazon Route 53 プライベートホストゾーンの到達範囲を拡張します。インターネット上の任意の場所で認可されたクライアントがプライベートドメイン名を解決できるため、分散チームは従来のネットワーク接続要件なしで内部リソースにアクセスできます。

シームレスなフェイルオーバー

シームレスなフェイルオーバーにより、個々の AWS リージョンが使用できなくなっても、プライベートリソースとパブリックリソースの両方に継続的にアクセスできます。エニーキャストアーキテクチャは、一貫した解決動作を維持しながら、クエリを正常なリージョンに自動的にルーティングします。

高可用性とグローバルプレゼンス

Route 53 Global Resolver は、分散アーキテクチャと自動フェイルオーバー機能を通じてエンタープライズグレードの可用性を提供します。

マルチリージョンデプロイ

マルチリージョンデプロイは、Route 53 Global Resolver インスタンスを少なくとも 2 AWS リージョンに分散して、高可用性を確保し、サービス停止中のフェイルオーバーを可能にします。地理的要件とコンプライアンスのニーズに基づいて、特定のリージョンを選択できます。

自動地理的最適化

自動地理的最適化は、ネットワークトポロジとレイテンシーに基づいて、DNS クエリを利用可能な最も近い AWS リージョンにルーティングします。これにより、応答時間が短縮され、グローバルに分散された組織のユーザーエクスペリエンスが向上します。

組み込みの冗長性

冗長性が組み込まれているため、プライマリリージョンが使用できなくなっても、代替リージョンへの自動フェイルオーバーによってサービスの継続性を維持できます。トラフィックが透過的に再ルーティングされる間も、クライアントは同じエニーキャスト IP アドレスを引き続き使用します。

DNS 解決と転送

プライベートホストゾーンの解決

プライベートホストゾーン解決により、Route 53 Global Resolver は AWS リージョン間で Route 53 プライベートホストゾーンの DNS クエリを解決できます。これにより、承認されたクライアントは、インターネット上のどこからでも Route 53 によってホストされるアプリケーションとリソースのドメインを解決できます。

分割期間 DNS

分割期間 DNS は、クエリを実行するクライアントに基づいて異なる DNS レスポンスを提供します。Route 53 Global Resolver は、インターネット上のパブリックドメインを解決できると同時に、プライベートドメインを解決できるため、パブリックリソースとプライベートリソースの両方にシームレスにアクセスできます。

DNSSEC 検証

DNSSEC 検証は、DNSSEC 署名ドメインのパブリックネームサーバーからの DNS レスポンスの信頼性と整合性を検証します。この検証により、送信中に DNS レスポンスが改ざんされることがなくなり、DNS スプーフィング攻撃やキャッシュポイズニング攻撃から保護されます。

EDNS クライアントサブネット (ECS)

EDNS クライアントサブネットは、DNS クエリのクライアントサブネット情報を信頼できるネームサーバーに転送するオプション機能です。これにより、より正確な地理的ベースの DNS レスポンスが可能になり、クライアントをより近いコンテンツ配信ネットワークまたはサーバーに誘導することでレイテンシーが短縮される可能性があります。DNS-over-TLS (DoT) および DNS-over-HTTPS (DoH) 接続の場合、EDNS0 を使用してクライアント IP アドレス情報を渡すことができます。グローバルリゾルバーで ECS を有効にすると、クエリで指定されていない場合、サービスは自動的にクライアント IP を挿入します。

DNS フィルタリングとドメインリスト

Route 53 Global Resolver は、 によって管理されるドメインリストを使用してドメインベースのフィルタリングを提供し、特定のドメイン AWS をブロックまたは許可します。

DNS フィルタリングルール

DNS フィルタリングルールはRoute 53 Global Resolver がドメイン一致基準に基づいて DNS クエリを処理する方法を定義します。ルールは優先順位で評価され、特定のドメインまたはドメインカテゴリへのクエリのアクション (許可、ブロック、または ALERT) を指定できます。

ドメインリスト

ドメインリストは、フィルタリングルールで使用されるドメインのコレクションです。これらは、次のようになります。

- カスタムドメインリスト - 作成および管理するドメインコレクション
- AWS マネージドドメインリスト - 脅威インテリジェンスを活用して悪意のあるドメインを識別する、 によって管理 AWS される事前設定された脅威リストとコンテンツカテゴリ。利用可能な脅威リストは次のとおりです。
  - マルウェアドメイン - マルウェアをホストまたは配布することが知られているドメイン
  - ボットネットのコマンドとコントロール - ボットネットがコマンドとコントロールの通信に使用するドメイン

- スパム - スパムキャンペーンと不要な E メールキャンペーンに関連付けられたドメイン
- フィッシング - 認証情報と個人情報を盗むためにフィッシング攻撃で使用されるドメイン
- Amazon GuardDuty 脅威リスト - GuardDuty 脅威インテリジェンスによって識別されるドメイン

利用可能なコンテンツカテゴリには、ソーシャルメディア、ギャンブル、および組織が特定のタイプのコンテンツへのアクセスを制御するのに役立つその他のカテゴリが含まれます。

マネージドリストの個々のドメイン仕様を表示または編集して、知的財産を保護し、セキュリティの有効性を維持することはできません。

高度な DNS 脅威検出

Route 53 Global Resolver は、動的アルゴリズム分析を使用して、DNS トンネリングやドメイン生成アルゴリズムなどの高度な DNS 脅威を検出します。既知の不正なドメインに一致するドメインリストとは異なり、アルゴリズム検出は DNS クエリパターンをリアルタイムで分析して疑わしい動作を特定します。

DNS トンネリング検出

DNS トンネリングは、攻撃者がクライアントへのネットワーク接続を行わずに DNS トンネルを使用してクライアントからデータを抽出するために使用されます。

ドメイン生成アルゴリズム (DGA) 検出

ドメイン生成アルゴリズム (DGAs) は、攻撃者がcommand-and-controlサーバーの多数のドメイン名を作成するために使用されます。

信頼度のしきい値

各検出アルゴリズムは、ルールのトリガーを決定する信頼スコアを出力します。信頼度しきい値が高いほど誤検出は減少しますが、高度な攻撃を見逃す可能性があります。しきい値が低いほど検出感度は高くなりますが、誤検出をフィルタリングするには追加のアラート分析が必要です。

アクションの制限

高度な脅威保護ルールは、 `ALERT`および `BLOCK`アクションのみをサポートします。この`ALLOW`アクションはサポートされていません。アルゴリズム検出では、無害なトラフィックを明確に分類できず、悪意のある可能性のあるパターンのみを識別できるためです。

モニタリングとログ記録

ログをクエリする

クエリログは、ソース IP、クエリされたドメイン、レスポンスコード、実行されたポリシーアクション、タイムスタンプなど、Route 53 Global Resolver によって処理された DNS クエリに関する詳細情報を提供します。ログは、分析とコンプライアンスレポートのために Amazon CloudWatch、Amazon Data Firehose、または Amazon Simple Storage Service に配信できます。

OCSF 形式

Open Cybersecurity Schema Framework (OCSF) 形式は、Route 53 Global Resolver が DNS クエリログに使用する標準化されたログ記録形式です。この形式は、セキュリティ情報およびイベント管理 (SIEM) システムやその他のセキュリティツールと簡単に統合できる、一貫性のある構造化データを提供します。

ログの宛先

ログの送信先は、それぞれ異なる特性を持つ DNS クエリログの配信先を決定します。

- Amazon Simple Storage Service - コンプライアンスとバッチ分析に最適なコスト効率の高い長期ストレージ。Amazon Athena や Amazon EMR などの分析ツールと統合できます。
- Amazon CloudWatch Logs - Amazon CloudWatch アラームとダッシュボードとの統合によるリアルタイムのモニタリングとアラート。アドホッククエリのログインサイトをサポートします。
- Amazon Data Firehose - データ変換機能が組み込まれた外部システムへのリアルタイムストリーミング。自動スケーリングとバッファリングをサポートします。

オブザーバビリティリージョン

オブザーバビリティリージョンは、DNS クエリログの配信先を決定します。

Route 53 Global Resolver の仕組み

Route 53 Global Resolver は、パブリックドメインとプライベートドメイン間のトラフィック分割 DNS 解決を有効にし、 AWS リージョン 選択した 2 つ以上の を通じて を通じて高可用性を提供し、リクエストを傍受して DNS フィルタリングポリシーを適用することで DNS クエリを保護します。このプロセスを理解すると、問題をトラブルシューティングし、パフォーマンス、可用性、セキュリティのためにデプロイを最適化できます。

クライアントが DNS クエリを実行するとどうなるか

お客様の場所の誰かがドメインをクエリしようとすると、Route 53 Global Resolver は複数のセキュリティレイヤーを介して DNS リクエストを処理します。

DNS クエリ処理には、次のシーケンシャルステップが含まれます。

1. クエリの受信 - クライアントデバイスは、Route 53 Global Resolver のエニーキャスト IP アドレスに DNS クエリを送信します。エニーキャストルーティングは、クエリを最も近い AWS リージョンに自動的に送信します。
2. 認証 - Route 53 Global Resolver は、設定された認証方法 (DoH/DoT の場合はトークンベース、すべてのプロトコルの場合は IP アクセスソース) を使用してクライアントを認証します。
3. ポリシー評価 - サービスは、設定されたセキュリティポリシーとドメインリストに対して DNS クエリを評価し、適切なアクション (許可、ブロック、またはアラート) を決定します。プライベートホストゾーンをターゲットとするクエリの場合、Route 53 Global Resolver は、解決に進む前に、管理者が管理する DNS ビュールールに基づいて、クライアントがプライベートドメインにアクセスする権限があるかどうかを確認します。
4. 解決策 - 許可されたクエリの場合、Route 53 Global Resolver は、必要に応じてパブリック DNS リゾルバーまたはプライベートホストゾーン解決を使用して DNS 解決を実行します。
5. レスポンス配信 - サービスは DNS レスポンスをクライアントに返し、モニタリングと分析のためにクエリの詳細をログに記録します。

グローバルエニーキャストアーキテクチャ

Route 53 Global Resolver は、エニーキャスト IP アドレスを使用して、グローバルな可用性と自動地理的ルーティングを提供します。

Route 53 Global Resolver は、エニーキャスト IP アドレスを使用して以下を提供します。

- 自動地理的ルーティング - DNS クエリは、最適なパフォーマンスを得るために最も近い AWS リージョンに自動的にルーティングされます。
- 組み込み冗長性 - リージョンが使用できなくなった場合、トラフィックは次に近いリージョンに自動的にフェイルオーバーします。
- 整合性のある IP アドレス - クライアントは場所に関係なく同じエニーキャスト IP アドレスを使用し、設定を簡素化します。

DNS フィルタリングとセキュリティ

Route 53 Global Resolver は、複数のレイヤーを通じて包括的な DNS フィルタリングとセキュリティを提供します。DNS フィルタリングとセキュリティアーキテクチャの図は、認証、ポリシー評価、解決レイヤーを通じてクエリを処理する方法を示しています。

Route 53 Global Resolver は、以下を通じて包括的な DNS セキュリティを提供します。

- ドメインベースのフィルタリング - カスタムドメインリストまたは AWS マネージドドメインリストを使用して、ドメイン名に基づいてクエリをブロックまたは許可します。
- 脅威インテリジェンスの統合 - AWS マネージド脅威インテリジェンスを活用して、既知の悪意のあるドメインを自動的にブロックします。
- 高度な脅威検出 - DNS トンネリングの試行とドメイン生成アルゴリズム (DGA) パターンを検出してブロックします。
- リアルタイムモニタリング - セキュリティイベントとポリシー違反のアラートとログを生成します。

Route 53 Global Resolver の DNS セキュリティと分割期間ユースケース

Route 53 Global Resolver は、組織の 3 つの主要な DNS 課題に対処します。

パブリック DNS 解決とプライベート DNS 解決間の分割トラフィックの有効化

インターネット上のパブリックドメインを解決しながら、任意の場所から Amazon Route 53 のプライベートホストゾーン (PHZs) へのグローバルアクセスを有効にします。リモートロケーションとブランチオフィスが、複雑な VPN 設定やリージョン固有の転送なしで内部アプリケーション名を解決できるようにします。分割期間 DNS を実装して、クエリを実行するクライアントに基づいて異なる DNS レスポンスを提供し、リモートクライアントがプライベートドメインとパブリックドメインのクエリを解決できるようにします。

DNS 流出攻撃からの DNS トラフィックの保護

悪意のあるドメインへのクエリをフィルタリングすることで、DNS ベースのデータ流出攻撃からリモートロケーションとブランチオフィスを保護します。DNS-over-HTTPS (DoH) と DNS-over-TLS (DoT) を使用して転送中の DNS トラフィックを暗号化することでプライバシーを向上させ、承認されたクライアントのみが DNS サービスにアクセスできるようにします。セキュリ

ティポリシーを適用して、DNS トンネリングやドメイン生成アルゴリズム (DGAs。DNSSEC 署名ドメインの DNSSEC (ドメインネームシステムセキュリティ拡張機能) を使用して DNS レスポンスの信頼性を検証し、DNS スプーフィング攻撃やキャッシュポイズニング攻撃から保護します。

高可用性とグローバルプレゼンス

グローバルデプロイを通じて高可用性を実現し、単一の管理インターフェイスから世界中の一貫した DNS 設定を維持します。Route 53 Global Resolver は、最適なパフォーマンスと信頼性を実現するために、クエリを利用可能な最も近いリージョンに自動的にルーティングする任意のキャスト IP アドレスを使用して、 AWS リージョン 選択した 全体で実行されます。グローバル企業は、DNS ポリシーを一元的に設定および管理しながら、自動的な地理的最適化でグローバルに機能する単一の IP アドレスセットをクライアントに提供できます。組み込みの冗長性は、個々のリージョンが使用できなくなってもサービスの継続性を維持するように設計されています。

追加機能は、以下の主要なユースケースをサポートします。

DNS フィルタリングとコンテンツポリシーの実装

カスタムドメインリストを作成するか、 AWS マネージドドメインリストを使用して、複数の場所でインターネットアクセスを管理します。ニーズに応じてフィルタリングポリシーとコンテンツポリシーを実装しやすくするために、マネージドドメインリストには、複数のドメインをカバーする複数のカテゴリの DNS 脅威が含まれています。IP 許可リストまたはアクセストークンを使用してアクセスソースを設定し、オフィスの場所やクライアントグループごとに異なるフィルタリングポリシーを設定します。

さまざまなデプロイシナリオに対応する柔軟な認証

デプロイに最適な認証方法を選択します。トークンベースの認証またはソース CIDR 範囲許可リストを使用した IP ベースの認証です。

可視性とコンプライアンスの維持

Amazon CloudWatch、Firehose、または Amazon Simple Storage Service にログを配信することで、組織全体の DNS アクティビティをモニタリングします。セキュリティ監査、コンプライアンス要件、脅威調査をサポートするために、一元化されたログストレージの宛先リージョンを 1 つ選択します。

AWS Route 53 Global Resolver と統合して DNS セキュリティを強化する サービス

Route 53 Global Resolver は、他の AWS サービスとシームレスに統合して、包括的な DNS セキュリティおよび管理機能を提供します。これらの統合により、Route 53 Global Resolver のコア機能が強化され、高度なユースケースが可能になります。

Amazon Route 53

Route 53 Global Resolver は Amazon Route 53 と統合して、プライベートホストゾーンをグローバルに解決します。詳細については、Amazon Route 53 デベロッパーガイドを参照してください。

Amazon CloudWatch

Route 53 Global Resolver は、モニタリングと分析のためにクエリログを Amazon CloudWatch に配信できます。詳細については、「Amazon CloudWatch ユーザーガイド」を参照してください。

Amazon Simple Storage Service

Route 53 Global Resolver は、クエリログを Amazon Simple Storage Service バケットに保存して、長期保存と分析を行うことができます。詳細については、「Amazon S3 ユーザーガイド」を参照してください。

Amazon Data Firehose

Route 53 Global Resolver は、リアルタイム処理のためにクエリログを Amazon Data Firehose にストリーミングできます。詳細については、「Amazon Data Firehose デベロッパーガイド」を参照してください。

Route 53 Resolver DNS ファイアウォール

Route 53 Global Resolver は、グローバル DNS フィルタリング機能を提供することで、Route 53 Resolver DNS Firewall を補完します。詳細については、Route 53 Resolver DNS Firewall のドキュメントを参照してください。

AWS Global Accelerator

Route 53 Global Resolver は と連携して AWS Global Accelerator 、DNS 解決のために最適化されたグローバルネットワークパフォーマンスを提供します。詳細については、AWS Global Accelerator デベロッパーガイドを参照してください。

AWS インターフェイスを介して Route 53 Global Resolver にアクセスして管理する方法

Route 53 Global Resolver には、さまざまな管理設定と自動化要件に対応するための複数のアクセス方法が用意されています。Route 53 Global Resolver は、次のインターフェイスを使用して管理できます。

AWS マネジメントコンソール

AWS マネジメントコンソール は、Route 53 Global Resolver 用のウェブベースのインターフェイスを提供します。コンソールを使用して、DNS フィルタリングポリシーの設定、認証設定の管理、クエリログのモニタリングを行うことができます。

AWS Command Line Interface (AWS CLI)

AWS CLI は、Route 53 Global Resolver API オペレーションへの直接アクセスを提供します。を使用して Route 53 Global Resolver タスク AWS CLI を自動化し、スクリプトとワークフローに統合できます。

AWS SDKs

AWS にはSDKs が用意されています。SDKs を使用して、Cloud Resolver の機能をアプリケーションに統合できます。

REST API

Route 53 Global Resolver には、DNS 解決ポリシーとフィルタリングポリシーをプログラムで管理するために使用できる REST API が用意されています。

サポートされている AWS リージョン

Route 53 Global Resolver は、以下でご利用いただけます AWS リージョン。

- 米国東部 (バージニア北部)
- 米国東部 (オハイオ)
- 米国西部 (北カリフォルニア)
- 米国西部 (オレゴン)
- 欧州 (フランクフルト)
- 欧州 (アイルランド)

- 欧州 (ロンドン)
- アジアパシフィック (ムンバイ)
- アジアパシフィック (シンガポール)
- アジアパシフィック (東京)
- アジアパシフィック (ソウル)
- アジアパシフィック (シドニー)
- アフリカ (ケープタウン)
- アジアパシフィック (香港)
- アジアパシフィック (台北)
- アジアパシフィック (大阪)
- アジアパシフィック (ハイデラバード)
- アジアパシフィック (ジャカルタ)
- アジアパシフィック (メルボルン)
- アジアパシフィック (マレーシア)
- アジアパシフィック (タイ)
- カナダ (中部)
- カナダ西部 (カルガリー)
- 欧州 (チューリッヒ)
- 欧州 (ストックホルム)
- 欧州 (ミラノ)
- 欧州 (スペイン)
- 欧州 (パリ)
- メキシコ (中部)
- 南米 (サンパウロ)

Route 53 Global Resolver のオプトインリージョンに関する考慮事項

AWS アカウントでデフォルトでアクティブ AWS リージョン になっているものもあります。特定のリージョンは、手動で選択した場合にのみアクティブ化されます。このドキュメントでは、これらのリージョンをオプトインリージョンと呼んでいます。対照的に、 AWS アカウントが作成されるとす

ぐに、デフォルトでアクティブなリージョンは商用リージョン、デフォルトリージョン、または単にリージョンと呼ばれます。

AWS リージョン 2019 年 3 月 20 日以降に導入された は、オプトインリージョンとしてデプロイされます。オプトインリージョンでは、そのリージョン内でアカウントが有効になっていません。Route 53 Global Resolver データは、そのリージョンの使用をオプトインしない限り、リージョンにレプリケートされません。オプトインリージョンの詳細については、AWS「リージョンの管理」を参照してください。

オプトインリージョンで Route 53 Global Resolver を使用する場合は、いくつかの考慮事項に留意してください。

動作に関する注意事項

- Global Resolver デプロイのオプトインリージョンを選択するには、アカウントをリージョンにオプトインする必要があります。
- グローバルリゾルバーのデフォルトリージョンまたはオプトインリージョンの任意のセットを選択できます。
- グローバルリゾルバーのオ AWS プトインリージョンを選択した場合、そのリージョンからアカウントをオプトアウトすると、サービスはグローバルリゾルバーデータのそのリージョンへの伝播を停止します。また、そのリージョン内のすべてのリソースの削除もトリガーされます。これにより、リソースがクリーンアップされると、そのリージョン宛ての DNS トラフィックに障害が発生しますが、トラフィックは最終的に他の選択したリージョンに転送されます。
- 同様に、グローバルリゾルバーのオプトインリージョンのセットのみを選択し、すべてのリージョンからアカウントをオプトアウトすると、グローバルリゾルバーは事実上削除されます。
- DNS ログが配信されるオブザーバビリティリージョンのデフォルトリージョンまたはオプトインリージョンを選択することもできます。アカウントをオプトアウトすることを選択した場合、サービスはそのリージョンの送信先への DNS ログの送信を停止します。ログ配信の障害を防ぐために、別のリージョンに新しいログ配信先を設定し、それに応じて Global Resolver でオブザーバビリティリージョンを更新することをお勧めします。
- グローバルリゾルバーは、現時点ではグローバルリゾルバーでのリージョンの拡張と縮小をサポートしていません。グローバルリゾルバーを作成する前に、オプトインして選択するリージョンを計画することをお勧めします。

Route 53 Global Resolver のアカウントアクセスの設定

Route 53 Global Resolver の使用を開始する前に、Route 53 Global Resolver リソースにアクセスするための AWS アカウントと適切なアクセス許可が必要です。これには、必要なアクセス許可を持つ IAM ユーザーとロールの作成が含まれます。

このセクションでは、Route 53 Global Resolver にアクセスするようにユーザーとロールを設定するために必要な手順について説明します。

トピック

- ポリシーとロールの作成
- ネットワークに関する考慮事項

ポリシーとロールの作成

AWS Identity and Access Management (IAM) アクセス許可を設定して、チームが Route 53 Global Resolver リソースをデプロイおよび管理できるようにします。フルアクセスには管理アクセス許可を使用し、設定のモニタリングと表示には読み取り専用アクセス許可を使用できます。

すべての Route 53 Global Resolver API オペレーションには、適切な IAM アクセス許可が必要です。必要なアクセス許可がない場合、API コールは `AccessDeniedException` (401) または `UnauthorizedException` (401) エラーを返します。

管理者のアクセス許可

Route 53 Global Resolver を初めて設定する場合、またはサービスのすべての側面を管理する場合は、管理アクセス許可が必要です。以下の AWS 管理ポリシーを使用できます。

- `AmazonRoute53GlobalResolverFullAccess` - グローバルリゾルバー、DNS ビュー、ファイアウォールルール、ドメインリストの作成、更新、削除など、Route 53 Global Resolver リソースへのフルアクセスを提供します。
- `AmazonRoute53FullAccess` - プライベートホストゾーン転送を使用する場合は必須
- `CloudWatchLogsFullAccess` - Amazon CloudWatch にログを送信する予定がある場合に必要です
- `AmazonS3FullAccess` - Amazon S3 からファイアウォールドメインリストをインポートするか、Amazon S3 にログを送信する場合に必要です

読み取り専用のアクセス許可

Route 53 Global Resolver の設定とログのみを表示する必要がある場合は、次の AWS 管理ポリシーを使用できます。

- `AmazonRoute53GlobalResolverReadOnlyAccess` - グローバルリゾルバー、DNS ビュー、ファイアウォールルール、ドメインリスト、アクセスソースの表示など、Route 53 Global Resolver リソースへの読み取り専用アクセスを提供します
- `AmazonRoute53ReadOnlyAccess` - プライベートホストゾーンの関連付けを表示するために必要です
- `CloudWatchReadOnlyAccess` - Amazon CloudWatch でログを表示するために必要です
- `AmazonS3ReadOnlyAccess` - Amazon S3 に保存されているファイアウォールドメインリストファイルを表示するために必要です

ネットワークに関する考慮事項

Route 53 Global Resolver を実装する前に、次のネットワーク要件を考慮してください。

クライアント IP 範囲

これは、アクセスソースベースの認証を使用する場合にのみ必要です。Route 53 Global Resolver を使用するすべてのクライアントの IP アドレス範囲 (CIDR ブロック) を特定します。アクセスソースのルールを設定するには、これらが必要です。

DNS プロトコル

クライアントが使用する DNS プロトコルを決定します。

- Do53 - ポート 53 経由の標準 DNS (UDP/TCP)
- DoH - 暗号化されたクエリの DNS-over-HTTPS
- DoT - 暗号化されたクエリの DNS-over-TLS

ファイアウォールとセキュリティグループ

ネットワークファイアウォールとセキュリティグループが、適切なポート (Do53 の場合は 53、DoH の場合は 443、DoT の場合は 853) の Route 53 Global Resolver エニーキャスト IP アドレスへのアウトバウンドトラフィックを許可していることを確認します。 Do53 DoH DoT

チュートリアル: 最初の Route 53 Global Resolver を作成する

この入門ガイドでは、Route 53 Global Resolver の基本コンポーネントと、オプションで簡単な DNS フィルタリング設定を作成する方法を示します。このチュートリアルでは、主要な概念について説明しますが、クライアント設定、ログ記録、プライベートドメイン解決などの本番稼働要件は含まれていません。

完了すると、DNS クエリをフィルタリングし、悪意のあるドメインをブロックできる基本的な Route 53 Global Resolver のセットアップが行われます。

以下のセクションでは、Route 53 Global Resolver を使用して DNS セキュリティとフィルタリングをすばやく開始する方法について説明します。

前提条件

Route 53 Global Resolver を使用する前に、Route 53 Global Resolver コンポーネントにアクセス、表示、編集するための AWS アカウントと適切なアクセス許可が必要です。システム管理者は、「」の手順を完了してからthe section called “アカウントアクセスの設定”、このチュートリアルに戻る必要があります。

ステップ 1: グローバルリゾルバーを作成する

まず、グローバルリゾルバーインスタンスを作成し、それが動作する AWS リージョンを選択します。

1. https://console.aws.amazon.com/route53globalresolver/ で Route 53 Global Resolver コンソールを開きます。
2. グローバルリゾルバーの作成を選択します。
3. 名前 に、グローバルリゾルバーのわかりやすい名前を入力します。
4. 説明 には、オプションで説明を入力します。
5. リージョンでは、グローバルリゾルバーをインスタンス化する AWS リージョン 2 つ以上の を選択します。最適なパフォーマンスを得るには、クライアントに最も近いリージョンを選択します。
6. IP アドレスタイプで、このリゾルバーの IP アドレスタイプを選択します。
   - IPv4 - IPv4 アドレスのみが含まれます。
   - デュアルスタック - IPv4 アドレスと IPv6 アドレスが含まれます。
7. 必要に応じて、リソースの整理と管理に役立つタグを追加します。

8. グローバルリゾルバーの作成を選択します。

クライアントが Resolver に到達するために使用できるエニーキャスト IPv4 アドレスがすぐに届きます。グローバルリゾルバーの作成プロセスは、アドレスが機能するまでに数分かかります。

ステップ 2: DNS ビューを作成して認証を設定する

DNS ビューを作成してクライアントを整理し、IP データソースを使用して認証を設定します。このチュートリアルでは、IP ベースの認証を使用します。DoH/DoT プロトコルのアクセストークンを使用することもできます。

1. Route 53 グローバルリゾルバーコンソールで、グローバルリゾルバーを選択します。
2. DNS ビューの作成 を選択します。
3. 名前 に、DNS ビューのわかりやすい名前を入力します。
4. 説明 には、オプションで説明を入力します。
5. DNS ビューの作成 を選択します。
6. DNS ビューを作成したら、アクセスソースを選択し、アクセスソースを作成します。
7. CIDR ブロックには、クライアントの IP アドレス範囲 (例:) を入力します`203.0.113.0/24`。
8. Protocol では、基本的なセットアップのために Do53 (ポート 53 経由の DNS) を選択します。
9. アクセスソースルールの作成を選択します。

ステップ 3: DNS フィルタリングルールを設定する (オプション)

基本的な DNS フィルタリングルールを設定して、悪意のあるドメインへのアクセスをブロックします。

1. DNS ビューで、ファイアウォールルールを選択し、ファイアウォールルールを作成します。
2. Name に、ルールのわかりやすい名前を入力します。
3. Priority には、 と入力します `100` (低い数値の方が優先度が高くなります) 。
4. アクション で、ブロック を選択します。
5. ドメインリストタイプで、AWS マネージドドメインリストを選択します。
6. マネージドドメインリストで、AmazonGuardDutyThreatList、Malware and Botnet Command and Control を選択して、既知の悪意のあるドメインをブロックします (他のマネージドリストを追加したり、後でカスタムリストを作成したりできます) 。

7. ファイアウォールルールの作成 を選択します。

ステップ 4: 設定をテストする

Route 53 Global Resolver 設定が正しく動作していることをテストします。

1. 設定した CIDR 範囲内のクライアントマシンから、グローバルリゾルバーが提供するエニーキャスト IP アドレスを使用して DNS 解決をテストします。

```
nslookup example.com <anycast-ip-address>
```

2. 正当なドメインが正しく解決することを確認します。
3. ブロックされたドメインが適切にフィルタリングされていることをテストします。テストドメインを使用してカスタムドメインリストを作成して、ファイアウォールルールが正しく動作していることを確認できます。マネージドドメインリストの詳細については、「マネージドドメインリスト」を参照してください。
4. Route 53 Global Resolver コンソールでクエリログとフィルタリングアクティビティを確認します。

包括的なテスト手順とトラブルシューティングについては、Route 53トラブルシューティング」を参照してください。

ステップ 5: DNS アクティビティのモニタリング

DNS アクティビティのログ記録を設定します。

1. オブザーバビリティリージョンを選択します。
2. クエリログの送信先を選択します。

包括的なテスト手順とトラブルシューティングについては、Route 53テストとトラブルシューティング」を参照してください。

ステップ 6: クリーンアップする (オプション)

テスト目的でこの設定を作成し、Route 53 Global Resolver を引き続き使用しない場合は、継続的な料金が発生しないようにリソースをクリーンアップします。

1. Route 53 Global Resolver コンソールで、作成したファイアウォールルールをすべて削除します。
2. 作成したアクセスソースルールをすべて削除します。
3. DNS ビューを削除します。
4. グローバルリゾルバーを削除します。

> **Important**
>
> これらのリソースを削除すると、それらを使用するように設定されたクライアントの DNS 解決が停止します。リゾルバーを削除するか、アクセスルールを削除する前に、クライアント設定を更新します。

次の手順

これで、Route 53 Global Resolver の基本的な設定ができました。次に、追加の機能について説明します。

- リゾルバーを使用するようにクライアントデバイスを設定します (本番稼働に必要) 。Global Resolver が提供するエニーキャスト IP アドレスを使用するようにクライアント DNS 設定を更新します。
- モニタリングとコンプライアンスのためのログ記録を設定します (本番稼働用に推奨)。モニタリングと分析のために Amazon CloudWatch、Amazon S3、または Amazon Data Firehose へのログ記録を設定します。詳細については、「Route 53 Global Resolver による DNS アクティビティとパフォーマンスのモニタリング」を参照してください。
- 内部ドメインのプライベートホストゾーン転送を設定します (プライベート AWS リソースがある場合は必須) 。詳細については、「プライベートホストゾーンの使用」を参照してください。
- DNS-over-HTTPS (DoH) または DNS-over-TLS (DoT) を使用して、暗号化された DNS 接続を設定します。詳細については、「暗号化された DNS の設定」を参照してください。
- カスタムドメインリストと高度なフィルタリングルールを作成します。詳細については、「DNS フィルタリング」を参照してください。

Route 53 Global Resolver による DNS ビューの管理

DNS ビューの更新など、進行中の Route 53 Global Resolver オペレーションを管理して、どのクライアントデバイスグループを内部リソースに解決できるか、どのドメインをフィルタリングするかを制御できます。

DNS ビューの管理

DNS ビューを作成したら、設定を更新し、有効または無効にして、ライフサイクルを管理できます。

クライアントデバイスグループの DNS ビューの作成

DNS ビューは、リモートワーカー、ブランチオフィスデバイス、オンプレミス機器などのクライアントデバイスのグループのセキュリティポリシーを定義する論理グループです。各ビューには、独自の認証要件、フィルタリングルール、プライベートホストゾーンの関連付けがあります。

DNS ビューを作成するには

1. https://console.aws.amazon.com/route53globalresolver/ でコンソールを開きます。
2. リストからグローバルリゾルバーを選択します。
3. DNS ビュータブを選択します。
4. DNS ビューの作成 を選択します。
5. DNS ビューの詳細セクションで、次の操作を行います。
   a. DNS ビュー名には、DNS ビューのわかりやすい名前 (最大 128 文字) を入力します。
   b. (オプション) 説明に、DNS ビューの説明を入力します (最大 255 文字) 。
6. DNS クエリ処理セクションで、次の設定を行います。
   - DNSSEC 検証 - 有効化または無効化を選択します。DNSSEC 検証により、グローバルリゾルバーは DNS レスポンスの信頼性を検証できます。
   - ファイアウォールルールがオープンに失敗する動作 - DNS Firewall が評価できない場合にクエリを続行できるようにするには Enable、そのようなクエリをブロックするにはDisable を選択します。
   - EDNS0 クライアントサブネット - Enable を選択して、近くのリソースへのトラフィックルーティングと効率的なキャッシュのクライアントロケーション精度を向上させるか、Disable を選択してこの機能をオフにします。

7. DNS ビューの作成 を選択します。

DNS ビューを作成したら、アクセスコントロール、ファイアウォールルール、プライベートホストゾーンの関連付けを設定できます。

DNS ビューの編集

DNS クエリ処理オプションや関連リソースなど、作成後に DNS ビュー設定を変更できます。

DNS ビューを編集するには

1. コンソールで、グローバルリゾルバーに移動します。
2. DNS ビュータブを選択します。
3. 編集する DNS ビューを選択し、編集を選択します。
4. 必要に応じて DNS ビュー設定を変更し、変更を保存を選択します。

DNS ビューの有効化と無効化

DNS ビューは、削除せずに一時的に無効にすることができます。無効にすると、Global Resolver はその DNS ビューに関連付けられたクライアントデバイスのリクエストの処理を停止します。

> **Warning**
>
> DNS ビューを無効にすると、そのビューに関連付けられているすべてのクライアントデバイスの DNS 解決が直ちに停止します。影響を受けるクライアントデバイスに代替 DNS 解決が設定されていることを確認します。

DNS ビューの削除

DNS ビューを削除する前に、まず、アクセスソースルール、アクセストークン、ファイアウォールルール、プライベートホストゾーンの関連付けなど、関連するすべてのリソースを削除する必要があります。

> **Warning**
>
> DNS ビューの削除は元に戻せず、そのビューに関連付けられているすべてのクライアントデバイスの DNS 解決を直ちに停止します。

プライベートホストゾーンの関連付けの管理

必要に応じてプライベートホストゾーンの関連付けを表示、更新、削除して、内部リソースにアクセスできるクライアントデバイスグループを制御できます。

関連付けの表示

DNS ビューのすべてのプライベートホストゾーンの関連付けを表示するには、DNS ビューに移動し、プライベートホストゾーンセクションをチェックして、関連するすべてのゾーンのステータスと関連付けの詳細を確認します。

関連付けの更新

プライベートホストゾーンの関連付けの名前を更新するには、関連付けの選択、編集の選択、関連付け名の更新、変更の保存を行います。

関連付けの削除

プライベートホストゾーンの関連付けを削除すると、Route 53 Global Resolver はそのゾーンを使用して、関連付けられた DNS ビューの DNS クエリを解決しなくなります。

> **Warning**
>
> プライベートホストゾーンの関連付けを削除すると、DNS 解決にすぐに影響します。関連付けが解除されたゾーンのドメインのクエリは、プライベートゾーンレコードの代わりにパブリック DNS を使用して解決されます。

Route 53 Global Resolver で DNS ビューの設定を構成する

Route 53 Global Resolver では、セキュリティ要件とアクセスニーズに基づいて、クライアントデバイスのグループごとに異なる DNS ポリシーとアクセスコントロールを設定できます。セキュリティ要件とアクセスニーズに基づいて、さまざまなクライアントデバイスのグループに対して Route 53 Global Resolver で DNS ポリシーとアクセスコントロールを設定します。

クライアントグループの DNS 設定の構成

各 DNS ビューには、さまざまなクライアントデバイスグループに対して DNS クエリがどのように処理および解決されるかを制御するいくつかの設定があります。

DNSSEC 検証

DNSSEC 検証は、パブリックドメインの DNS レスポンスが真正であり、改ざんされていないことを確認するのに役立ちます。DNSSEC 検証を有効にすると、Route 53 Global Resolver は DNSSEC 署名をチェックし、無効な署名を持つドメインの SERVFAIL を返します。

次の場合は、DNSSEC 検証を有効にすることを検討してください。

- 組織で DNS レスポンスの暗号化検証が必要である
- DNS スプーフィングおよびキャッシュポイズニング攻撃に対する保護が必要
- DNSSEC 検証を必要とするコンプライアンス要件がある

> **Note**
>
> DNSSEC 検証はパブリックドメインにのみ適用されます。プライベートホストゾーンは、独自の認証メカニズムを使用します。

EDNS クライアントサブネット (ECS)

EDNS クライアントサブネットには、信頼できるサーバーに送信される DNS クエリ内のクライアントのネットワークの場所に関する情報が含まれます。これにより、コンテンツ配信ネットワークと地理的に分散されたサービスが、ロケーションに適したレスポンスを提供できるようになります。

ECS は以下に役立ちます。

- 地理的に分散されたサービスによるパフォーマンスの向上
- コンテンツ配信ネットワークルーティングの精度の向上
- リージョンのコンテンツ制限への準拠の向上

プライバシーに関する考慮事項:

- ECS は、クライアント IP 情報の一部を信頼できるサーバーに公開します (IPv4 の場合は最大 /24、IPv6 の場合は最大 /48)
- を有効にする前に、組織のプライバシー要件を考慮してください。

ファイアウォールのフェイルオープン

ファイアウォールのフェイルオープン設定は、サービスの障害や設定の問題が原因で DNS ファイアウォールルールを評価できない場合の動作を決定します。

無効 (デフォルト)

ファイアウォールルールを評価できない場合、DNS クエリはブロックされます。これによりセキュリティは最大になりますが、サービスの問題発生時の可用性に影響する可能性があります。

有効

DNS クエリは、ファイアウォールルールを評価できない場合に許可されます。これにより、サービスの問題発生時のセキュリティよりも可用性が優先されます。

クライアントデバイスグループを整理するためのベストプラクティス

さまざまなクライアントデバイスグループの DNS ビューを設計する際は、次のベストプラクティスに従います。

組織戦略を確認する

- セキュリティ要件で区切る - セキュリティクリアランスまたはアクセスレベルが異なるクライアントデバイス用に異なるビューを作成する
- 場所別に整理 - 地理的な場所やネットワークセグメントごとに個別のビューを使用する
- デバイスタイプ別にグループ化 - サーバー、ワークステーション、モバイルデバイス、または IoT デバイス専用のビューを作成する
- わかりやすい名前を使用する - ビューの目的とターゲットクライアントデバイスを明確に示す名前を選択します。

セキュリティに関する考慮事項

- 最小特権の原則 - クライアントデバイスに必要な最小限のアクセスで各ビューを設定します。
- デフォルトの拒否 - 制限的なファイアウォールルールから開始し、必要に応じて例外を追加します
- 定期的なレビュー - DNS ビュー設定の定期的なレビューと更新
- 使用状況のモニタリング - DNS クエリログを使用して DNS ビューの使用状況パターンをモニタリングおよび分析する

Route 53 Global Resolver でのアクセスソースとトークンを使用したアクセスコントロールの管理

Route 53 Global Resolver には、クライアントデバイスアクセスを制御するための 2 つの主要な方法があります。IP ベースの認証用のアクセスソースとトークンベースの認証用のアクセストークンです。この章では、両方のアプローチについて説明し、環境に適した認証方法を選択し、包括的なアクセスコントロールを実装するのに役立ちます。

トピック

- アクセスコントロール方法
- アクセスソースとアクセスソースルールの設定
- 暗号化された認証のアクセストークンの管理
- アクセスコントロールのベストプラクティスとセキュリティ上の考慮事項

アクセスコントロール方法

Route 53 Global Resolver には、DNS インフラストラクチャへのクライアントアクセスを制御するための 2 つの異なる認証方法が用意されています。各メソッドは、さまざまなユースケースと環境に対応します。

アクセスソース

アクセスソースは IP ベースの認証を使用して DNS クエリを制御します。クライアントの IP アドレスに基づいてクエリを許可または拒否するアクセスソースルールを設定します。この方法は、ブランチオフィスや VPN 接続など、予測可能な IP 範囲を持つ環境に適しています。アクセスソースは、すべての DNS プロトコル (Do53、DoT、DoH) をサポートし、ネットワーク管理者に簡単な設定を提供します。

アクセストークン

アクセストークンは、DoH および DoTプロトコルの暗号化された時間制限付き認証情報を使用したトークンベースの認証を使用します。この方法は、IP アドレスが頻繁に変化するモバイルクライアントと環境に適しています。トークンは有効期限が切れる前に更新でき、暗号化によってセキュリティを強化します。

認証アプローチを選択するときは、次の要素を考慮してください。

認証方法の比較

Factor	アクセスソース	アクセストークン
ユースケース	固定 IP 範囲、オフィスネットワーク、VPN ユーザー	モバイルデバイス、動的 IPs、リモートワーカー
セキュリティレベル	ネットワークベース、IP 信頼に依存	暗号化された認証情報、時間制限付き
管理の複雑さ	シンプルな IP 範囲管理	トークンのライフサイクルとディストリビューション
プロトコルサポート	Do53、DoT、DoH	DoT、DoH のみ

両方のメソッドを同時に使用して、レイヤードセキュリティを作成できます。たとえば、オフィスネットワークにはアクセスソースを使用し、リモートワーカーにはトークンを使用します。

アクセスソースとアクセスソースルールの設定

アクセスソースは、IP アドレスに基づいてクライアントアクセスを制御します。DNS インフラストラクチャをクエリできる IP 範囲と使用できるプロトコルを指定するアクセスソースルールを作成します。

アクセスソースルールの作成

以下の手順に従って、特定の IP 範囲に DNS インフラストラクチャのクエリを許可するアクセスソースルールを作成します。

1. Route 53 Global Resolver コンソールを開き、DNS ビューに移動します。
2. アクセスソースセクションで、アクセスソースルールの作成を選択します。
3. ルール名には、 `office-network`や など、このルールの目的を識別するわかりやすい名前を入力します`vpn-users`。
4. IP アドレスタイプで、IPV4 または IPV6 を選択します。
5. CIDR ブロックには、 がアクセスする必要がある IP アドレスを指定します。IP 範囲: `203.0.113.0/24`または `2001:db8::/112`、または個々の IP アドレス: `203.0.113.5/32`または に CIDR 表記を使用できます`2001:db8::1/128`。

6. プロトコル では、このルールが適用される DNS プロトコルを選択します。
   - Do53 - UDP/TCP 経由の標準 DNS (ポート 53)
   - DoT - TLS 経由の DNS (ポート 853)
   - DoH - HTTPS 経由の DNS (ポート 443)
7. アクセスソースルールの作成を選択します。

指定された IP 範囲のクライアントデバイスが、選択したプロトコルを使用して DNS インフラストラクチャをクエリできるようになりました。

ルールの評価と優先度について

Route 53 Global Resolver は、使用する正しいビューを識別するときに、アクセスソースルールを評価します。

- ルールは、最も具体的な IP 範囲から最も具体的な IP 範囲まで処理され、最も具体的な一致ルールが優先されます。
- 一致するルールがない場合、リクエストはデフォルトで拒否されます。

異なる IP アドレスからクエリを実行してアクセスソース設定をテストし、ルールが期待どおりに動作することを確認します。

暗号化された認証のアクセストークンの管理

アクセストークンは、DoH プロトコルと DoT プロトコルの暗号化された認証を提供します。IP ベースのアクセスソースとは異なり、トークンはクライアントの場所に関係なく機能し、暗号化と有効期限の制御を通じてセキュリティを強化します。

アクセストークンの作成

DoH または DoTプロトコルを使用するクライアントデバイスを認証するためのアクセストークンを作成するには、次の手順に従います。

1. Route 53 Global Resolver コンソールを開き、DNS ビューに移動します。
2. アクセスソースセクションで、アクセストークンの作成を選択します。
3. Name には、 `mobile-devices`や など、トークンの目的を識別するわかりやすい名前を入力しますremote-workers-q4。

4. 有効期限 では、トークンの有効期限を設定します。セキュリティのために 90 日以内をお勧めします。有効期限を設定するときは、トークンの配布と更新の機能を検討してください。
5. アクセストークンの作成を選択します。
6. 組織の安全な通信チャネルを使用して、トークンをクライアントデバイスに安全に配布します。

アクセストークンを使用したクライアントデバイスの設定

Route 53 Global Resolver インフラストラクチャでの認証にアクセストークンを使用するようにクライアントデバイスを設定します。

DoH 設定

アクセストークンを使用して DoH を設定するには、グローバルリゾルバーの DNS 名または IP アドレスが必要です。

1. GetGlobalResolver API を使用して、リゾルバーの接続の詳細を取得します。
2. (3.3.3.3、3.3.3.4 `ipv4Addresses` など) と `dnsName` (a1bc234567890a.route53globalresolver.global.on.aws など) に注意してください。
3. DNS 名を使用して DoH エンドポイントに URL パラメータとしてトークンを含めます。

```
https://a1bc234567890a.route53globalresolver.global.on.aws/dns-query?token=<token-value>
```

を、生成した実際のトークン`<token-value>`に置き換えます。

DoT 設定

アクセストークンを含む DoT クエリの場合、次の仕様の EDNS0 オプションにトークンを含めます。

- オプションコード: `0xffa0`
- オプションデータ: 文字列形式のアクセストークン

具体的な実装は、DoT クライアントソフトウェアと EDNS0 オプションの処理方法によって異なります。

トークンライフサイクル管理

トークンの有効期限と更新を管理し、クライアントデバイスの安全なアクセスを維持します。

- 有効期限のモニタリング - トークンの有効期限を追跡し、事前に更新を計画します。
- 有効期限前に更新 - サービスの中断を避けるため、古いトークンの有効期限が切れる前に新しいトークンを作成します。
- トークンを定期的にローテーションする - セキュリティを強化するために、有効期限が切れる前にトークンを定期的に置き換えます。
- 侵害されたトークンを取り消す - 侵害されたと思われる場合は、トークンをすぐに削除します。

管理オーバーヘッドを減らすために、大規模なデプロイの自動トークン更新プロセスを実装することを検討してください。

プラットフォーム設定の例

これらのプラットフォーム固有の例を使用して、Route 53 Global Resolver アクセストークンと接続の詳細でクライアントデバイスを設定します。

Windows 設定

netsh コマンドを使用して、アクセストークンで DoH を使用するように Windows クライアントを設定するには、次の手順に従います。

1. 管理者としてコマンドプロンプトを開きます。
2. グローバル DoH 設定を有効にします。

```
netsh dns add global doh=yes
```

3. DoH サーバーをアクセストークンに登録します。サンプル値を実際のリゾルバーの詳細に置き換えます。

```
netsh dns add encryption server=3.3.3.3 dohtemplate=https://
a1bc234567890a.route53globalresolver.global.on.aws/dns-query?token=<your-token>
 autoupgrade=yes
netsh dns add encryption server=3.3.3.4 dohtemplate=https://
a1bc234567890a.route53globalresolver.global.on.aws/dns-query?token=<your-token>
 autoupgrade=yes
```

4. DNS キャッシュをフラッシュします。

```
ipconfig /flushdns
```

5. 設定の検証:

```
netsh dns show global
```

macOS 設定

アクセストークンを使用して DoH のモバイル設定プロファイルを使用して macOS クライアントを設定するには、次の手順に従います。

次の構造でモバイル設定プロファイルを作成します。

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/
PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>PayloadContent</key>
  <array>
    <dict>
      <key>DNSSettings</key>
      <dict>
        <key>DNSProtocol</key>
        <string>HTTPS</string>
        <key>ServerAddresses</key>
        <array>
          <string>3.3.3.3</string>
          <string>3.3.3.4</string>
        </array>
        <key>ServerURL</key>
        <string>https://a1bc234567890a.route53globalresolver.global.on.aws/dns-query?
token=<your-token></string>
      </dict>
      <key>PayloadType</key>
      <string>com.apple.dnsSettings.managed</string>
    </dict>
  </array>
</dict>
</plist>
```

システム設定 > デバイス管理を使用してプロファイルをインストールします。

アクセスコントロールのベストプラクティスとセキュリティ上の考慮事項

Route 53 Global Resolver インフラストラクチャの安全で効果的なアクセスコントロールを維持するには、以下のベストプラクティスに従います。

セキュリティのベストプラクティス

DNS インフラストラクチャを保護するために、次のセキュリティ対策を実装します。

- レイヤー認証を使用する - 信頼できるネットワークのアクセスソースをモバイルユーザーのトークンと組み合わせます。このアプローチは、多層防御を提供し、さまざまなクライアントシナリオに対応します。
- 最小特権アクセスの実装 - クライアントが実際に必要とする IP 範囲とプロトコルにのみアクセスを許可します。インフラストラクチャを不正使用にさらす可能性のある過度に広範なアクセスソースルールは避けてください。
- トークンを定期的にローテーションする - アクセストークンは、有効期限が切れる前であっても、定期的なスケジュールで置き換えます。このプラクティスは、侵害されたトークンの影響を制限し、セキュリティの健全性を維持します。
- アクセスパターンのモニタリング - DNS クエリログを確認して、異常なアクセスパターンや潜在的なセキュリティ問題を特定します。予期しない IP 範囲または期限切れトークンを使用したクエリのアラートを設定します。

運用のベストプラクティス

信頼性の高いアクセスコントロールを維持するには、以下の運用プラクティスに従います。

- アクセスコントロール戦略を文書化する - どのアクセスソースとトークンがどのクライアントグループに役立つかを明確に文書化します。
- アクセスコントロールを定期的にテストする - 異なるクライアントの場所やシナリオからアクセスソースルールとトークンが正しく動作することを確認します。
- トークン更新の計画 - サービスの中断を避けるために、古いトークンの有効期限が切れる前に新しいトークンを配布するプロセスを確立します。
- アクセスコントロールを定期的に確認する - 未使用のアクセスソースルールと期限切れトークンを削除して、クリーンな設定を維持します。

Route 53 Global Resolver を使用したクライアントの DNS の保護

以下のセクションでは、クライアントによって行われた DNS クエリを保護するためのルールを作成する方法について説明します。

トピック

- DNS Firewall ルールの設定と管理
- Route 53 Global Resolver のマネージドドメインリスト
- ブロックまたは許可するドメインのビルドリスト
- DNS Firewall Advanced 保護
- Route 53 Global Resolver で DNS セキュリティポリシーを管理する

DNS Firewall ルールの設定と管理

ファイアウォールルールの作成と表示

ファイアウォールルールはRoute 53 Global Resolver がドメインリスト、マネージドドメインリスト、コンテンツカテゴリ、または高度な脅威保護に基づいて DNS クエリを処理する方法を定義します。各ルールは、優先度、ターゲットドメイン、実行するアクションを指定します。

ルールの優先度に関するベストプラクティス:

- 優先度の高い許可ルール (信頼されたドメイン) に優先度 100～999 を使用する
- ブロックルール (既知の脅威) に優先度 1000-4999 を使用する
- アラートルールに優先度 5000-9999 を使用する (モニタリングと分析)
- 今後のルール挿入を可能にするために優先順位の間にギャップを残す

DNS Firewall ルールを作成するには

1. Route 53 Global Resolver コンソールで、DNS ビューに移動します。
2. ファイアウォールルールタブを選択します。
3. ファイアウォールルールの作成 を選択します。
4. ルールの詳細セクションで、次の操作を行います。
   a. ルール名には、ルールのわかりやすい名前 (最大 128 文字) を入力します。
   b. (オプション) ルールの説明に、ルールの説明を入力します (最大 255 文字) 。

5. ルール設定セクションで、ルール設定タイプを選択します。
   - カスタマーマネージドドメインリスト - 作成して管理するドメインリストを使用する
   - AWS マネージドドメインリスト - 利用できる Amazon が提供するドメインリストを使用します。
   - DNS Firewall Advanced Protections - マネージド保護の範囲から選択し、信頼度しきい値を指定します。
6. ルールアクションで、ルールが一致するときに実行するアクションを選択します。
   - 許可 - DNS クエリが解決されました
   - アラート - DNS クエリを許可しますが、アラートを作成します
   - ブロック - DNS クエリがブロックされます
7. ファイアウォールルールの作成 を選択します。

割り当てられたルールを表示するには、次の手順に従います。ルールとルール設定を更新することもできます。

ルールを表示および更新するには

1. Route 53 Global Resolver コンソールで、DNS ビューに移動します。
2. DNS ファイアウォールルールタブを選択します。
3. 表示または編集するルールを選択し、編集を選択します。
4. ルールページで、設定を表示および編集できます。

ルールの値の詳細については、「the section called “DNS ファイアウォールのルール設定”」を参照してください。

ルールを削除するには

1. Route 53 Global Resolver コンソールで、DNS ビューに移動します。
2. DNS ファイアウォールルールタブを選択します。
3. 削除するルールを選択し、削除を選択して削除を確定します。

DNS ファイアウォールのルール設定

DNS ビューで DNS ファイアウォールルールを作成または編集するときは、次の値を指定します。

名前

DNS ビューのルールの一意の識別子。

(オプション) 説明

ルールの詳細についての簡単な説明。

ドメインリスト

ルールが調査するドメインのリスト。独自のドメインリストを作成および管理することも、 が AWS 管理するドメインリストにサブスクライブすることもできます。

ルールには、ドメインリストまたは DNS Firewall Advanced 保護を含めることができますが、両方を含めることはできません。

クエリタイプ (ドメインリストのみ)

ルールが検査する DNS クエリタイプのリスト。有効な値を次に示します。

- A: IPv4 アドレスを返します。
- AAAA: Ipv6 アドレスを返します。
- CAA: ドメインの SSL/TLS 証明書を作成できる CA を制限します。
- CNAME: 別のドメイン名を返します。
- DS: 委任ゾーンの DNSSEC 署名キーを識別するレコード。
- MX: メールサーバーを指定します。
- NAPTR: ドメイン名の正規表現ベースの書き換え。
- NS: 権威ネームサーバー。
- PTR: IP アドレスをドメイン名にマッピングします。
- SOA: ゾーンの管理情報の始点レコード。
- SPF: ドメインから E メールを送信する権限を持つサーバーを一覧表示します。
- SRV: サーバーを識別するアプリケーション固有の値。
- TXT: E メール送信者とアプリケーション固有の値を検証します。

DNS タイプ ID を使用して定義するクエリタイプ (例えば、AAAA の場合は 28)。値は TYPE として定義する必要があります。ここでNUMBER、 は 1 ~ 65334、たとえば TYPE28 NUMBERです。詳細については、「DNS レコードタイプの一覧」を参照してください。

ルールごとに 1 つのクエリタイプを作成できます。

DNS Firewall Advanced 保護

DNS クエリの既知の脅威署名に基づいて、疑わしい DNS クエリを検出します。保護は、以下から選択できます。

- ドメイン生成アルゴリズム (DGAs)

  DGAs は、攻撃者が多数のドメインを生成してマルウェア攻撃を開始するために使用されます。

- DNS トンネリング

  DNS トンネリングは、攻撃者がクライアントへのネットワーク接続を行わずに DNS トンネルを使用してクライアントからデータを抽出するために使用されます。

DNS Firewall Advanced ルールでは、脅威に一致するクエリをブロックするか、アラートするかを選択できます。

詳細については、「DNS Firewall Advanced Protections」を参照してください。

ルールには、DNS Firewall Advanced 保護またはドメインリストを含めることができますが、両方を含めることはできません。

信頼度のしきい値 (DNS Firewall Advanced のみ)。

DNS Firewall Advanced の信頼度のしきい値。DNS Firewall Advanced のルールを作成するときに、この値を指定する必要があります。信頼度の値は次のことを意味します。

- 高 – 誤検出率が低く、最も裏付けのある脅威のみを検出します。
- 中 – 脅威の検出と誤検出のバランスが取れています。
- 低 – 脅威の検出率が最も高いが、誤検出も増加します。

詳細については、「DNS Firewall のルール設定」を参照してください。

アクション

DNS Firewall で、ルールのドメインリストの仕様と一致するドメイン名を持つ DNS クエリを処理する方法 詳細については、「the section called “DNS Firewall でのルールアクション”」を参照してください。

優先度

処理順序を決定する DNS ビュー内のルールの一意の正の整数設定。DNS Firewall は、DNS ビューのルールに対して DNS クエリを検査します。優先順位は数値が最も低い設定から順に上

がります。ルールの優先度はいつでも変更できます。例えば、処理の順序を変更したり、他のルールのためのスペースを確保できます。

DNS Firewall でのルールアクション

DNS Firewallでは、DNS クエリとルールのドメイン仕様の間で一致が検出されると、ルールで指定されたアクションがクエリに適用されます。

作成する各ルールで、次のオプションのいずれかを指定する必要があります：

- Allow - クエリの検査を停止し、通過を許可します。DNS Firewall Advanced では使用できません。
- 警告 — クエリの検査を停止し、通過を許可して、Route 53 Resolver ログにクエリのアラートを記録します。
- ブロック — クエリの検査を中断し、目的の送信先への送信をブロックして、Route 53 Resolver ログにそのクエリのブロックアクションを記録します。

  次のように、設定されたブロックレスポンスで応答します。
  - NODATA - クエリが成功したことを示す応答がありますが、それに対して利用可能になったという応答はありません。
  - NXDOMAIN – クエリのドメイン名が存在しないことを示す応答。
  - OVERRIDE – レスポンスにカスタムオーバーライドを指定します。このオプションには、次の設定が必要です。
    - Record value — クエリにレスポンスを返送するカスタム DNS レコード。
    - レコードタイプ – DNS レコードのタイプ。これによりレコード値の形式が決定します。これは、CNAME である必要があります。
    - 秒単位の存続時間 – DNS リゾルバーまたはウェブブラウザがオーバーライドレコードをキャッシュし、再度受信された場合にこのクエリに応答して使用するための推奨時間。デフォルトではこの値はゼロであり、レコードはキャッシュされません。

Route 53 Global Resolver のマネージドドメインリスト

マネージドドメインリストには、悪意のあるアクティビティやその他の潜在的な脅威に関連するドメイン名が含まれています。Route 53 Global Resolver のお客様が DNS Firewall を使用する際に、インターネットにバインドされた DNS クエリをチェックできるように、 はこれらのリスト AWS を維持します。

絶えず変化する脅威の状況に遅れずについていくには、時間とコストがかかることがあります。マネージドドメインリストを使用すると、Global Resolver で DNS Firewall を実装して使用する時間を短縮できます。 は、新しい脆弱性や脅威が発生したときにリスト AWS を自動的に更新します。

マネージドドメインリストは脅威カテゴリとコンテンツカテゴリに分類され、一般的なウェブ脅威からユーザーを保護し、safe-for-workでないドメインへのクエリ解決をブロックするように設計されています。

ベストプラクティスとして、本番稼働環境でマネージドドメインリストを使用する前に、ルールアクションを `Alert` に設定して、非本稼働環境でテストを行います。Amazon CloudWatch メトリクスと DNS Firewall のサンプルリクエストまたはグローバルリゾルバーログを組み合わせてルールを評価します。ルールが希望通りであることを確認したら、必要に応じてアクション設定を変更します。

利用可能な AWS マネージドドメインリスト

このセクションでは、グローバルリゾルバーで現在利用可能なマネージドドメインリストについて説明します。 は、脅威またはコンテンツタイプ別に分類されたグローバルリゾルバーのすべてのユーザーに対して、次のマネージドドメインリスト AWS を提供します。

脅威カテゴリ

脅威タイプ
Malware
ボットネット/コマンドとコントロール
脅威リストの集約
Amazon GuardDuty 脅威リスト
フィッシング
スパム

コンテンツカテゴリ

コンテンツタイプ
暴力とヘイトスピーチ

コンテンツタイプ
子供向け
オンライン広告
サイエンス
家族と子育て
Pets
キャリアとジョブの検索
宗教
Lifestyle
ホームとガーデン
犯罪および違法行為
スポーツと娯楽
車両
金融サービス
不動産
趣味と興味
Travel
レストランとレストラン
政府と法律
教育
ファッション

コンテンツタイプ
健康
ショッピング
アダルトコンテンツと成熟コンテンツ
テクノロジーとインターネット
ビジネスと経済
ニュース
検索エンジンとポータル
アートと文化
エンターテインメント
軍事
ソーシャルネットワーキング
プロキシ回避
リダイレクト
E メール
[Translation] (変換)
児童虐待
中止
ギャンブル
ハッキング
マリファナ

コンテンツタイプ
Cryptocurrency
日付
人工知能とMachine Learning
パークされたドメイン
プライベート IP アドレス

マネージドドメインリストは、ダウンロードや閲覧はできません。知的財産を保護するために、マネージドドメインリスト内の個々のドメイン仕様を表示または編集することはできません。この制限はまた、悪意のあるユーザーが具体的に公開されているリストを避けて脅威を作り出すことを防ぐのにも役立ちます。

ブロックまたは許可するドメインのビルドリスト

独自のドメインリストを作成すると、マネージドドメインリストのサービスに見つからないドメインカテゴリや、自分で処理したいドメインカテゴリを指定できます。

このセクションで説明する手順に加えて、 コンソールでは、ルールを作成または更新するときに、DNS Firewall ルール管理のコンテキストでドメインリストを作成できます。

ドメインリストの各ドメイン仕様は、次の要件を満たす必要があります。

- オプションで * (アスタリスク) から始めます。
- ラベル間の区切り文字として、オプションで先頭に付加するアスタリスクとピリオドを除き、使用できるのは `A-Z`、`a-z`、`0-9`、`-` (ハイフン) の各文字だけです。
- 長さは 1～255 文字にする必要があります。

ドメインリストを作成するには

1. Route 53 グローバルリゾルバーコンソールで、グローバルリゾルバーに移動します。
2. ドメインリストタブを選択します。
3. ドメインリストの作成 を選択します。

4. ドメインリストの名前とオプションの説明をタグとともに指定し、ドメインリストの作成を選択します。
5. ドメインリストの作成と運用が完了したら、ドメインの追加を選択してドメインリストへのドメインの追加を開始できます。
6. Amazon S3 バケットからドメインのリストをアップロードすることを選択した場合は、ドメインリストを作成した Amazon S3 バケットの URI を入力します。このドメインリストには、1 行につき 1 つのドメイン名が必要です。
7. それ以外の場合は、テキストボックスにドメイン仕様を 1 行に 1 つずつ入力します。
8. ドメインの追加 を選択します。

ドメインリストを削除するには

1. Route 53 グローバルリゾルバーコンソールで、グローバルリゾルバーに移動します。
2. ドメインリストタブを選択します。
3. 削除するドメインリストを選択し、[削除] をクリックして、削除されたことを確認します。

DNS Firewall Advanced 保護

DNS Firewall Advanced は、DNS クエリの既知の脅威シグネチャに基づいて、疑わしい DNS クエリを検出します。DNS ビューに関連付けられた DNS ファイアウォールルールで使用するルールで脅威タイプを指定できます。

DNS Firewall Advanced は、リクエストのタイムスタンプ、リクエストとレスポンスの頻度、DNS クエリ文字列、アウトバウンドとインバウンドの両方の DNS クエリの長さ、タイプ、サイズなど、DNS ペイロード内のキー識別子の範囲を調べることで、疑わしい DNS 脅威シグネチャを識別します。脅威署名のタイプに基づいて、ブロックするか、単にクエリをログに記録して警告するようにポリシーを設定できます。拡張された脅威識別子のセットを使用することで、より広範なセキュリティコミュニティによって維持されている脅威インテリジェンスフィードによってまだ分類されていないドメインソースからの DNS 脅威から保護できます。

現在、DNS Firewall Advanced は以下からの保護を提供しています。

- ドメイン生成アルゴリズム (DGAs)

  DGAs は、攻撃者が多数のドメインを生成してマルウェア攻撃を開始するために使用されます。
- ディクショナリ DGA

多数のディクショナリ単語に関連付けられたドメイン名を使用して悪意のあるコマンドを実行し、DNS 通信を制御する DGA 攻撃を検出します。

- DNS トンネリング

  DNS トンネリングは、攻撃者がクライアントへのネットワーク接続を行わずに DNS トンネルを使用してクライアントからデータを抽出するために使用されます。

ルールの作成方法については、「」を参照してくださいthe section called “DNS Firewall ルールの設定と管理”。

誤検出シナリオの軽減

DNS Firewall Advanced 保護を使用してクエリをブロックするルールで誤検出のシナリオが発生した場合は、次の手順を実行します。

1. グローバルリゾルバーログで、誤検出の原因となっているルールと DNS Firewall Advanced 保護を特定します。これを行うには、DNS Firewall がブロックしているが、通過を許可するクエリのログを見つけます。ログレコードには、DNS ビュー、ルール、ルールアクション、DNS Firewall Advanced 保護が一覧表示されます。
2. ブロックされたクエリを明示的に許可する新しいルールを DNS ビューに作成します。ルールを作成するときに、許可するドメイン仕様のみを使用して、独自のドメインリストを定義できます。のルール管理のガイダンスに従ってくださいthe section called “DNS Firewall ルールの設定と管理”。
3. マネージドリストを使用しているルールの前に実行されるように、ルール内で新しいルールに優先順位を付けます。これを行うには、新しいルールの優先順位の数値を小さく設定します。

ルールを更新すると、新しいルールはブロッキングルールを実行する前に許可するドメイン名を明示的に許可します。

Route 53 Global Resolver で DNS セキュリティポリシーを管理する

グローバルリゾルバーの管理

グローバルリゾルバーを作成したら、グローバルリゾルバーページから詳細を表示し、設定を編集して、関連するリソースを管理できます。

リゾルバーの詳細の表示

グローバルリゾルバーページには、リゾルバー名、デプロイされたリージョン、関連する DNS ビュー、オブザーバビリティリージョン、運用ステータスなどのキー情報を含むすべてのリゾルバーのリストが表示されます。

グローバルリゾルバーの編集

リゾルバーの名前と説明は、作成後に変更できます。作成後にグローバルリゾルバーがデプロイされるリージョンを変更することはできません。

ファイアウォールルールの管理

ファイアウォールルールを作成したら、優先順位を変更したり、設定を更新したり、必要に応じて削除したりできます。

ルールの優先度と評価順序

ファイアウォールルールは優先順位で評価され、少数が最初に処理されます。クエリが複数のルールに一致する場合、最初に一致するルールのアクションのみが適用されます。

ファイアウォールルールの更新

ファイアウォールルールの優先度、アクション、ターゲットドメインなど、ファイアウォールルールのほとんどの側面は作成後に更新できます。

Route 53 Global Resolver とのプライベートホストゾーンの関連付けの設定

Route 53 Global Resolver を使用すると、承認されたクライアントから Route 53 プライベートホストゾーンに関連付けられたレコードを解決できます。Route 53 プライベートホストゾーンを、クライアントが DNS ビューで許可した DNS ビューに関連付けることができます。

トピック

- Route 53 Global Resolver とのプライベートホストゾーンの関連付けを管理する

Route 53 Global Resolver とのプライベートホストゾーンの関連付けを管理する

内部アプリケーションのプライベートホストゾーンの作成

プライベートホストゾーンを DNS ビューに関連付ける前に、まず Amazon Route 53 コンソールまたは API を使用してゾーンを作成する必要があります。

プライベートホストゾーンを作成するには

1. https://console.aws.amazon.com/route53/ で Amazon Route 53 コンソールを開きます。
2. ナビゲーションペインで [Hosted zones] を選択します。
3. [ホストゾーンの作成] を選択します。
4. ドメイン名には、プライベートゾーンのドメイン名を入力します (例: `internal.example.com`)。
5. [タイプ] には、[プライベートホストゾーン] を選択します。
6. VPCsホストゾーンに関連付けるには、ホストゾーンに関連付ける VPCs を選択します。必要に応じて、代わりにゾーンを Route 53 Global Resolver に関連付けるため、 `CreateHostedZone` API オペレーションを使用して値の入力をスキップできます。
7. [ホストゾーンの作成] を選択します。

プライベートホストゾーンを作成したら、内部サービスに必要な DNS レコードを追加します。

プライベートホストゾーンと DNS ビューの関連付け

Route 53 Global Resolver がプライベートホストゾーンのクエリを解決できるようにするには、ゾーンを 1 つ以上の DNS ビューに関連付ける必要があります。

プライベートホストゾーンを DNS ビューに関連付けるには

1. Route 53 グローバルリゾルバーコンソールで、グローバルリゾルバーに移動します。
2. プライベートホストゾーンを関連付ける DNS ビューを選択します。
3. プライベートホストゾーンセクションで、ホストゾーンの関連付けを選択します。
4. ホストゾーンで、関連付けるプライベートホストゾーンを選択します。
5. 関連付け名には、この関連付けのわかりやすい名前を入力します。

6. ホストゾーンの関連付けを選択します。

関連付けプロセスは通常、完了までに数分かかります。これが完了すると、Route 53 Global Resolver はプライベートホストゾーンのレコードを使用して、DNS ビューに関連付けられたクライアントデバイスからの DNS クエリに応答します。

アカウントのプライベートホストゾーンを、別の AWS アカウントが共有した DNS ビューに関連付けることもできます AWS Resource Access Manager。詳細については、「AWS アカウント間の Route 53 Global Resolver DNS ビューの共有」を参照してください。

AWS アカウント間の Route 53 Global Resolver DNS ビューの共有

Route 53 Global Resolver DNS ビューは、 AWS Resource Access Manager (AWS RAM) を使用して他の AWS アカウントと共有できます。 AWS RAM は、 AWS アカウント または を介して AWS リソースを共有します AWS Organizations。詳細については、「Resource Access Manager ユーザーガイド」を参照してください。

DNS ビューを共有すると、受信アカウント (コンシューマー) は独自の Route 53 プライベートホストゾーンをビューに関連付けることができます。これらのゾーンのレコードは、グローバルリゾルバーを通じて解決されます。コンシューマーは、ホストゾーンまたは DNS ビューの所有権を移管する必要はありません。DNS ビューを所有するアカウント (所有者) は、グローバルリゾルバーと DNS ビューを完全に制御します。所有者はいつでもビューの共有を停止したり、関連付けを削除したりできます。

> **Note**
>
> 共有 DNS ビューは、所有者のグローバルリゾルバー AWS リージョン が実行されるすべての で、コンシューマーのプライベートホストゾーンレコードを DNS 解決に適用します。信頼するアカウントとのみ DNS ビューを共有します。

次の点に注意してください。

所有者がコンシューマーに付与するアクセス許可

DNS ビューを共有するときは、コンシューマーがビューで実行できる操作を定義する AWS RAM 管理アクセス許可を選択します。Route 53 Global Resolver は、`route53globalresolver:dns-view`リソースタイプに対して次の AWS 管理アクセス許可を提供します。

- AWSRAMDefaultPermissionDNSView (デフォルト) – 共有 DNS ビューを表示し、独自のプライベートホストゾーンをビューに関連付けることをコンシューマーに許可します。このアクセス許可により、 `AssociateHostedZone` および `GetDNSView`アクションが許可されます。
- AWSRAMPermissionDNSViewLifecycleManagement – コンシューマーが共有 DNS ビューを表示、更新、有効化、無効化できるようにします。プライベートホストゾーンをビューに関連付けることはできません。
- AWSRAMPermissionDNSViewFullAccess – コンシューマーがプライベートホストゾーンを関連付け、共有 DNS ビューのライフサイクルを管理できるようにします。

これらのアクションの一部のみを付与するカスタマー管理アクセス許可を作成することもできます。詳細については、「 AWS Resource Access Manager ユーザーガイド」の「カスタマー管理アクセス許可の作成」を参照してください。

ホストゾーンの関連付けはコンシューマーが所有します

コンシューマーが共有 DNS ビューに作成するプライベートホストゾーンの関連付けは、コンシューマーのアカウントに属します。DNS ビューの所有者は、これらの関連付けを表示および削除できます。コンシューマーは、作成した関連付けを管理できます。

DNS ビューの共有 (共有解除) の停止

DNS ビューの共有を停止すると、コンシューマーはビューに新しいホストゾーンの関連付けを作成したり、ビューを更新したりできなくなります。ただし、既存の関連付けは自動的に削除されません。所有者またはコンシューマーがそれらを削除するまで、DNS 解決には引き続き影響します。コンシューマーのレコードがすぐに解決されないようにするには、DNS ビューからコンシューマーのホストゾーンの関連付けを削除します。

共有 DNS ビューの削除

共有されている DNS ビューは削除できません。最初にビューの共有を停止してから、削除します。

クォータ

コンシューマーが共有 DNS ビューに作成するホストゾーンの関連付けは、DNS ビューあたりの関連付けの所有者のクォータにカウントされます。現在の Route 53 Global Resolver のクォータについては、「」を参照してくださいRoute 53 Global Resolver のクォータ。

オプトインのデータ AWS リージョン

所有者のグローバルリゾルバーは、コンシューマー AWS リージョン がオンになっていないオプトインで実行される場合があります。コンシューマーがプライベートホストゾーンを共有 DNS ビューに関連付けると、ホストゾーン ID とドメイン名は、所有者のグローバルリゾルバーが実

行されるすべてのリージョンにコピーされます。これには、コンシューマーがオンになっていないオプトインリージョンが含まれます。

所有している DNS ビューの共有

DNS ビューを共有するには、 でリソース共有を作成します AWS RAM。リソース共有は、共有するリソース、適用するマネージドアクセス許可、共有するプリンシパル (アカウント、組織単位、または組織) を指定します。

DNS ビューは、所有している場合にのみ共有できます。共有された DNS ビューを共有することはできません。

- コンソール
- CLI

DNS ビューの共有 (コンソール)

DNS ビューを別の AWS アカウントと共有するには

1. https://console.aws.amazon.com/ram/ で AWS RAM コンソールを開きます。

   > **Note**
   >
   > DNS ビューはグローバルリソースです。リソース共有は、米国東部 (バージニア北部) (us-east-1) リージョンで作成する必要があります。

2. [リソースの共有の作成] を選択します。
3. [Name] (名前) に、リソース共有のわかりやすい名前を入力します。
4. リソースで、Route 53 Global Resolver DNS Views リソースタイプを選択し、共有する DNS ビューを選択します。
5. 管理アクセス許可で、必要なアクセスを許可するアクセス許可を選択します。詳細については、このトピックの前半で所有者がコンシューマーリストに付与するアクセス許可を参照してください。
6. プリンシパルには、DNS ビューを共有する AWS アカウント ID、OU、または組織を入力し、追加を選択します。
7. [リソースの共有の作成] を選択します。

DNS ビューを組織外のアカウントと共有すると AWS Organizations、コンシューマーはリソース共有への招待を受け取ります。コンシューマーは、共有 DNS ビューを使用する前に招待を受け入れる必要があります。

DNS ビューの共有 (CLI)

DNS ビューを共有するには、 コマンドを使用します AWS RAM `create-resource-share`。DNS ビューの ARN とコンシューマーアカウントを指定します。米国東部 (バージニア北部) (`us-east-1`) リージョンで コマンドを実行します。次の の例では、デフォルトの管理アクセス許可222233334444を使用して DNS ビューをアカウントと共有します。

```
aws ram create-resource-share --region us-east-1 --name MyDNSViewShare --resource-arns arn:aws:route53globalresolver::111122223333:dns-view/dnsv-abcdef1234567890 --principals 222233334444
```

より多くのアクセスを許可するには、 `--permission-arns`パラメータに `AWSRAMPermissionDNSViewLifecycleManagement`または `AWSRAMPermissionDNSViewFullAccess`マネージドアクセス許可の ARN を含めます。アクセス許可の ARN を検索するには、 AWS RAM `list-permissions` コマンドを使用します。

自分と共有されている DNS ビューの使用

別のアカウントが DNS ビューを共有したら、送信された招待を受け入れます。その後、独自の Route 53 プライベートホストゾーンを共有 DNS ビューに関連付けることができます。これらのホストゾーンのレコードは、承認されたクライアントの所有者のグローバルリゾルバーを通じて解決されます。

アカウントと共有されている DNS ビューを検索するには、https://console.aws.amazon.com/ram/ で AWS RAM コンソールを開き、共有リソースを選択します。プライベートホストゾーンを共有 DNS ビューにリンクするには、所有している DNS ビューと同じ手順に従います。共有 DNS ビューの ARN を指定します。詳細については、「Route 53 Global Resolver とのプライベートホストゾーンの関連付けの設定」を参照してください。

共有されている DNS ビューについては、次の点に注意してください。

- 独自のプライベートホストゾーンの関連付けと関連付け解除を行うことができます。所有者がそれらのアクションを許可する管理アクセス許可を付与しない限り、DNS ビュー自体を変更または削除することはできません。
- 作成したプライベートホストゾーンの関連付けは、アカウントに属します。表示、更新、削除できます。

- 所有者が DNS ビューの共有を停止すると、ビューに新しい関連付けを作成できなくなります。ただし、既存の関連付けは、ユーザーまたは所有者がそれらを削除するまで引き続き機能します。

Route 53 Global Resolver による DNS アクティビティとパフォーマンスのモニタリング

Route 53 Global Resolver は、組織全体の DNS アクティビティを包括的に可視化し、セキュリティ脅威の特定、クライアントデバイスの動作の分析、コンプライアンスの維持を可能にします。この章では、DNS モニタリングの設定、ログ記録の送信先の設定、DNS データの分析のための利用可能なモニタリングツールと詳細な手順の両方について説明し、脅威を調査してパフォーマンスを最適化します。

AWS には、安全で信頼性の高い DNS サービスの維持に役立つ以下のモニタリングツールが用意されています。

- Amazon CloudWatch Logs では、Amazon EC2 インスタンス、CloudTrail、およびその他のソースからのログファイルをモニタリング、保存、およびアクセスできます。Route 53 Global Resolver は、DNS クエリログを CloudWatch Logs に直接配信して、リアルタイムのモニタリングと分析を行うことができます。高い耐久性を備えたストレージにログデータをアーカイブすることもできます。詳細については、「Amazon CloudWatch Logs ユーザーガイド」を参照してください。
  - メトリクスフィルターを使用して、CloudWatch Logs に入るログデータを検索およびフィルタリングし、ログイベントから CloudWatch メトリクスを作成できます。これらのメトリクスを使用して、DNS クエリボリューム、応答時間、セキュリティイベントを追跡します。ロケーション間で DNS パフォーマンスをモニタリングするダッシュボードを作成し、クエリボリュームの急増や応答時間の増加を通知するアラームを設定することもできます。詳細については、「Amazon CloudWatch ユーザーガイド」を参照してください。
- Amazon EventBridge を使用して AWS サービスを自動化し、アプリケーションの可用性の問題やリソースの変更などのシステムイベントに自動的に対応できます。 AWS サービスからのイベントは、ほぼリアルタイムで EventBridge に配信されます。簡単なルールを記述して、注目するイベントと、イベントがルールに一致した場合に自動的に実行するアクションを指定できます。詳細については、「Amazon EventBridge ユーザーガイド」を参照してください。
- AWS CloudTrail は、 AWS アカウントによって、またはアカウントに代わって行われた API コールおよび関連イベントをキャプチャし、指定した Amazon S3 バケットにログファイルを配信します。呼び出し元のユーザーとアカウント AWS、呼び出し元の送信元 IP アドレス、呼び出しの発生日時を特定できます。詳細については、「AWS CloudTrail ユーザーガイド」を参照してください。

Route 53 Global Resolver ログから Amazon CloudWatch メトリクス、アラーム、分析を作成する方法については、「」を参照してくださいthe section called “CloudWatch によるモニタリング”。

トピック

- Route 53 Global Resolver を使用して DNS アクティビティを可視化する
- Route 53 Global Resolver で DNS モニタリングと ログ記録を設定する
- Amazon CloudWatch による Route 53 Global Resolver のモニタリング

Route 53 Global Resolver を使用して DNS アクティビティを可視化する

Route 53 Global Resolver は、クライアントデバイスのアクティビティをモニタリングし、セキュリティの脅威を特定するための包括的な DNS クエリログ記録機能を提供します。Route 53 Global Resolver で DNS クエリログ記録を有効にして、クライアントデバイスがどのウェブサイトにアクセスするかを確認し、潜在的なセキュリティ脅威を特定し、DNS 解決パターンを分析します。ログは、適用されたセキュリティポリシーなど、各クエリに関する包括的な情報をキャプチャします。

DNS ログにキャプチャされる情報

各 DNS クエリログエントリは、クライアントデバイスのアクティビティとセキュリティポリシーの適用に関する詳細情報を提供します。

- クエリ情報 - ドメイン名、クエリタイプ、クエリクラス、および使用されるプロトコル
- クライアントデバイス情報 - ソース IP アドレス、DNS ビュー、認証方法
- 応答情報 - 応答コード、応答レコード、応答時間
- セキュリティアクション - ファイアウォールルールの一致、脅威検出結果、実行されたアクション
- メタデータ - タイムスタンプ、グローバルリゾルバー ID、リージョン、トレース情報

セキュリティ統合用の OCSF 形式

DNS クエリログは、セキュリティイベントデータの標準化された形式を提供する Open Cybersecurity Schema Framework (OCSF) を使用します。この形式により、以下が可能になります。

- 標準化された分析 - さまざまなセキュリティツールにまたがる一貫したスキーマ
- 相互運用性の向上 - SIEM および分析プラットフォームとの簡単な統合
- 相関の強化 - DNS イベントを他のセキュリティデータと相関させる機能

- 将来の互換性 - 進化するセキュリティ分析要件のサポート

OCSF ログ形式の例

Route 53 Global Resolver DNS クエリログは OCSF スキーマ構造に従い、各 DNS クエリ、レスポンス、セキュリティアクションに関する詳細情報を提供します。次の例は、許可されたクエリと拒否されたクエリのログ形式を示しています。

Route 53 Global Resolver DNS ログ - アクセス許可の例

この例では、ファイアウォールルールを通じて許可された DNS クエリを示しています。ログには、Route 53 Global Resolver 固有の識別子を含むクエリの詳細、レスポンス情報、エンリッチメントデータが含まれます。


```
{
    "action_id": 1,
    "action_name": "Allowed",
    "activity_id": 6,
    "activity_name": "Traffic",
    "category_name": "Network Activity",
    "category_uid": 4,
    "class_name": "DNS Activity",
    "class_uid": 4003,
    "cloud": {
        "provider": "AWS",
        "region": "us-east-1",
        "account": {
            "uid": "123456789012"
        }
    },
    "connection_info": {
        "direction": "Inbound",
        "direction_id": 1,
        "protocol_name": "udp",
        "protocol_num": 17,
        "protocol_ver": "",
        "uid": "db21d1739ddb423a"
    },
    "duration": 1,
    "end_time": 1761358379996,
    "answers": [{
        "rdata": "3.3.3.3",
```

```
        "type": "A",
        "class": "IN",
        "ttl": 300
    },
    {
        "rdata": "3.3.3.4",
        "type": "A",
        "class": "IN",
        "ttl": 300
    }],
    "src_endpoint": {
        "ip": "3.3.3.1",
        "port": 56576
    },
    "enrichments": [{
        "name": "global-resolver",
        "value": "gr-a1b2c3d4fexample",
        "data": {
            "dns_view_id": "dnsv-a1b2c3d4fexample",
            "firewall_rule_id": "fr-a1b2c3d4fexample",
            "token_id": "t-a1b2c3d4fexample",
            "token_name": "device-123456",
            "token_expiration": "1789419206",
            "access_source_cidr": "3.3.3.0/24",
        }
    }],
    "message": "",
    "metadata": {
        "version": "1.2.0",
        "product": {
            "name": "Global Resolver",
            "vendor_name": "AWS",
            "feature": {
                "name": "DNS"
            }
        }
    },
    "query": {
        "hostname": "example.com.",
        "class": "IN",
        "type": "A",
        "opcode": "Query",
        "opcode_id": 0
    },
```

```
    "query_time": 1761358379995,
    "rcode": "NOERROR",
    "rcode_id": 0,
    "response_time": 1761358379995,
    "severity": "Informational",
    "severity_id": 1,
    "src_endpoint": {
        "ip": "3.3.3.3",
        "port": 28276
    },
    "start_time": 1761358379995,
    "status": "Success",
    "status_id": 1,
    "time": 1761358379995,
    "type_name": "DNS Activity: Traffic",
    "type_uid": 400306
}
```


Route 53 Global Resolver DNS ログ - アクセス拒否の例

この例では、ファイアウォールルールによってブロックされた DNS クエリを示しています。ログには、拒否アクション、空の回答配列、およびクエリが処理されなかったことを示す REFUSED レスポンスコードが含まれます。


```
{
    "action_id": 2,
    "action_name": "Denied",
    "activity_id": 6,
    "activity_name": "Traffic",
    "category_name": "Network Activity",
    "category_uid": 4,
    "class_name": "DNS Activity",
    "class_uid": 4003,
    "cloud": {
        "provider": "AWS",
        "region": "us-west-2",
        "account": {
            "uid": "123456789012"
        }
    },
    "connection_info": {
        "direction": "Inbound",
        "direction_id": 1,
```

```
        "protocol_name": "tcp",
        "protocol_num": 6,
        "protocol_ver_id": 4,
        "uid": "9fdc6fbc09794d5e"
    },
    "duration": 1,
    "end_time": 1761358379996,
    "answers": [],
    "src_endpoint": {
        "ip": "3.3.3.3",
        "port": 28276
    },
    "enrichments": [
        {
            "name": "global-resolver",
            "value": "gr-a1b2c3d4fexample",
            "data": {
                "dns_view_id": "dnsv-a1b2c3d4fexample",
                "firewall_rule_id": "fr-a1b2c3d4fexample",
                "token_id": "t-a1b2c3d4fexample",
                "token_name": "device-123456",
                "token_expiration": "1789419206",
                "access_source_cidr": "3.3.3.0/24",
            }
        }
    ],
    "message": "",
    "metadata": {
        "version": "1.2.0",
        "product": {
            "name": "Global Resolver",
            "vendor_name": "AWS",
            "feature": {
                "name": "DNS"
            }
        }
    },
    "query": {
        "hostname": "example.com.",
        "class": "IN",
        "type": "A",
        "opcode": "Query",
        "opcode_id": 0
    },
```

```
    "query_time": 1761358379995,
    "rcode": "REFUSED",
    "rcode_id": 5,
    "response_time": 1761358379995,
    "severity": "Informational",
    "severity_id": 1,
    "start_time": 1761358379995,
    "status": "Failure",
    "status_id": 1,
    "time": 1761358379995,
    "type_name": "DNS Activity: Traffic",
    "type_uid": 400306
}
```


Route 53 Global Resolver で DNS モニタリングとログ記録を設定する

Route 53 Global Resolver で DNS モニタリングを設定して、DNS クエリ、レスポンス、セキュリティアクションに関する詳細情報をキャプチャします。このセクションでは、ログ記録の送信先を設定し、モニタリングツールを設定する手順について説明します。

オブザーバビリティリージョンの設定

DNS ログ記録を設定する前に、ログとメトリクスが保存されるオブザーバビリティリージョンを設定する必要があります。このリージョンによって、モニタリングデータが処理および保存される場所が決まります。

1. https://console.aws.amazon.com/route53globalresolver/ で Route 53 Global Resolver コンソールを開きます。
2. ナビゲーションペインで [設定] を選択します。
3. 「オブザーバビリティリージョン」セクションで、「リージョンの設定」を選択します。
4. モニタリングデータを保存する AWS リージョンを選択し、リージョンの設定を選択します。

オブザーバビリティリージョンを設定したら、そのリージョンでログ配信先を設定できます。

DNS モニタリングとログ配信を設定したら、Route 53 Global Resolver ログから Amazon CloudWatch メトリクスとアラームを作成できます。詳細については、「the section called “CloudWatch によるモニタリング”」を参照してください。

Amazon CloudWatch による Route 53 Global Resolver のモニタリング

Route 53 Global Resolver DNS は、クエリログデータを Amazon CloudWatch Logs に直接発行します。CloudWatch Logs を使用すると、ログデータを検索および分析し、データ内で検索するパターンを定義するメトリクスフィルターを作成し、それらのメトリクスフィルターに基づいて通知を送信するアラームを設定できます。Amazon CloudWatch Logs の詳細については、Amazon CloudWatch Logs とは」を参照してください。

CloudWatch Logs が収集する他のログイベントと同様に、Route 53 Global Resolver DNS クエリログレコードを処理できます。ログデータとメトリクスフィルターのモニタリングの詳細については、Amazon CloudWatch Logs ユーザーガイド」の「フィルターを使用したログイベントからのメトリクスの作成」を参照してください。

トピック

- 例: ブロックされた DNS クエリの Amazon CloudWatch メトリクスフィルターとアラームを作成する
- メトリクスフィルターの例
- DNS クエリログから CloudWatch メトリクスを発行するための IAM ロール
- Route 53 Global Resolver データでの Amazon CloudWatch Contributor Insights の使用
- Amazon CloudWatch Logs Insights を使用した Route 53 Global Resolver ログの分析

例: ブロックされた DNS クエリの Amazon CloudWatch メトリクスフィルターとアラームを作成する

次の例は、Route 53 Global Resolver ログでブロックされた DNS クエリをカウントするメトリクスフィルターを作成する方法を示しています。また、1 時間以内に 10 件以上のブロックされたクエリが発生したときに通知するアラームを作成する方法も示します。

ステップ 1: メトリクスフィルターを作成する

1. CloudWatch コンソールの https://console.aws.amazon.com/cloudwatch/ を開いてください。
2. ナビゲーションペインで、[ログ]、[ロググループ] の順に選択します。
3. Route 53 Global Resolver に設定したオブザーバビリティリージョンにある Route 53 Global Resolver ロググループを選択し、アクション、メトリクスフィルターの作成を選択します。
4. フィルターパターンには、次のように入力します。これは、ファイアウォールルールが DNS クエリをブロックしたログエントリと一致します。`{ $.disposition = "Blocked" }`

5. パターンが機能することを確認するには、「テストするログデータの選択」でログストリームを選択し、「テストパターン」を選択します。
6. [次へ] を選択します。
7. フィルター名を指定し、メトリクス名前空間を に設定しRoute53GlobalResolver、メトリクス名を指定します。
8. ブロックされた各クエリがカウントを増分するように、メトリクス値を 1 に設定します。
9. ディメンションを選択し、カスタムディメンションを追加します。ディメンション名と値は、次のいずれかになります。

   Route 53 Global Resolver ログのメトリクスフィルターディメンション

ディメンション名	値
DNSViewId	$.enrichments[0].data.dns_view_id
AccessTokenId	$.enrichments[0].data.token_id
AccessSourceCidr	$.enrichments[0].data.access_source_cidr
GlobalResolverId	$.enrichments[0].value

10. Next、Create metric filter を選択します。

ステップ 2: アラームを作成する

1. ナビゲーションペインで、[アラーム]、[すべてのアラーム] の順に選択します。
2. [アラームの作成] を選択します。
3. 作成したメトリクスを検索して選択し、メトリクスの選択を選択します。
4. アラームを次のように設定し、次へを選択します。

   - 統計 では、合計 を選択して、ブロックされたすべてのクエリをウィンドウにカウントします。
   - [期間] で、[1 時間] を選択します。
   - [Whenever] で、[Greater/Equal] を選択し、しきい値は「10」と入力します。
   - [追加設定]、[Datapoints to alarm] はデフォルトの「1」のままにしておきます。

5. 通知を受信する Amazon SNS トピックを選択または作成します。[次へ] を選択します。
6. 次のページで、アラームの名前と説明を入力し、[次へ] を選択します。
7. 設定を確認し、アラームの作成を選択します。

メトリクスフィルターの例

このセクションでは、Route 53 Global Resolver DNS クエリログのメトリクスフィルターパターンの例と Amazon CloudWatch Logs Insights クエリについて説明します。

Global Resolver によるブロックされたクエリ

```
{
 "logGroupName": "/aws/vendedlogs/route53globalresolver/global-resolver/
GLOBAL_RESOLVER_LOGS/gr-<resolverId>",
 "filterName": "BlockedQueriesByGlobalResolverId",
 "filterPattern": "{ $.disposition = \"Blocked\" }",
 "metricTransformations": [
   {
     "metricName": "BlockedQueriesByGlobalResolverId",
     "metricNamespace": "Route53GlobalResolver",
     "metricValue": "1",
     "dimensions": { "GlobalResolverId": "$.enrichments[0].value" }
   }
 ]
}
```

アクセスソースで許可されるクエリ

```
{
 "logGroupName": "/aws/vendedlogs/route53globalresolver/global-resolver/
GLOBAL_RESOLVER_LOGS/gr-<resolverId>",
 "filterName": "AllowedQueriesByAccessSourceCidr",
 "filterPattern": "{ $.disposition = \"Allowed\" }",
 "metricTransformations": [
   {
     "metricName": "AllowedQueriesByAccessSourceCidr",
     "metricNamespace": "Route53GlobalResolver",
     "metricValue": "1",
     "dimensions": { "AccessSourceCidr": "$.enrichments[0].data.access_source_cidr" }
   }
 ]
```

```
}
```

アクセストークンによるアラートクエリ

```
{
 "logGroupName": "/aws/vendedlogs/route53globalresolver/global-resolver/
GLOBAL_RESOLVER_LOGS/gr-<resolverId>",
 "filterName": "AlertQueriesByAccessTokenId",
 "filterPattern": "{ $.disposition = \"Alert\" }",
 "metricTransformations": [
   {
     "metricName": "AlertQueriesByAccessTokenId",
     "metricNamespace": "Route53GlobalResolver",
     "metricValue": "1",
     "dimensions": { "AccessTokenId": "$.enrichments[0].data.token_id" }
   }
 ]
}
```

DNS ビュー別のクエリの合計数

```
{
 "logGroupName": "/aws/vendedlogs/route53globalresolver/global-resolver/
GLOBAL_RESOLVER_LOGS/gr-<resolverId>",
 "filterName": "TotalQueriesByDNSViewId",
 "filterPattern": "{ $.query_time = * }",
 "metricTransformations": [
   {
     "metricName": "TotalQueriesByDNSViewId",
     "metricNamespace": "Route53GlobalResolver",
     "metricValue": "1",
     "dimensions": { "DNSViewId": "$.enrichments[0].data.dns_view_id" }
   }
 ]
}
```

グローバルリゾルバーによる SERVFAIL

```
{
 "logGroupName": "/aws/vendedlogs/route53globalresolver/global-resolver/
GLOBAL_RESOLVER_LOGS/gr-<resolverId>",
 "filterName": "ServfailQueriesByGlobalResolverId",
```

```
 "filterPattern": "{ $.rcode = \"SERVFAIL\" }",
 "metricTransformations": [
   {
     "metricName": "ServfailQueriesByGlobalResolverId",
     "metricNamespace": "Route53GlobalResolver",
     "metricValue": "1",
     "dimensions": { "GlobalResolverId": "$.enrichments[0].value" }
   }
 ]
}
```

アクセスソースによって拒否

```
{
 "logGroupName": "/aws/vendedlogs/route53globalresolver/global-resolver/
GLOBAL_RESOLVER_LOGS/gr-<resolverId>",
 "filterName": "RefusedQueriesByAccessSourceCidr",
 "filterPattern": "{ $.rcode = \"REFUSED\" }",
 "metricTransformations": [
   {
     "metricName": "RefusedQueriesByAccessSourceCidr",
     "metricNamespace": "Route53GlobalResolver",
     "metricValue": "1",
     "dimensions": { "AccessSourceCidr": "$.enrichments[0].data.access_source_cidr" }
   }
 ]
}
```

アクセストークン別の NXDOMAIN

```
{
 "logGroupName": "/aws/vendedlogs/route53globalresolver/global-resolver/
GLOBAL_RESOLVER_LOGS/gr-<resolverId>",
 "filterName": "NxdomainQueriesByAccessTokenId",
 "filterPattern": "{ $.rcode = \"NXDOMAIN\" }",
 "metricTransformations": [
   {
     "metricName": "NxdomainQueriesByAccessTokenId",
     "metricNamespace": "Route53GlobalResolver",
     "metricValue": "1",
     "dimensions": { "AccessTokenId": "$.enrichments[0].data.token_id" }
   }
 ]
```

```
}
```

DNS ビュー別の NOERROR

```
{
 "logGroupName": "/aws/vendedlogs/route53globalresolver/global-resolver/
GLOBAL_RESOLVER_LOGS/gr-<resolverId>",
 "filterName": "NoerrorQueriesByDNSViewId",
 "filterPattern": "{ $.rcode = \"NOERROR\" }",
 "metricTransformations": [
   {
     "metricName": "NoerrorQueriesByDNSViewId",
     "metricNamespace": "Route53GlobalResolver",
     "metricValue": "1",
     "dimensions": { "DNSViewId": "$.enrichments[0].data.dns_view_id" }
   }
 ]
}
```

P90 応答時間の Amazon CloudWatch Logs Insights クエリ

グローバルリゾルバー別の P90 応答時間

```
fields @timestamp,
      enrichments.0.value as GlobalResolverId,
      (response_time - query_time) as ResponseTime
| filter ispresent(response_time) and ispresent(query_time)
| stats pct(ResponseTime, 90) as P90ResponseTime by GlobalResolverId
```

アクセストークンによるトークンの有効期限が切れるまでの日数

```
fields @timestamp,
      enrichments.0.data.token_id as AccessTokenId,
      enrichments.0.data.token_ttl_days as DaysUntilExpiry
| filter ispresent(enrichments.0.data.token_ttl_days)
| stats latest(DaysUntilExpiry) by AccessTokenId
```

DNS クエリログから CloudWatch メトリクスを発行するための IAM ロール

IAM ロールまたはユーザーにアタッチされている AWS Identity and Access Management (IAM) ポリシーには、少なくとも次のアクセス許可が含まれている必要があります。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CloudWatchMetricFilterPermissions",
            "Effect": "Allow",
            "Action": [
                "logs:PutMetricFilter",
                "logs:DescribeMetricFilters",
                "logs:DeleteMetricFilter",
                "logs:TestMetricFilter"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CloudWatchLogsInsightsPermissions",
            "Effect": "Allow",
            "Action": [
                "logs:StartQuery",
                "logs:StopQuery",
                "logs:GetQueryResults",
                "logs:DescribeQueries",
                "logs:DescribeLogGroups"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CloudWatchMetricsNamespacePermissions",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData",
                "cloudwatch:GetMetricData",
                "cloudwatch:ListMetrics"
            ],
            "Resource": "*"
        }
    ]
}
```

Route 53 Global Resolver データでの Amazon CloudWatch Contributor Insights の使用

Amazon CloudWatch Contributor Insights はログデータを分析し、コントリビューターデータを表示する時系列を作成します。トップ N コントリビューター、一意のコントリビューターの合計数、およびそれらの使用状況に関するメトリクスを確認できます。この情報は、システムにとって最も影響の大きい要因を見つけるのに役立ちます。Route 53 Global Resolver DNS クエリログを使用すると、Contributor Insights を使用して、DNS トラフィックに対する上位のクエリソース、最もブロックされたドメイン、最もノイズの多いアクセストークン、およびその他の影響の大きい寄与要因を特定できます。詳細については、「Contributor Insights を使用した高カーディナリティデータの分析」を参照してください。

1. 開始する前に、グローバルリゾルバーの DNS クエリログ記録を設定して、クエリログを Amazon CloudWatch Logs に配信します。詳細については、「the section called “DNS モニタリングの設定”」を参照してください。
2. コンソールで、Route 53、Route 53 Global Resolver、Global Resolver に移動します。必要なグローバルリゾルバーを選択し、分析タブを選択します。

   > **Note**
   >
   > 分析タブから Contributor Insights と Logs Insights の両方にアクセスできます。個々のルールグループを選択して分析を表示することもできます。

3. Contributor Insights を選択し、ルールを作成します。詳細については、「Contributor Insights ルールを作成する」を参照してください。
4. Route 53 Global Resolver クエリログを含むロググループを選択します。
5. [Rule type] (ルールタイプ) で、[Sample rule] (サンプルルール) を選択します。次に、サンプルルールの選択を選択し、Route 53 グローバルリゾルバーログのサンプルルールのいずれかを選択します。

   > **Note**
   >
   > グローバルリゾルバー ID をルール名に含めて、ルールが適用されるグローバルリゾルバーを特定できるようにします。

6. サンプルルールのいずれかを選択すると、CloudWatch ルールページのすべての必須フィールドが入力されます。

7. 結果のメトリクスを表示するには、CloudWatch コンソールを開き、メトリクス、すべてのメトリクスを選択し、DNS Firewall メトリクスを含む Route 53 Resolver 名前空間を探します。

Amazon CloudWatch Logs Insights を使用した Route 53 Global Resolver ログの分析

Amazon CloudWatch Logs Insights を使用すると、Route 53 Global Resolver ログデータをクエリでインタラクティブに検索および分析できます。クエリを実行して運用上の問題に対応し、DNS トラフィックのパターンを特定できます。詳細については、「CloudWatch Logs Insights を使用したログデータの分析」を参照してください。

1. 開始する前に、グローバルリゾルバーの DNS クエリログ記録を設定して、クエリログを Amazon CloudWatch Logs に配信します。詳細については、「the section called “DNS モニタリングの設定”」を参照してください。
2. コンソールで、Route 53、Route 53 Global Resolver、Global Resolver に移動します。必要なグローバルリゾルバーを選択し、分析タブを選択し、Logs Insights を選択します。
3. 分析するロググループを 1 つ以上選択します。DNS クエリログ記録を設定すると、グローバルリゾルバーはクエリログをこれらのロググループに配信します。
4. 分析するディメンションを選択します。メトリクスとアクションの 2 つのディメンションから選択できます。または、独自の CloudWatch Logs Insights クエリを入力して、他の方法でログデータを分析することもできます。

Route 53 Global Resolver の DNS 問題のトラブルシューティング

Route 53 Global Resolver には包括的な DNS 解決機能がありますが、接続、パフォーマンス、または設定の問題をトラブルシューティングする必要がある場合があります。DNS ログ、モニタリングデータ、診断手法を使用して、Route 53 Global Resolver でクライアントデバイスの DNS 解決に影響する問題を特定して解決します。この章では、一般的な DNS 問題をトラブルシューティングし、パフォーマンスを最適化するための体系的なアプローチについて説明します。

トピック

- Route 53 Global Resolver の DNS 接続の問題の診断
- Route 53 Global Resolver の DNS パフォーマンスの問題を解決する
- Route 53 Global Resolver の設定問題のトラブルシューティング
- 内部リソースアクセスのトラブルシューティング

Route 53 Global Resolver の DNS 接続の問題の診断

Route 53 Global Resolver は信頼性の高い DNS 解決を提供しますが、設定、認証、またはネットワークの問題が原因で接続の問題が発生することがあります。クライアントデバイスが Route 53 Global Resolver を使用してドメイン名を解決できない場合は、これらの体系的なアプローチを使用して接続の問題を特定して解決します。

クライアントデバイスがドメインを解決できない

解決の失敗を診断するには、次の手順に従います。

1. クエリがグローバルリゾルバーに到達することを確認する
   - DNS クエリログで、影響を受けるクライアントデバイスの IP アドレスからのクエリを確認する
   - クライアントデバイスが正しいエニーキャスト IP アドレスで設定されていることを確認します。
   - クライアントデバイスからエニーキャスト IPs
2. クライアントデバイスの認証を確認する
   - クライアントデバイスが正しい DNS ビューに対して認証されていることを確認します。
   - クライアントデバイスの IP アドレスまたは CIDR ブロックのアクセスソースルールを確認する
   - アクセストークンが有効で有効期限が切れていないことを確認する (トークンベースの認証の場合)
3. ファイアウォールルールを確認する
   - ファイアウォールルールがクエリをブロックしているかどうかを確認します。
   - ルールの優先度を確認し、許可ルールの優先度がブロックルールよりも高いことを確認します。
   - ファイアウォールのフェイルオープン動作設定を確認する
4. DNS ビューの関連付けを確認する
   - 内部ドメインのプライベートホストゾーンの関連付けを検証する
   - 関連付けられたプライベートホストゾーンに DNS レコードが存在することを確認する
   - クエリのドメイン名がゾーン名と完全に一致することを確認する

断続的な解決の失敗

散発的な DNS 解決の問題については、以下の潜在的な原因を調査します。

認証問題

- アクセストークンの有効期限と更新パターンを確認する
- 失敗した認証試行の認証ログを確認する
- トークン検証のためにクライアントデバイスのクロック同期を検証する

ネットワーク接続

- ネットワークパスの変更やルーティングの問題を監視する
- ファイアウォールまたは NAT デバイスの設定変更を確認する
- 最も近いリージョンへの一貫した工二ーキャストルーティングを検証する

サービス状態

- Route 53 Global Resolver の問題に関する AWS サービスヘルスダッシュボードの確認
- エラー率の急増について CloudWatch メトリクスを確認する
- プライベートホストゾーンの関連付けステータスをモニタリングする

予期しないパブリック解決

クエリがプライベートホストゾーンではなくパブリック DNS に解決される場合:

1. プライベートホストゾーンの設定を確認する
   - プライベートホストゾーンに予想される DNS レコードが含まれていることを確認する
   - レコード名がクエリされたドメインと完全に一致することを確認する
   - レコードタイプがクエリタイプ (A、AAAA、CNAME など) と一致することを確認する
2. DNS ビューの関連付けを確認する
   - プライベートホストゾーンが正しい DNS ビューに関連付けられていることを確認する
   - クライアントデバイスが DNS ビューに対して認証されていることを確認します。
   - コンソールで関連付けステータスを確認する
3. ファイアウォールルールを確認する
   - プライベートゾーンクエリをブロックしている可能性のあるファイアウォールルールを確認する
   - ルール評価の順序と優先度を検証する
   - ファイアウォールアクションの DNS クエリログを確認する

Route 53 Global Resolver の DNS パフォーマンスの問題を解決する

Route 53 Global Resolver は、グローバルエニーキャストアーキテクチャで最適なパフォーマンスを実現するように設計されていますが、さまざまな要因が DNS 解決速度に影響を与える可能性があります。Route 53 Global Resolver を使用して、DNS 解決の遅延に対処し、クエリ応答時間を最適化してクライアントデバイスのパフォーマンスを向上させます。

DNS 解決が遅い

遅い DNS 応答時間を診断して解決するには:

1. クエリの応答時間を分析する
   - DNS クエリログを使用して応答時間が長いクエリを特定する
   - 異なるドメインとクエリタイプ間で応答時間を比較する
   - 時間の経過に伴う応答時間の傾向をモニタリングする
2. クエリボリュームが多いかどうかを確認する
   - クエリボリュームの急増について CloudWatch メトリクスをモニタリングする
   - 過剰なクエリを生成するクライアントデバイスまたは DNS ビューを特定する
   - 設定ミスを示す可能性のあるクエリパターンを探す
3. キャッシュパフォーマンスを確認する
   - 頻繁にクエリされるドメインのキャッシュヒット率を分析する
   - DNS レコードの TTL 設定を確認する
   - クエリパターンに基づいて TTL 値を調整することを検討してください
4. 最適なリージョンの選択を検証する
   - グローバルリゾルバーリージョンがクライアントデバイスの口ケーションに近いことを確認する
   - エニーキャストルーティングをモニタリングして、クエリが最寄りのリージョンに到達することを確認する
   - クライアントデバイスが地理的に離れている場合は、リージョンの追加を検討してください。

パフォーマンス最適化戦略

DNS のパフォーマンスを最適化するには、次の戦略を使用します。

キャッシュの最適化

- クエリパターンと変更頻度に基づいて TTL 値を調整する
- 安定したレコードTTLs を使用し、頻繁に変化するレコードには短い TTLsを使用します。
- キャッシュヒット率をモニタリングし、それに応じて TTLsを調整する

リージョンの最適化

- クライアントデバイスの濃度に最も近いリージョンにグローバルリゾルバーをデプロイする
- リージョン別のクエリルーティングパターンと応答時間をモニタリングする
- 地理的カバレッジを向上させるためにリージョンを追加することを検討する

プロトコルの最適化

- セキュリティとパフォーマンスの要件に基づいて適切な DNS プロトコルを選択する
- キャッシュの利点がある暗号化された接続に DNS-over-HTTPS (DoH) を検討する
- オーバーヘッドの少ない暗号化された接続に DNS-over-TLS (DoT) を使用する

ルールの最適化

- ファイアウォールルールの優先度と複雑さを確認して最適化する
- 頻繁に一致するルールを優先度の高い順序で配置する
- 可能な場合は複雑なルール条件を簡素化する

Route 53 Global Resolver の設定問題のトラブルシューティング

Route 53 Global Resolver には、DNS ビュー、認証、ファイアウォールルールの広範な設定オプションが用意されており、設定の競合や不一致が発生する可能性があります。DNS 解決に影響する Route 53 Global Resolver の一般的な設定問題を特定して解決します。

認証の問題

一般的な認証の問題と解決策:

アクセスソースルールの不一致

- クライアントデバイスの IP アドレスが設定済み CIDR ブロックと一致することを確認する
- ソース IP アドレスを変更する NAT またはプロキシデバイスを確認する
- アクセスソースルールが、予想されるクライアントデバイスの IP 範囲をすべてカバーしていることを確認します。

トークン認証の失敗

- クライアントデバイスでトークンが正しく設定されていることを確認する
- トークンの有効期限と更新プロセスを確認する
- クライアントデバイスクロックがトークン検証用に同期されていることを確認します。

プロトコルの不一致

- クライアントデバイスがアクセスソースルールで許可されているプロトコルを使用していることを確認する
- DoH と DoT の設定がトークンプロトコルと一致することを確認する
- ファイアウォールルールが必要なプロトコルをブロックしないようにする

DNS ビュー設定の問題

DNS ビュー設定の一般的な問題:

DNS ビューの関連付けが正しくない

- クライアントデバイスが目的の DNS ビューに対して認証されていることを確認する
- プライベートホストゾーンが正しい DNS ビューに関連付けられていることを確認します。
- 各 DNS ビューに適用されるファイアウォールルールを確認する

DNS 設定の競合

- DNSSEC 検証設定でクライアントデバイスとの互換性を確認する
- EDNS クライアントサブネットの設定でプライバシーとパフォーマンスのバランスを確認する
- ファイアウォールのフェイルオープン動作がセキュリティ要件と一致していることを確認する

ファイアウォールルールの問題

ファイアウォールルール設定の一般的な問題:

ルールの優先度の競合

- ルールの評価順序を確認し、正しい優先度の割り当てを検証する
- 意図した許可ルールよりも高い優先度のブロックルールを確認する
- 本番環境のデプロイ前に、制御された環境でルールの変更をテストする

ドメインリストの不一致

- カスタムドメインリストでドメイン仕様を検証する

- ワイルドカードパターンで正しい構文とカバレッジを確認する
- ドメインリストが更新され、同期されていることを確認する

内部リソースアクセスのトラブルシューティング

内部リソースアクセスを管理する際の一般的な問題と解決策:

クライアントデバイスがプライベートゾーンレコードに解決されない

- プライベートホストゾーンが正しい DNS ビューに関連付けられていることを確認する
- クライアントデバイスが正しい DNS ビューに対して認証されていることを確認します。
- クエリのドメイン名がゾーン名と完全に一致することを確認します。
- DNS レコードがプライベートホストゾーンに存在することを確認する

断続的な解決の失敗

- コンソールで関連付けステータスを確認する
- DNS クエリログでエラーパターンを確認する
- Route 53 Global Resolver と Amazon Route 53 間のネットワーク接続を検証する

予期しないパブリック解決

- プライベートホストゾーンに期待されるレコードが含まれていることを確認する
- クエリをブロックしている可能性のあるファイアウォールルールを確認する
- クエリが DNS ビューに関連付けられたクライアントデバイスから送信されていることを確認します。

Route 53 Global Resolver のクォータ

AWS アカウントには、 AWS サービスごとに、以前は制限と呼ばれていたデフォルトのクォータがあります。特に明記していない限り、クォータはリージョン固有です。一部のクォータについては、引き上げをリクエストできます。他のクォータを増やすことはできません。

Route 53 Global Resolver のクォータを表示するには、Service Quotas コンソールを開きます。ナビゲーションペインで、AWS サービスを選択し、Route 53 Global Resolver を選択します。

クォータの引き上げをリクエストするには、Service Quotas ユーザーガイド の「クォータ引き上げリクエスト」を参照してください。Service Quotas でクォータがまだ利用できない場合は、[上限引き上げ] フォームを使用してください。

AWS アカウントには、Route 53 Global Resolver に関連する次のクォータがあります。

ソフトクォータ

次の表は、Route 53 Global Resolver で引き上げることができるクォータを示しています。クォータを変更するには、Service Quotas ユーザーガイド」の「クォータの引き上げのリクエスト」を参照してください。

一部のお客様のアカウントのクォータは、これらの公開されたクォータ以下である可能性があります。リソース制限の超過エラーが発生した場合は、Service Quotas コンソールを使用してクォータの引き上げをリクエストします。

グローバルリゾルバーのソフトクォータ

[リソース]	デフォルトのクォータ	引き上げ可能
アカウントあたりのグローバルリゾルバー	2	はい
グローバルリゾルバーあたりの DNS ビュー	5	はい
アカウントあたりの DNS ビュー	50	はい
アカウントあたりのドメインリスト	1,000	はい
ドメインリストあたりのドメイン	100,000	はい
アカウントあたりのドメイン	100,000	はい
S3 からインポートされたファイルのドメイン	10,000	はい
すべてのファイアウォールルールで参照されるドメインの数	1,000,000	はい

[リソース]	デフォルトのクォータ	引き上げ可能
DNS ビューあたりのファイアウォールルール	100	はい
グローバルリゾルバーあたりのアクセストークン	5,000	はい
グローバルリゾルバーあたりのアクセスソース	1,000	はい
グローバルリゾルバーあたりのアクセスソース CIDR サイズ	65,000	いいえ
グローバルリゾルバーあたりの IPv6 アクセスソース/48 ブロック	1	はい
DNS ビューあたりのプライベートホストゾーン	1,000	はい

を使用した Amazon Route 53 および Route 53 VPC Resolver リソースの作成 AWS CloudFormation

Amazon Route 53 および Route 53 VPC Resolver は と統合されています。これは AWS CloudFormation、 AWS リソースとインフラストラクチャの作成と管理に費やす時間を短縮できるように、リソースのモデル化とセットアップに役立つサービスです。必要なすべての AWS リソースを記述するテンプレートを作成し、それらのリソースを CloudFormation プロビジョニングして設定します。

を使用すると CloudFormation、テンプレートを再利用して Route 53 および VPC Resolver リソースを一貫して繰り返しセットアップできます。リソースを一度記述し、複数の AWS アカウント およびリージョンで同じリソースを何度もプロビジョニングします。

Route 53、VPC Resolver、および CloudFormation テンプレート

Route 53、VPC Resolver、および関連サービスのリソースをプロビジョニングおよび設定するには、 CloudFormation テンプレートを理解する必要があります。テンプレートは、JSON や YAML でフォーマットされたテキストファイルです。これらのテンプレートは、 CloudFormation スタックにプロビジョニングするリソースを記述します。JSON または YAML に慣れていない場合は、CloudFormation デザイナー を使用して CloudFormation テンプレートの使用を開始できます。詳細については、CloudFormation 「デザイナーとは」を参照してください。 AWS CloudFormation 「 ユーザーガイド」の「」を参照してください。

Route 53 は、 で次のリソースタイプの作成をサポートしています CloudFormation。

- `AWS::Route53::DNSSEC`
- `AWS::Route53::HealthCheck`
- `AWS::Route53::HostedZone`
- `AWS::Route53::KeySigningKey`
- `AWS::Route53::RecordSet`
- `AWS::Route53::RecordSetGroup`

Route 53 リソースの JSON テンプレートと YAML テンプレートの例を含む詳細については、AWS CloudFormation ユーザーガイドの「Amazon Route 53 resource type reference」を参照してください。

VPC Resolver は、 で次のリソースタイプの作成をサポートしています CloudFormation。

- `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`

VPC Resolver リソースの JSON テンプレートと YAML テンプレートの例を含む詳細については、AWS CloudFormation ユーザーガイドの Route 53 VPC Resolver リソースタイプのリファレンスを参照してください。

Route 53 と のベストプラクティス CloudFormation

CloudFormation を使用して Route 53 リソースを管理する場合は、以下のベストプラクティスに従って一般的な問題を回避し、信頼性の高いデプロイを確保します。

結果整合性について理解する

Route 53 は、DNS の変更に結果整合性モデルを使用します。これは、特にロールバックや連続した急激な変更中に、 CloudFormation オペレーションに影響を与える可能性があります。

> **Important**
>
> が DNS レコードの変更をロールバック CloudFormation しようとすると、Route 53 の結果整合性モデルが原因でロールバックが失敗する可能性があります。最近削除されたが、結果整合性のためにまだ存在するように見えるレコードを再作成 CloudFormation しようとすると、DNS が壊れた状態のままになる`InvalidChangeBatch`エラーが発生する可能性があります。

結果整合性に関連する問題を最小限に抑えるには:

- 変更を慎重に計画する - 同じ DNS レコードに迅速で連続した変更を加えないようにします。
- 本番環境以外で最初にテストする - 本番環境に適用する前に、開発環境で必ず DNS の変更をテストします。
- デプロイのモニタリング - DNS 関連のデプロイ中に CloudFormation スタックイベントを注意深く監視します。モニタリングのガイダンスについては、「Amazon Route 53 のモニタリング」を参照してください。
- ロールバック手順の準備をする - 自動ロールバックが失敗した場合の手動復旧手順を準備します。

DNS レコードの順序付けと論理 ID

で複数の DNS レコードを作成するときは CloudFormation、レコードの順序付けと論理 ID の割り当てに注意してください。

> **Warning**
>
> CloudFormation テンプレート内の配列またはリストで DNS レコードを定義すると、リストの中央に新しいレコードを挿入すると、 が既存のレコード CloudFormation に論理 IDs を再割り当てする可能性があります。これにより、サービスの中断やロールバックの失敗につながる可能性のあるレコードの置き換えがトリガーされます。

DNS レコード管理のベストプラクティス:

- 明示的な論理 ID を使用する - 配列インデックスに依存するのではなく、常に明示的で意味のある論理 ID を DNS レコードに割り当てます。 CloudFormation 論理 IDs「リソース」セクション構造を参照してください。 AWS CloudFormation
- 新しいレコードを追加する - 既存のリストに新しい DNS レコードを追加するときは、中央に挿入するのではなく、末尾に追加します。
- 関連レコードをグループ化する - 関連レコードを一緒に管理するために `AWS::Route53::RecordSetGroup` を使用することを検討してください。詳細については、「AWS CloudFormation ユーザーガイド」の「AWS::Route53::RecordSetGroup」を参照してください。
- 変更セットを確認する - デプロイ前に必ず CloudFormation 変更セットを確認して、予期しないレコードの置き換えを特定します。詳細については、AWS CloudFormation ユーザーガイドの「変更セットを使用したスタックの更新」を参照してください。

ロールバック失敗の処理

DNS 関連の問題が原因で CloudFormation ロールバックが失敗した場合、手動復旧の実行が必要になる場合があります。

失敗した DNS ロールバックから手動復旧を実行するには

1. CloudFormation スタックイベントと Route 53 ホストゾーンレコードを確認して、失敗した DNS レコードを特定する
2. Route 53 コンソールまたは API を使用して、欠落している DNS レコードを手動で作成または更新します。レコード作成について詳しくは、「レコードを使用する」を参照してください。
3. DNS が復元されたら、現在の状態に合わせて CloudFormation テンプレートを更新します。
4. 修正されたテンプレートをデプロイして、実際のリソースと同期 CloudFormation させます。

ロールバックの失敗を防ぐには:

- トラフィックの多い時間帯に DNS レコードの置き換えをトリガーする可能性のある変更を行わないでください。
- ヘルスチェックとモニタリングを実装して、DNS の問題をすばやく検出します。ヘルスチェックの詳細については、「ヘルスチェックの作成と更新」を参照してください。
- 重要な DNS 変更には、ブルー/グリーンデプロイ戦略の使用を検討してください。デプロイのベストプラクティスの詳細については、「Amazon Route 53 のベストプラクティス」を参照してください。
- 手動 DNS 復旧の緊急手順を文書化する

の詳細 CloudFormation

詳細については CloudFormation、次のリソースを参照してください。

- AWS CloudFormation
- AWS CloudFormation ユーザーガイド
- CloudFormation API リファレンス
- AWS CloudFormation コマンドラインインターフェイスユーザーガイド

AWS SDK を使用した Route 53 のコード例

以下は、AWS Software Development Kit (SDK) で Route 53 を使用する方法を説明するコード例です。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「AWS SDK での Route 53 の使用」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

コードの例

- SDK を使用した Route 53 のコード例 AWS SDKs
  - SDK を使用した Route 53 の基本的な例 AWS SDKs
    - SDK を使用した Route 53 のアクション AWS SDKs
      - CLI で ChangeResourceRecordSets を使用する
      - CLI で CreateHostedZone を使用する
      - CLI で DeleteHostedZone を使用する
      - CLI で GetHostedZone を使用する
      - AWS SDK または CLI ListHostedZonesで を使用する
      - CLI で ListHostedZonesByName を使用する
      - CLI で ListQueryLoggingConfigs を使用する
- SDK を使用した Route 53 ドメイン登録のコード例 AWS SDKs
  - AWS SDKs を使用した Route 53 ドメイン登録の基本的な例
    - ハロー Route 53 ドメイン登録
    - AWS SDK での Route 53 ドメイン登録の基本について説明します。
    - AWS SDKs を使用した Route 53 ドメイン登録のアクション
      - AWS SDK または CLI CheckDomainAvailabilityで を使用する
      - AWS SDK または CLI CheckDomainTransferabilityで を使用する
      - AWS SDK または CLI GetDomainDetailで を使用する
      - AWS SDK または CLI GetDomainSuggestionsで を使用する
      - AWS SDK または CLI GetOperationDetailで を使用する
      - AWS SDK または CLI ListDomainsで を使用する
      - AWS SDK または CLI ListOperationsで を使用する

- AWS SDK ListPricesで を使用する
- AWS SDK または CLI RegisterDomainで を使用する
- AWS SDK または CLI ViewBillingで を使用する

SDK を使用した Route 53 のコード例 AWS SDKs

次のコード例は、 AWS Software Development Kit (SDK) で Route 53 を使用する方法を示しています。

アクションはより大きなプログラムからのコードの抜粋であり、コンテキスト内で実行する必要があります。アクションは個々のサービス機能を呼び出す方法を示していますが、コンテキスト内のアクションは、関連するシナリオで確認できます。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK での Route 53 の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

Route 53

- SDK を使用した Route 53 の基本的な例 AWS SDKs
  - SDK を使用した Route 53 のアクション AWS SDKs
    - CLI で ChangeResourceRecordSets を使用する
    - CLI で CreateHostedZone を使用する
    - CLI で DeleteHostedZone を使用する
    - CLI で GetHostedZone を使用する
    - AWS SDK または CLI ListHostedZonesで を使用する
    - CLI で ListHostedZonesByName を使用する
    - CLI で ListQueryLoggingConfigs を使用する

SDK を使用した Route 53 の基本的な例 AWS SDKs

次のコード例は、 AWS SDK を使用した Amazon Route 53 の基本的な使用方法を示しています。

例

- SDK を使用した Route 53 のアクション AWS SDKs
  - CLI で ChangeResourceRecordSets を使用する

- CLI で CreateHostedZone を使用する
- CLI で DeleteHostedZone を使用する
- CLI で GetHostedZone を使用する
- AWS SDK または CLI ListHostedZonesで を使用する
- CLI で ListHostedZonesByName を使用する
- CLI で ListQueryLoggingConfigs を使用する

SDK を使用した Route 53 のアクション AWS SDKs

次のコード例は、 AWS SDKs で個々の Route 53 アクションを実行する方法を示しています。それぞれの例には、GitHub へのリンクがあり、そこにはコードの設定と実行に関する説明が記載されています。

以下の例には、最も一般的に使用されるアクションのみ含まれています。詳細な一覧については、「Amazon Route 53 API リファレンス」を参照してください。

例

- CLI で ChangeResourceRecordSets を使用する
- CLI で CreateHostedZone を使用する
- CLI で DeleteHostedZone を使用する
- CLI で GetHostedZone を使用する
- AWS SDK または CLI ListHostedZonesで を使用する
- CLI で ListHostedZonesByName を使用する
- CLI で ListQueryLoggingConfigs を使用する

CLI で **ChangeResourceRecordSets** を使用する

次のサンプルコードは、ChangeResourceRecordSets を使用する方法を説明しています。

CLI

AWS CLI

リソースレコードセットを作成、更新、または削除するには

次の change-resource-record-sets コマンドは、ファイル C:\awscli\route53\change-resource-record-sets.json の hosted-zone-id Z1R8UBAEXAMPLE と JSON 形式の設定を使用してリソースレコードセットを作成します。

```
aws route53 change-resource-record-sets --hosted-zone-id Z1R8UBAEXAMPLE --change-batch file://C:\awscli\route53\change-resource-record-sets.json
```

詳細については、Amazon Route 53 API リファレンスの「POST ChangeResourceRecordSets」を参照してください。

JSON ファイルの設定は、作成するリソースレコードセットの種類によって異なります。

BasicWeightedAliasWeighted AliasLatencyLatency AliasFailoverFailover Alias

基本構文:

```
{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
        "TTL": time to live in seconds,
        "ResourceRecords": [
          {
            "Value": "applicable value for the record type"
          },
          {...}
        ]
      }
    },
    {...}
  ]
}
```

加重構文:

```
{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
```

```
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
        "SetIdentifier": "unique description for this resource record set",
        "Weight": value between 0 and 255,
        "TTL": time to live in seconds,
        "ResourceRecords": [
          {
            "Value": "applicable value for the record type"
          },
          {...}
        ],
        "HealthCheckId": "optional ID of an Amazon Route 53 health check"
      }
    },
    {...}
  ]
}
```

エイリアス構文:

```
{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
        "AliasTarget": {
          "HostedZoneId": "hosted zone ID for your CloudFront distribution,
 Amazon S3 bucket, Elastic Load Balancing load balancer, or Amazon Route 53
 hosted zone",
          "DNSName": "DNS domain name for your CloudFront distribution, Amazon S3
 bucket, Elastic Load Balancing load balancer, or another resource record set in
 this hosted zone",
          "EvaluateTargetHealth": true|false
        },
        "HealthCheckId": "optional ID of an Amazon Route 53 health check"
      }
    },
```

```
    {...}
  ]
}
```

加重エイリアス構文:

```
{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
        "SetIdentifier": "unique description for this resource record set",
        "Weight": value between 0 and 255,
        "AliasTarget": {
          "HostedZoneId": "hosted zone ID for your CloudFront distribution,
 Amazon S3 bucket, Elastic Load Balancing load balancer, or Amazon Route 53
 hosted zone",
          "DNSName": "DNS domain name for your CloudFront distribution, Amazon S3
 bucket, Elastic Load Balancing load balancer, or another resource record set in
 this hosted zone",
          "EvaluateTargetHealth": true|false
        },
        "HealthCheckId": "optional ID of an Amazon Route 53 health check"
      }
    },
    {...}
  ]
}
```

レイテンシー構文:

```
{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
        "SetIdentifier": "unique description for this resource record set",
```

```
        "Region": "Amazon EC2 region name",
        "TTL": time to live in seconds,
        "ResourceRecords": [
          {
            "Value": "applicable value for the record type"
          },
          {...}
        ],
        "HealthCheckId": "optional ID of an Amazon Route 53 health check"
      }
    },
    {...}
  ]
}
```

レイテンシーエイリアス構文:

```
{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
        "SetIdentifier": "unique description for this resource record set",
        "Region": "Amazon EC2 region name",
        "AliasTarget": {
          "HostedZoneId": "hosted zone ID for your CloudFront distribution,
 Amazon S3 bucket, Elastic Load Balancing load balancer, or Amazon Route 53
 hosted zone",
          "DNSName": "DNS domain name for your CloudFront distribution, Amazon S3
 bucket, Elastic Load Balancing load balancer, or another resource record set in
 this hosted zone",
          "EvaluateTargetHealth": true|false
        },
        "HealthCheckId": "optional ID of an Amazon Route 53 health check"
      }
    },
    {...}
  ]
}
```

フェイルオーバー構文:

```
{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
        "SetIdentifier": "unique description for this resource record set",
        "Failover": "PRIMARY" | "SECONDARY",
        "TTL": time to live in seconds,
        "ResourceRecords": [
          {
            "Value": "applicable value for the record type"
          },
          {...}
        ],
        "HealthCheckId": "ID of an Amazon Route 53 health check"
      }
    },
    {...}
  ]
}
```

フェイルオーバーエイリアス構文:

```
{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
        "SetIdentifier": "unique description for this resource record set",
        "Failover": "PRIMARY" | "SECONDARY",
        "AliasTarget": {
          "HostedZoneId": "hosted zone ID for your CloudFront distribution,
 Amazon S3 bucket, Elastic Load Balancing load balancer, or Amazon Route 53
 hosted zone",
```

```
          "DNSName": "DNS domain name for your CloudFront distribution, Amazon S3
 bucket, Elastic Load Balancing load balancer, or another resource record set in
 this hosted zone",
          "EvaluateTargetHealth": true|false
        },
        "HealthCheckId": "optional ID of an Amazon Route 53 health check"
      }
    },
    {...}
  ]
}
```

- API の詳細については、「AWS CLI コマンドリファレンス」の「ChangeResourceRecordSets」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、www.example.com の A レコードを作成し、test.example.com の A レコードを 192.0.2.3 から 192.0.2.1 に変更します。変更 TXT タイプのレコードの値は二重引用符で囲む必要があることに注意してください。詳細については、Amazon Route 53 のドキュメントを参照してください。Get-R53Change コマンドレットを使用してポーリングし、変更が完了したタイミングを確認できます。

```
$change1 = New-Object Amazon.Route53.Model.Change
$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "www.example.com"
$change1.ResourceRecordSet.Type = "TXT"
$change1.ResourceRecordSet.TTL = 600
$change1.ResourceRecordSet.ResourceRecords.Add(@{Value="item 1 item 2 item 3"})

$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "DELETE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change2.ResourceRecordSet.Name = "test.example.com"
$change2.ResourceRecordSet.Type = "A"
$change2.ResourceRecordSet.TTL = 600
$change2.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.3"})

$change3 = New-Object Amazon.Route53.Model.Change
```

```
$change3.Action = "CREATE"
$change3.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change3.ResourceRecordSet.Name = "test.example.com"
$change3.ResourceRecordSet.Type = "A"
$change3.ResourceRecordSet.TTL = 600
$change3.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.1"})

$params = @{
    HostedZoneId="Z1PA6795UKMFR9"
 ChangeBatch_Comment="This change batch creates a TXT record for www.example.com.
 and changes the A record for test.example.com. from 192.0.2.3 to 192.0.2.1."
 ChangeBatch_Change=$change1,$change2,$change3
}

Edit-R53ResourceRecordSet @params
```

例 2: この例は、エイリアスリソースレコードセットの作成方法を示します。「Z222222222」は、エイリアスリソースレコードセットを作成する Amazon Route 53 ホストゾーンの ID です。「example.com」は、エイリアスを作成するゾーン頂点 Zone Apex で、「www.example.com」は、エイリアスを作成するサブドメインです。「Z1111111111111」はロードバランサーのホストゾーン ID の例で、「example-load-balancer-1111111111.us-east-1.elb.amazonaws.com」は Amazon Route 53 が example.com および www.example.com のクエリに応答するロードバランサードメイン名の例です。詳細については、Amazon Route 53 のドキュメントを参照してください。Get-R53Change コマンドレットを使用してポーリングし、変更が完了したタイミングを確認できます。

```
$change1 = New-Object Amazon.Route53.Model.Change
$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "example.com"
$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.AliasTarget = New-Object
 Amazon.Route53.Model.AliasTarget
$change1.ResourceRecordSet.AliasTarget.HostedZoneId = "Z1111111111111"
$change1.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-1111111111.us-east-1.elb.amazonaws.com."
$change1.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $true

$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "CREATE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "www.example.com"
```

```
$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.AliasTarget = New-Object
 Amazon.Route53.Model.AliasTarget
$change1.ResourceRecordSet.AliasTarget.HostedZoneId = "Z1111111111111"
$change1.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-1111111111.us-east-1.elb.amazonaws.com."
$change1.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $false

$params = @{
    HostedZoneId="Z222222222"
 ChangeBatch_Comment="This change batch creates two alias resource record sets,
 one for the zone apex, example.com, and one for www.example.com, that both point
 to example-load-balancer-1111111111.us-east-1.elb.amazonaws.com."
 ChangeBatch_Change=$change1,$change2
}

Edit-R53ResourceRecordSet @params
```

例 3: この例では、www.example.com の A レコードを 2 つ作成します。割合が 4 分の 1 (1/(1+3)) の Amazon Route 53 は、最初のリソースレコードセット (192.0.2.9 と 192.0.2.10) の 2 つの値を使用して www.example.com のクエリに応答します。割合が 4 分の 3 (3/(1+3)) の Amazon Route 53 は、2 番目のリソースレコードセット (192.0.2.11 と 192.0.2.12) の 2 つの値を使用して www.example.com のクエリに応答します。詳細については、Amazon Route 53 のドキュメントを参照してください。Get-R53Change コマンドレットを使用してポーリングし、変更が完了したタイミングを確認できます。

```
$change1 = New-Object Amazon.Route53.Model.Change
$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "www.example.com"
$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.SetIdentifier = "Rack 2, Positions 4 and 5"
$change1.ResourceRecordSet.Weight = 1
$change1.ResourceRecordSet.TTL = 600
$change1.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.9"})
$change1.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.10"})

$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "CREATE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change2.ResourceRecordSet.Name = "www.example.com"
$change2.ResourceRecordSet.Type = "A"
```

```
$change2.ResourceRecordSet.SetIdentifier = "Rack 5, Positions 1 and 2"
$change2.ResourceRecordSet.Weight = 3
$change2.ResourceRecordSet.TTL = 600
$change2.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.11"})
$change2.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.12"})

$params = @{
    HostedZoneId="Z1PA6795UKMFR9"
    ChangeBatch_Comment="This change creates two weighted resource record sets,
 each of which has two values."
    ChangeBatch_Change=$change1,$change2
}

Edit-R53ResourceRecordSet @params
```

例 4: この例は、example.com が加重エイリアスリソースレコードセットを作成するドメインであると仮定した、加重エイリアスリソースレコードセットの作成方法を示します。SetIdentifier は、2 つの加重エイリアスリソースレコードセットを相互に区別します。Name 要素と Type 要素が両方のリソースレコードセットに同じ値を持つため、この要素は必要です。Z1111111111111 および Z3333333333333 は、DNSName の値で指定された ELB ロードバランサーのホストゾーン ID の例です。example-load-balancer-2222222222.us-east-1.elb.amazonaws.com および example-load-balancer-4444444444.us-east-1.elb.amazonaws.com は Amazon Route 53 が example.com のクエリに応答する Elastic Load Balancing ドメインの例です。詳細については、Amazon Route 53 のドキュメントを参照してください。Get-R53Change コマンドレットを使用してポーリングし、変更が完了したタイミングを確認できます。

```
$change1 = New-Object Amazon.Route53.Model.Change
$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "example.com"
$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.SetIdentifier = "1"
$change1.ResourceRecordSet.Weight = 3
$change1.ResourceRecordSet.AliasTarget = New-Object
 Amazon.Route53.Model.AliasTarget
$change1.ResourceRecordSet.AliasTarget.HostedZoneId = "Z1111111111111"
$change1.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-2222222222.us-east-1.elb.amazonaws.com."
$change1.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $true
```

```
$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "CREATE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change2.ResourceRecordSet.Name = "example.com"
$change2.ResourceRecordSet.Type = "A"
$change2.ResourceRecordSet.SetIdentifier = "2"
$change2.ResourceRecordSet.Weight = 1
$change2.ResourceRecordSet.AliasTarget = New-Object
 Amazon.Route53.Model.AliasTarget
$change2.ResourceRecordSet.AliasTarget.HostedZoneId = "Z3333333333333"
$change2.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-4444444444.us-east-1.elb.amazonaws.com."
$change2.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $false

$params = @{
    HostedZoneId="Z5555555555"
    ChangeBatch_Comment="This change batch creates two weighted alias resource
 record sets. Amazon Route 53 responds to queries for example.com with the first
 ELB domain 3/4ths of the times and the second one 1/4th of the time."
    ChangeBatch_Change=$change1,$change2
}

Edit-R53ResourceRecordSet @params
```

例 5: この例では、レイテンシーエイリアスリソースレコードセットを 2 つ作成します。1 つは米国西部 (オレゴン) リージョン (us-west-2) の ELB ロードバランサー用で、もう 1 つはアジアパシフィック (シンガポール) リージョン (ap-southeast-1) のロードバランサー用です。詳細については、Amazon Route 53 のドキュメントを参照してください。Get-R53Change コマンドレットを使用してポーリングし、変更が完了したタイミングを確認できます。

```
$change1 = New-Object Amazon.Route53.Model.Change
$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "example.com"
$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.SetIdentifier = "Oregon load balancer 1"
$change1.ResourceRecordSet.Region = us-west-2
$change1.ResourceRecordSet.AliasTarget = New-Object
 Amazon.Route53.Model.AliasTarget
$change1.ResourceRecordSet.AliasTarget.HostedZoneId = "Z1111111111111"
$change1.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-2222222222.us-west-2.elb.amazonaws.com"
$change1.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $true
```

```
$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "CREATE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change2.ResourceRecordSet.Name = "example.com"
$change2.ResourceRecordSet.Type = "A"
$change2.ResourceRecordSet.SetIdentifier = "Singapore load balancer 1"
$change2.ResourceRecordSet.Region = ap-southeast-1
$change2.ResourceRecordSet.AliasTarget = New-Object
 Amazon.Route53.Model.AliasTarget
$change2.ResourceRecordSet.AliasTarget.HostedZoneId = "Z2222222222222"
$change2.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-1111111111.ap-southeast-1.elb.amazonaws.com"
$change2.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $true

$params = @{
    HostedZoneId="Z5555555555"
    ChangeBatch_Comment="This change batch creates two latency resource
 record sets, one for the US West (Oregon) region and one for the Asia Pacific
 (Singapore) region."
    ChangeBatch_Change=$change1,$change2
}

Edit-R53ResourceRecordSet @params
```

- API の詳細については、「AWS Tools for PowerShell コマンドレットリファレンス (V4)」の「ChangeResourceRecordSets」を参照してください。

Tools for PowerShell V5

例 1: この例では、www.example.com の A レコードを作成し、test.example.com の A レコードを 192.0.2.3 から 192.0.2.1 に変更します。変更 TXT タイプのレコードの値は二重引用符で囲む必要があることに注意してください。詳細については、Amazon Route 53 のドキュメントを参照してください。Get-R53Change コマンドレットを使用してポーリングし、変更が完了したタイミングを確認できます。

```
$change1 = New-Object Amazon.Route53.Model.Change
$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "www.example.com"
$change1.ResourceRecordSet.Type = "TXT"
$change1.ResourceRecordSet.TTL = 600
$change1.ResourceRecordSet.ResourceRecords = @()
```

```
$change1.ResourceRecordSet.ResourceRecords.Add(@{Value="item 1 item 2 item 3"})

$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "DELETE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change2.ResourceRecordSet.Name = "test.example.com"
$change2.ResourceRecordSet.Type = "A"
$change2.ResourceRecordSet.TTL = 600
$change2.ResourceRecordSet.ResourceRecords = @()
$change2.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.3"})

$change3 = New-Object Amazon.Route53.Model.Change
$change3.Action = "CREATE"
$change3.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change3.ResourceRecordSet.Name = "test.example.com"
$change3.ResourceRecordSet.Type = "A"
$change3.ResourceRecordSet.TTL = 600
$change3.ResourceRecordSet.ResourceRecords = @()
$change3.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.1"})

$params = @{
    HostedZoneId="Z1PA6795UKMFR9"
 ChangeBatch_Comment="This change batch creates a TXT record for www.example.com.
 and changes the A record for test.example.com. from 192.0.2.3 to 192.0.2.1."
 ChangeBatch_Change=$change1,$change2,$change3
}

Edit-R53ResourceRecordSet @params
```

例 2: この例は、エイリアスリソースレコードセットの作成方法を示します。「Z222222222」は、エイリアスリソースレコードセットを作成する Amazon Route 53 ホストゾーンの ID です。「example.com」は、エイリアスを作成するゾーン頂点 Zone Apex で、「www.example.com」は、エイリアスを作成するサブドメインです。「Z1111111111111」はロードバランサーのホストゾーン ID の例で、「example-load-balancer-1111111111.us-east-1.elb.amazonaws.com」は Amazon Route 53 が example.com および www.example.com のクエリに応答するロードバランサードメイン名の例です。詳細については、Amazon Route 53 のドキュメントを参照してください。Get-R53Change コマンドレットを使用してポーリングし、変更が完了したタイミングを確認できます。

```
$change1 = New-Object Amazon.Route53.Model.Change
$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
```

```
$change1.ResourceRecordSet.Name = "example.com"
$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.AliasTarget = New-Object
 Amazon.Route53.Model.AliasTarget
$change1.ResourceRecordSet.AliasTarget.HostedZoneId = "Z1111111111111"
$change1.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-1111111111.us-east-1.elb.amazonaws.com."
$change1.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $true

$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "CREATE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "www.example.com"
$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.AliasTarget = New-Object
 Amazon.Route53.Model.AliasTarget
$change1.ResourceRecordSet.AliasTarget.HostedZoneId = "Z1111111111111"
$change1.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-1111111111.us-east-1.elb.amazonaws.com."
$change1.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $false

$params = @{
    HostedZoneId="Z222222222"
 ChangeBatch_Comment="This change batch creates two alias resource record sets,
 one for the zone apex, example.com, and one for www.example.com, that both point
 to example-load-balancer-1111111111.us-east-1.elb.amazonaws.com."
 ChangeBatch_Change=$change1,$change2
}

Edit-R53ResourceRecordSet @params
```

例 3: この例では、www.example.com の A レコードを 2 つ作成します。割合が 4 分の 1 (1/(1+3)) の Amazon Route 53 は、最初のリソースレコードセット (192.0.2.9 と 192.0.2.10) の 2 つの値を使用して www.example.com のクエリに応答します。割合が 4 分の 3 (3/(1+3)) の Amazon Route 53 は、2 番目のリソースレコードセット (192.0.2.11 と 192.0.2.12) の 2 つの値を使用して www.example.com のクエリに応答します。詳細については、Amazon Route 53 のドキュメントを参照してください。Get-R53Change コマンドレットを使用してポーリングし、変更が完了したタイミングを確認できます。

```
$change1 = New-Object Amazon.Route53.Model.Change
$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
```

```
$change1.ResourceRecordSet.Name = "www.example.com"
$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.SetIdentifier = "Rack 2, Positions 4 and 5"
$change1.ResourceRecordSet.Weight = 1
$change1.ResourceRecordSet.TTL = 600
$change1.ResourceRecordSet.ResourceRecords = @()
$change1.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.9"})
$change1.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.10"})

$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "CREATE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change2.ResourceRecordSet.Name = "www.example.com"
$change2.ResourceRecordSet.Type = "A"
$change2.ResourceRecordSet.SetIdentifier = "Rack 5, Positions 1 and 2"
$change2.ResourceRecordSet.Weight = 3
$change2.ResourceRecordSet.TTL = 600
$change2.ResourceRecordSet.ResourceRecords = @()
$change2.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.11"})
$change2.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.12"})

$params = @{
    HostedZoneId="Z1PA6795UKMFR9"
    ChangeBatch_Comment="This change creates two weighted resource record sets,
 each of which has two values."
    ChangeBatch_Change=$change1,$change2
}

Edit-R53ResourceRecordSet @params
```

例 4: この例は、example.com が加重エイリアスリソースレコードセットを作成するドメインであると仮定した、加重エイリアスリソースレコードセットの作成方法を示します。SetIdentifier は、2 つの加重エイリアスリソースレコードセットを相互に区別します。Name 要素と Type 要素が両方のリソースレコードセットに同じ値を持つため、この要素は必要です。Z1111111111111 および Z3333333333333 は、DNSName の値で指定された ELB ロードバランサーのホストゾーン ID の例です。example-load-balancer-2222222222.us-east-1.elb.amazonaws.com および example-load-balancer-4444444444.us-east-1.elb.amazonaws.com は Amazon Route 53 が example.com のクエリに応答する Elastic Load Balancing ドメインの例です。詳細については、Amazon Route 53 のドキュメントを参照してください。Get-R53Change コマンドレットを使用してポーリングし、変更が完了したタイミングを確認できます。

```
$change1 = New-Object Amazon.Route53.Model.Change
$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "example.com"
$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.SetIdentifier = "1"
$change1.ResourceRecordSet.Weight = 3
$change1.ResourceRecordSet.AliasTarget = New-Object
 Amazon.Route53.Model.AliasTarget
$change1.ResourceRecordSet.AliasTarget.HostedZoneId = "Z1111111111111"
$change1.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-2222222222.us-east-1.elb.amazonaws.com."
$change1.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $true

$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "CREATE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change2.ResourceRecordSet.Name = "example.com"
$change2.ResourceRecordSet.Type = "A"
$change2.ResourceRecordSet.SetIdentifier = "2"
$change2.ResourceRecordSet.Weight = 1
$change2.ResourceRecordSet.AliasTarget = New-Object
 Amazon.Route53.Model.AliasTarget
$change2.ResourceRecordSet.AliasTarget.HostedZoneId = "Z3333333333333"
$change2.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-4444444444.us-east-1.elb.amazonaws.com."
$change2.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $false

$params = @{
    HostedZoneId="Z5555555555"
    ChangeBatch_Comment="This change batch creates two weighted alias resource
 record sets. Amazon Route 53 responds to queries for example.com with the first
 ELB domain 3/4ths of the times and the second one 1/4th of the time."
    ChangeBatch_Change=$change1,$change2
}

Edit-R53ResourceRecordSet @params
```

例 5: この例では、レイテンシーエイリアスリソースレコードセットを 2 つ作成します。1 つは米国西部 (オレゴン) リージョン (us-west-2) の ELB ロードバランサー用で、もう 1 つはアジアパシフィック (シンガポール) リージョン (ap-southeast-1) のロードバランサー用です。

詳細については、Amazon Route 53 のドキュメントを参照してください。Get-R53Change コマンドレットを使用してポーリングし、変更が完了したタイミングを確認できます。

```
$change1 = New-Object Amazon.Route53.Model.Change
$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "example.com"
$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.SetIdentifier = "Oregon load balancer 1"
$change1.ResourceRecordSet.Region = us-west-2
$change1.ResourceRecordSet.AliasTarget = New-Object
 Amazon.Route53.Model.AliasTarget
$change1.ResourceRecordSet.AliasTarget.HostedZoneId = "Z1111111111111"
$change1.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-2222222222.us-west-2.elb.amazonaws.com"
$change1.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $true

$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "CREATE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change2.ResourceRecordSet.Name = "example.com"
$change2.ResourceRecordSet.Type = "A"
$change2.ResourceRecordSet.SetIdentifier = "Singapore load balancer 1"
$change2.ResourceRecordSet.Region = ap-southeast-1
$change2.ResourceRecordSet.AliasTarget = New-Object
 Amazon.Route53.Model.AliasTarget
$change2.ResourceRecordSet.AliasTarget.HostedZoneId = "Z2222222222222"
$change2.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-1111111111.ap-southeast-1.elb.amazonaws.com"
$change2.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $true

$params = @{
    HostedZoneId="Z5555555555"
    ChangeBatch_Comment="This change batch creates two latency resource
 record sets, one for the US West (Oregon) region and one for the Asia Pacific
 (Singapore) region."
    ChangeBatch_Change=$change1,$change2
}

Edit-R53ResourceRecordSet @params
```

- API の詳細については、AWS Tools for PowerShell コマンドレットリファレンス (V5) の「ChangeResourceRecordSets」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK での Route 53 の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **CreateHostedZone** を使用する

次のサンプルコードは、CreateHostedZone を使用する方法を説明しています。

CLI

AWS CLI

ホストゾーンを作成するには

次の create-hosted-zone コマンドは、発信者リファレンス 2014-04-01-18:47 を使用して example.com という名前のホストゾーンを追加します。オプションのコメントは、スペースを含むため、引用符で囲む必要があります。

```
aws route53 create-hosted-zone --name example.com --caller-
reference 2014-04-01-18:47 --hosted-zone-config Comment="command-line version"
```

詳細については、「Amazon Route 53 デベロッパーガイド」の「ホストゾーンの使用」を参照してください。

- API の詳細については、「AWS CLI コマンドレットリファレンス」の「CreateHostedZone」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: 再利用可能な委託セットに関連付けられた「example.com」という名前の新しいホストゾーンを作成します。CallerReference パラメータの値を指定する必要があります。それによって、必要に応じて再試行が必要なリクエストのオペレーションを 2 回実行するリスクがなくなります。ホストゾーンは VPC で作成され、自動的にプライベートになるため、-HostedZoneConfig_PrivateZone パラメータは設定しないでください。

```
$params = @{
    Name="example.com"
    CallerReference="myUniqueIdentifier"
```

```
    HostedZoneConfig_Comment="This is my first hosted zone"
    DelegationSetId="NZ8X2CISAMPLE"
    VPC_VPCId="vpc-1a2b3c4d"
    VPC_VPCRegion="us-east-1"
}

New-R53HostedZone @params
```

- API の詳細については、「AWS Tools for PowerShell コマンドレットリファレンス (V4)」の「CreateHostedZone」を参照してください。

Tools for PowerShell V5

例 1: 再利用可能な委託セットに関連付けられた「example.com」という名前の新しいホストゾーンを作成します。CallerReference パラメータの値を指定する必要があります。それによって、必要に応じて再試行が必要なリクエストのオペレーションを 2 回実行するリスクがなくなります。ホストゾーンは VPC で作成され、自動的にプライベートになるため、-HostedZoneConfig_PrivateZone パラメータは設定しないでください。

```
$params = @{
    Name="example.com"
    CallerReference="myUniqueIdentifier"
    HostedZoneConfig_Comment="This is my first hosted zone"
    DelegationSetId="NZ8X2CISAMPLE"
    VPC_VPCId="vpc-1a2b3c4d"
    VPC_VPCRegion="us-east-1"
}

New-R53HostedZone @params
```

- API の詳細については、AWS Tools for PowerShell コマンドレットリファレンス (V5) の「CreateHostedZone」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK での Route 53 の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **DeleteHostedZone** を使用する

次のサンプルコードは、DeleteHostedZone を使用する方法を説明しています。

CLI

AWS CLI

ホストゾーンを削除するには

次の delete-hosted-zone コマンドは、Z36KTIQEXAMPLE の id を使用してホストゾーンを削除します。

```
aws route53 delete-hosted-zone --id Z36KTIQEXAMPLE
```

- API の詳細については、「AWS CLI コマンドリファレンス」の「DeleteHostedZone」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: 指定された ID を持つホストゾーンを削除します。-Force スイッチパラメータを追加しない限り、コマンドを進める前に確認を求められます。

```
Remove-R53HostedZone -Id Z1PA6795UKMFR9
```

- API の詳細については、「AWS Tools for PowerShell コマンドレットリファレンス (V4)」の「DeleteHostedZone」を参照してください。

Tools for PowerShell V5

例 1: 指定された ID を持つホストゾーンを削除します。-Force スイッチパラメータを追加しない限り、コマンドを進める前に確認を求められます。

```
Remove-R53HostedZone -Id Z1PA6795UKMFR9
```

- API の詳細については、AWS Tools for PowerShell コマンドレットリファレンス (V5) の「DeleteHostedZone」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK での Route 53 の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **GetHostedZone** を使用する

次のサンプルコードは、GetHostedZone を使用する方法を説明しています。

CLI

AWS CLI

ホストゾーンに関する情報を取得するには

次の get-hosted-zone コマンドは、Z1R8UBAEXAMPLE の id を使用してホストゾーンに関する情報を取得します。

```
aws route53 get-hosted-zone --id Z1R8UBAEXAMPLE
```

- API の詳細については、「AWS CLI コマンドリファレンス」の「GetHostedZone」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: ID Z1D633PJN98FT9 を持つホストゾーンの詳細を返します。

```
Get-R53HostedZone -Id Z1D633PJN98FT9
```

- API の詳細については、「AWS Tools for PowerShell コマンドレットリファレンス (V4)」の「GetHostedZone」を参照してください。

Tools for PowerShell V5

例 1: ID Z1D633PJN98FT9 を持つホストゾーンの詳細を返します。

```
Get-R53HostedZone -Id Z1D633PJN98FT9
```

- API の詳細については、AWS Tools for PowerShell コマンドレットリファレンス (V5) の「GetHostedZone」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK での Route 53 の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

AWS SDK または CLI **ListHostedZones**で を使用する

次のサンプルコードは、ListHostedZones を使用する方法を説明しています。

CLI

AWS CLI

現在の AWS アカウントに関連付けられているホストゾーンを一覧表示するには

次のlist-hosted-zonesコマンドは、現在の AWS アカウントに関連付けられている最初の 100 個のホストゾーンに関する概要情報を一覧表示します。

```
aws route53 list-hosted-zones
```

ホストゾーンが 100 個を超える場合や、100 個未満のグループにホストゾーンを一覧表示する場合は、--max-items パラメータを含めてください。例えば、ホストゾーンを一度に一覧表示するには、次のコマンドを使用します。

```
aws route53 list-hosted-zones --max-items 1
```

次のホストゾーンに関する情報を表示するには、前のコマンドに対する応答から NextToken の値を取得し、その値を --starting-token パラメーターに含めます。次に例を示します。

```
aws route53 list-hosted-zones --max-items 1 --starting-token Z3M3LMPEXAMPLE
```

- API の詳細については、「AWS CLI コマンドリファレンス」の「ListHostedZones」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: すべてのパブリックホストゾーンとプライベートホストゾーンを出力します。

```
Get-R53HostedZoneList
```

例 2: ID NZ8X2CISAMPLE を持つ再利用可能な委託セットに関連付けられているすべてのホストゾーンを出力します

```
Get-R53HostedZoneList -DelegationSetId NZ8X2CISAMPLE
```

- API の詳細については、「AWS Tools for PowerShell コマンドレットリファレンス (V4)」の「ListHostedZones」を参照してください。

Tools for PowerShell V5

例 1: すべてのパブリックホストゾーンとプライベートホストゾーンを出力します。

```
Get-R53HostedZoneList
```

例 2: ID NZ8X2CISAMPLE を持つ再利用可能な委託セットに関連付けられているすべてのホストゾーンを出力します

```
Get-R53HostedZoneList -DelegationSetId NZ8X2CISAMPLE
```

- API の詳細については、「AWS Tools for PowerShell コマンドレットリファレンス (V5)」の「ListHostedZones」を参照してください。

Rust

SDK for Rust

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
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(())
}
```

- API の詳細については、AWS SDK for Rust API リファレンスの「ListHostedZones」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK での Route 53 の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **ListHostedZonesByName** を使用する

次のサンプルコードは、ListHostedZonesByName を使用する方法を説明しています。

CLI

AWS CLI

次のコマンドは、最大 100 個のホストゾーンをドメイン名順に一覧表示します。

```
aws route53 list-hosted-zones-by-name
```

出力:

```
{
  "HostedZones": [
      {
          "ResourceRecordSetCount": 2,
```

```
            "CallerReference": "test20150527-2",
            "Config": {
                "Comment": "test2",
                "PrivateZone": false
            },
            "Id": "/hostedzone/Z119WBBTVP5WFX",
            "Name": "2.example.com."
        },
        {
            "ResourceRecordSetCount": 2,
            "CallerReference": "test20150527-1",
            "Config": {
                "Comment": "test",
                "PrivateZone": false
            },
            "Id": "/hostedzone/Z3P5QSUBK4POTI",
            "Name": "www.example.com."
        }
    ],
    "IsTruncated": false,
    "MaxItems": "100"
}
```

次のコマンドは、www.example.com で始まる名前順にホストゾーンを一覧表示します。

```
aws route53 list-hosted-zones-by-name --dns-name www.example.com
```

出力:

```
{
    "HostedZones": [
        {
            "ResourceRecordSetCount": 2,
            "CallerReference": "mwunderl20150527-1",
            "Config": {
                "Comment": "test",
                "PrivateZone": false
            },
            "Id": "/hostedzone/Z3P5QSUBK4POTI",
            "Name": "www.example.com."
        }
    ],
    "DNSName": "www.example.com",
```

```
  "IsTruncated": false,
  "MaxItems": "100"
}
```

- API の詳細については、「AWS CLI コマンドリファレンス」の「ListHostedZonesByName」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: すべてのパブリックホストゾーンとプライベートホストゾーンを、ドメイン名で ASCII 順に返します。

```
Get-R53HostedZonesByName
```

例 2: パブリックホストゾーンとプライベートホストゾーンを、ドメイン名で ASCII 順に指定した DNS 名から返します。

```
Get-R53HostedZonesByName -DnsName example2.com
```

- API の詳細については、「AWS Tools for PowerShell コマンドレットリファレンス (V4)」の「ListHostedZonesByName」を参照してください。

Tools for PowerShell V5

例 1: すべてのパブリックホストゾーンとプライベートホストゾーンを、ドメイン名で ASCII 順に返します。

```
Get-R53HostedZonesByName
```

例 2: パブリックホストゾーンとプライベートホストゾーンを、ドメイン名で ASCII 順に指定した DNS 名から返します。

```
Get-R53HostedZonesByName -DnsName example2.com
```

- API の詳細については、AWS Tools for PowerShell コマンドレットリファレンス (V5) の「ListHostedZonesByName」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK での Route 53 の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **ListQueryLoggingConfigs** を使用する

次のサンプルコードは、ListQueryLoggingConfigs を使用する方法を説明しています。

CLI

AWS CLI

クエリログ記録の設定を一覧表示するには

次の のlist-query-logging-configs例では AWS 、ホストゾーン の最初の 100 件のクエリログ記録設定に関する情報を一覧表示しますZ1OX3WQEXAMPLE。

```
aws route53 list-query-logging-configs \
    --hosted-zone-id Z1OX3WQEXAMPLE
```

出力:

```
{
    "QueryLoggingConfigs": [
        {
            "Id": "964ff34e-ae03-4f06-80a2-9683cexample",
            "HostedZoneId": "Z1OX3WQEXAMPLE",
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-
east-1:111122223333:log-group:/aws/route53/example.com:*"
        }
    ]
}
```

詳細については、「Amazon Route 53 デベロッパーガイド」の「DNS クエリのログ」を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス」の「ListQueryLoggingConfigs」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、現在の AWS アカウントに関連付けられている DNS クエリのログ記録のすべての設定を返します。

```
Get-R53QueryLoggingConfigList
```

出力:

```
Id                                   HostedZoneId   CloudWatchLogsLogGroupArn
--                                   ------------   -------------------------
59b0fa33-4fea-4471-a88c-926476aaa40d Z385PDS6EAAAZR arn:aws:logs:us-
east-1:111111111112:log-group:/aws/route53/example1.com:*
ee528e95-4e03-4fdc-9d28-9e24ddaaa063 Z94SJHBV1AAAAZ arn:aws:logs:us-
east-1:111111111112:log-group:/aws/route53/example2.com:*
e38dddda-ceb6-45c1-8cb7-f0ae56aaaa2b Z3MEQ8T7AAA1BF arn:aws:logs:us-
east-1:111111111112:log-group:/aws/route53/example3.com:*
```

- API の詳細については、「AWS Tools for PowerShell コマンドレットリファレンス (V4)」の「ListQueryLoggingConfigs」を参照してください。

Tools for PowerShell V5

例 1: この例では、現在の AWS アカウントに関連付けられている DNS クエリのログ記録のすべての設定を返します。

```
Get-R53QueryLoggingConfigList
```

出力:

```
Id                                   HostedZoneId   CloudWatchLogsLogGroupArn
--                                   ------------   -------------------------
59b0fa33-4fea-4471-a88c-926476aaa40d Z385PDS6EAAAZR arn:aws:logs:us-
east-1:111111111112:log-group:/aws/route53/example1.com:*
ee528e95-4e03-4fdc-9d28-9e24ddaaa063 Z94SJHBV1AAAAZ arn:aws:logs:us-
east-1:111111111112:log-group:/aws/route53/example2.com:*
e38dddda-ceb6-45c1-8cb7-f0ae56aaaa2b Z3MEQ8T7AAA1BF arn:aws:logs:us-
east-1:111111111112:log-group:/aws/route53/example3.com:*
```

- API の詳細については、AWS Tools for PowerShell コマンドレットリファレンス (V5) の「ListQueryLoggingConfigs」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK での Route 53 の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

SDK を使用した Route 53 ドメイン登録のコード例 AWS SDKs

次のコード例は、 AWS Software Development Kit (SDK) で Route 53 ドメイン登録を使用する方法を示しています。

基本 は、重要なオペレーションをサービス内で実行する方法を示すコード例です。

アクションはより大きなプログラムからのコードの抜粋であり、コンテキスト内で実行する必要があります。アクションは個々のサービス機能を呼び出す方法を示していますが、コンテキスト内のアクションは、関連するシナリオで確認できます。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK での Route 53 の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

Route 53 ドメイン登録

- AWS SDKs を使用した Route 53 ドメイン登録の基本的な例
  - ハロー Route 53 ドメイン登録
  - AWS SDK での Route 53 ドメイン登録の基本について説明します。
  - AWS SDKs を使用した Route 53 ドメイン登録のアクション
    - AWS SDK または CLI CheckDomainAvailabilityで を使用する
    - AWS SDK または CLI CheckDomainTransferabilityで を使用する
    - AWS SDK または CLI GetDomainDetailで を使用する
    - AWS SDK または CLI GetDomainSuggestionsで を使用する
    - AWS SDK または CLI GetOperationDetailで を使用する
    - AWS SDK または CLI ListDomainsで を使用する
    - AWS SDK または CLI ListOperationsで を使用する
    - AWS SDK ListPricesで を使用する

- AWS SDK または CLI RegisterDomainで を使用する
- AWS SDK または CLI ViewBillingで を使用する

AWS SDKs を使用した Route 53 ドメイン登録の基本的な例

次のコード例は、 SDKs Amazon Route 53 domain registration で AWS の基本を使用する方法を示しています。

例

- ハロー Route 53 ドメイン登録
- AWS SDK での Route 53 ドメイン登録の基本について説明します。
- AWS SDKs を使用した Route 53 ドメイン登録のアクション
  - AWS SDK または CLI CheckDomainAvailabilityで を使用する
  - AWS SDK または CLI CheckDomainTransferabilityで を使用する
  - AWS SDK または CLI GetDomainDetailで を使用する
  - AWS SDK または CLI GetDomainSuggestionsで を使用する
  - AWS SDK または CLI GetOperationDetailで を使用する
  - AWS SDK または CLI ListDomainsで を使用する
  - AWS SDK または CLI ListOperationsで を使用する
  - AWS SDK ListPricesで を使用する
  - AWS SDK または CLI RegisterDomainで を使用する
  - AWS SDK または CLI ViewBillingで を使用する

ハロー Route 53 ドメイン登録

以下のコード例は、Route 53 ドメイン登録の使用を開始する方法を示しています。

.NET

SDK for .NET

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
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}");
        }
    }
```

```
}
```

- API の詳細については、「AWS SDK for .NET API リファレンス」の「ListPrices」を参照してください。

Java

SDK for Java 2.x

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
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);
        }
    }
}
```

- API の詳細については、「AWS SDK for Java 2.x API リファレンス」の「ListPrices」を参照してください。

Kotlin

SDK for Kotlin

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
/**
 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.fromEnvironment { 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}")
            }
```

```
    }
}
```

- API の詳細については、「AWS SDK for Kotlin API リファレンス」の「ListPrices」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK での Route 53 の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

AWS SDK での Route 53 ドメイン登録の基本について説明します。

次のコード例は、以下を実行する方法を示しています。

- 現在のドメインを一覧表示し、過去 1 年間の操作を一覧表示します。
- 過去 1 年間の請求記録とドメインタイプの価格を表示します。
- ドメインの候補を取得します。
- ドメインの可用性と移管可能性を確認します。
- オプションで、ドメイン登録をリクエストします。
- 操作の詳細を入手します。
- オプションで、ドメインの詳細を取得します。

.NET

SDK for .NET

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

コマンドプロンプトからインタラクティブなシナリオを実行します。

```
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 のドメイン登録アクションにシナリオが使用するラッパーメソッド。

```
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.";
        }
    }
}
```

- API の詳細については、「AWS SDK for .NET API リファレンス」の以下のトピックを参照してください。
  - CheckDomainAvailability
  - CheckDomainTransferability
  - GetDomainDetail
  - GetDomainSuggestions
  - GetOperationDetail
  - ListDomains
  - ListOperations
  - ListPrices
  - RegisterDomain
  - ViewBilling

Java

SDK for Java 2.x

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
/**
 * 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);
        }
    }
}
```

- API の詳細については、「AWS SDK for Java 2.x API リファレンス」の以下のトピックを参照してください。
  - CheckDomainAvailability
  - CheckDomainTransferability
  - GetDomainDetail
  - GetDomainSuggestions
  - GetOperationDetail
  - ListDomains
  - ListOperations
  - ListPrices
  - RegisterDomain
  - ViewBilling

Kotlin

SDK for Kotlin

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
/**
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.fromEnvironment { 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.fromEnvironment { 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.fromEnvironment { 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.fromEnvironment { 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.fromEnvironment { 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.fromEnvironment { 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.fromEnvironment { 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.fromEnvironment { 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.fromEnvironment { 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.fromEnvironment { 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}")
            }
    }
}
```

- API の詳細については、「AWS SDK for Kotlin API リファレンス」の以下のトピックを参照してください。
  - CheckDomainAvailability
  - CheckDomainTransferability
  - GetDomainDetail
  - GetDomainSuggestions
  - GetOperationDetail
  - ListDomains
  - ListOperations
  - ListPrices
  - RegisterDomain
  - ViewBilling

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK での Route 53 の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

AWS SDKs を使用した Route 53 ドメイン登録のアクション

次のコード例は、 AWS SDKs で個々の Route 53 ドメイン登録アクションを実行する方法を示しています。それぞれの例には、GitHub へのリンクがあり、そこにはコードの設定と実行に関する説明が記載されています。

以下の例には、最も一般的に使用されるアクションのみ含まれています。詳細な一覧については、「Amazon Route 53 domain registration API リファレンス」を参照してください。

例

- AWS SDK または CLI CheckDomainAvailabilityで を使用する
- AWS SDK または CLI CheckDomainTransferabilityで を使用する
- AWS SDK または CLI GetDomainDetailで を使用する
- AWS SDK または CLI GetDomainSuggestionsで を使用する
- AWS SDK または CLI GetOperationDetailで を使用する
- AWS SDK または CLI ListDomainsで を使用する
- AWS SDK または CLI ListOperationsで を使用する
- AWS SDK ListPricesで を使用する
- AWS SDK または CLI RegisterDomainで を使用する
- AWS SDK または CLI ViewBillingで を使用する

AWS SDK または CLI **CheckDomainAvailability**で を使用する

次のサンプルコードは、CheckDomainAvailability を使用する方法を説明しています。

アクション例は、より大きなプログラムからのコードの抜粋であり、コンテキスト内で実行する必要があります。次のコード例で、このアクションのコンテキストを確認できます。

- 基本を学ぶ

.NET

SDK for .NET

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
/// <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;
}
```

- API の詳細については、「AWS SDK for .NET API リファレンス」の「CheckDomainAvailability」を参照してください。

CLI

AWS CLI

Route 53 を使用してドメイン名を登録できるかどうかを確認するには

次の `check-domain-availability` コマンドは、Route 53 を使用してドメイン名 `example.com` を登録できるかどうかに関する情報を返します。

このコマンドは us-east-1 リージョンでのみ実行されます。デフォルトのリージョンが us-east-1 に設定されている場合は、region パラメータを省略できます。

```
aws route53domains check-domain-availability \
    --region us-east-1 \
    --domain-name example.com
```

出力:

```
{
    "Availability": "UNAVAILABLE"
}
```

Route 53 は、.com や .jp など、多数の最上位ドメイン (TLD) をサポートしていますが、利用可能なすべての TLD をサポートしているわけではありません。ドメインの可用性を確認し、Route 53 が TLD をサポートしていない場合、check-domain-availability は次のメッセージを返します。

```
An error occurred (UnsupportedTLD) when calling the CheckDomainAvailability
 operation: <top-level domain> tld is not supported.
```

Route 53 を使用してドメインを登録する時に使用できる TLD の一覧については、「Amazon Route 53 デベロッパーガイド」の「Amazon Route 53 に登録できるドメイン」を参照してください。Amazon Route 53 を使用してドメインを登録する方法の詳細については、「Amazon Route 53 デベロッパーガイド」の「新しいドメインを登録する」を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス」の「CheckDomainAvailability」を参照してください。

Java

SDK for Java 2.x

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
    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);
        }
    }
```

- API の詳細については、AWS SDK for Java 2.x API リファレンスの「CheckDomainAvailability」を参照してください。

Kotlin

SDK for Kotlin

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
suspend fun checkDomainAvailability(domainSuggestion: String) {
    val availabilityRequest =
        CheckDomainAvailabilityRequest {
            domainName = domainSuggestion
        }
    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
{ route53DomainsClient ->
```

```
        val response =
 route53DomainsClient.checkDomainAvailability(availabilityRequest)
        println("$domainSuggestion is ${response.availability}")
    }
}
```

- API の詳細については、AWS SDK for Kotlin API リファレンスの「CheckDomainAvailability」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK での Route 53 の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

AWS SDK または CLI **CheckDomainTransferability**で を使用する

次のサンプルコードは、CheckDomainTransferability を使用する方法を説明しています。

アクション例は、より大きなプログラムからのコードの抜粋であり、コンテキスト内で実行する必要があります。次のコード例で、このアクションのコンテキストを確認できます。

- 基本を学ぶ

.NET

SDK for .NET

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
    /// <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;
    }
```

- API の詳細については、「AWS SDK for .NET API リファレンス」の「CheckDomainTransferability」を参照してください。

CLI

AWS CLI

Route 53 にドメインを転送できるかどうかを確認するには

次の check-domain-transferability コマンドは、ドメイン名 example.com を Route 53 に転送できるかどうかに関する情報を返します。

このコマンドは us-east-1 リージョンでのみ実行されます。デフォルトのリージョンが us-east-1 に設定されている場合は、region パラメータを省略できます。

```
aws route53domains check-domain-transferability \
    --region us-east-1 \
    --domain-name example.com
```

出力:

```
{
    "Transferability": {
        "Transferable": "UNTRANSFERABLE"
    }
}
```

詳細については、「Amazon Route 53 デベロッパーガイド」の「ドメイン登録の Amazon Route 53 への移管」を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス」の「CheckDomainTransferability」を参照してください。

Java

SDK for Java 2.x

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
   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);
       }
   }
```

- API の詳細については、AWS SDK for Java 2.x API リファレンスの「CheckDomainTransferability」を参照してください。

Kotlin

SDK for Kotlin

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
suspend fun checkDomainTransferability(domainSuggestion: String?) {
    val transferabilityRequest =
        CheckDomainTransferabilityRequest {
            domainName = domainSuggestion
        }
    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
 { route53DomainsClient ->
        val response =
 route53DomainsClient.checkDomainTransferability(transferabilityRequest)
        println("Transferability: ${response.transferability?.transferable}")
    }
}
```

- API の詳細については、AWS SDK for Kotlin API リファレンスの「CheckDomainTransferability」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK での Route 53 の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

AWS SDK または CLI **GetDomainDetail**で を使用する

次のサンプルコードは、GetDomainDetail を使用する方法を説明しています。

アクション例は、より大きなプログラムからのコードの抜粋であり、コンテキスト内で実行する必要があります。次のコード例で、このアクションのコンテキストを確認できます。

- 基本を学ぶ

.NET

SDK for .NET

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
    /// <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.";
        }
    }
```

- API の詳細については、「AWS SDK for .NET API リファレンス」の「GetDomainDetail」を参照してください。

CLI

AWS CLI

指定されたドメインに関する詳細情報を取得するには

次の get-domain-detail コマンドは、指定されたドメインに関する詳細情報を表示します。

このコマンドは us-east-1 リージョンでのみ実行されます。デフォルトのリージョンが us-east-1 に設定されている場合は、region パラメータを省略できます。

```
aws route53domains get-domain-detail \
    --region us-east-1 \
    --domain-name example.com
```

出力:

```
{
    "DomainName": "example.com",
    "Nameservers": [
        {
            "Name": "ns-2048.awsdns-64.com",
            "GlueIps": []
        },
        {
            "Name": "ns-2049.awsdns-65.net",
            "GlueIps": []
        },
        {
            "Name": "ns-2050.awsdns-66.org",
            "GlueIps": []
        },
        {
            "Name": "ns-2051.awsdns-67.co.uk",
            "GlueIps": []
        }
    ],
    "AutoRenew": true,
    "AdminContact": {
        "FirstName": "Saanvi",
        "LastName": "Sarkar",
        "ContactType": "COMPANY",
```

```
        "OrganizationName": "Example",
        "AddressLine1": "123 Main Street",
        "City": "Anytown",
        "State": "WA",
        "CountryCode": "US",
        "ZipCode": "98101",
        "PhoneNumber": "+1.8005551212",
        "Email": "ssarkar@example.com",
        "ExtraParams": []
    },
    "RegistrantContact": {
        "FirstName": "Alejandro",
        "LastName": "Rosalez",
        "ContactType": "COMPANY",
        "OrganizationName": "Example",
        "AddressLine1": "123 Main Street",
        "City": "Anytown",
        "State": "WA",
        "CountryCode": "US",
        "ZipCode": "98101",
        "PhoneNumber": "+1.8005551212",
        "Email": "arosalez@example.com",
        "ExtraParams": []
    },
    "TechContact": {
        "FirstName": "Wang",
        "LastName": "Xiulan",
        "ContactType": "COMPANY",
        "OrganizationName": "Example",
        "AddressLine1": "123 Main Street",
        "City": "Anytown",
        "State": "WA",
        "CountryCode": "US",
        "ZipCode": "98101",
        "PhoneNumber": "+1.8005551212",
        "Email": "wxiulan@example.com",
        "ExtraParams": []
    },
    "AdminPrivacy": true,
    "RegistrantPrivacy": true,
    "TechPrivacy": true,
    "RegistrarName": "Amazon Registrar, Inc.",
    "WhoIsServer": "whois.registrar.amazon",
    "RegistrarUrl": "http://registrar.amazon.com",
```

```
    "AbuseContactEmail": "abuse@registrar.amazon.com",
    "AbuseContactPhone": "+1.2062661000",
    "CreationDate": 1444934889.601,
    "ExpirationDate": 1602787689.0,
    "StatusList": [
        "clientTransferProhibited"
    ]
}
```

- API の詳細については、「AWS CLI コマンドリファレンス」の「GetDomainDetail」を参照してください。

Java

SDK for Java 2.x

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
   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);
        }
    }
```

- API の詳細については、「AWS SDK for Java 2.x API リファレンス」の「GetDomainDetail」を参照してください。

Kotlin

SDK for Kotlin

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
suspend fun getDomainDetails(domainSuggestion: String?) {
    val detailRequest =
        GetDomainDetailRequest {
            domainName = domainSuggestion
        }
    Route53DomainsClient.fromEnvironment { 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}")
    }
}
```

- API の詳細については、「AWS SDK for Kotlin API リファレンス」の「GetDomainDetail」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK での Route 53 の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

AWS SDK または CLI **GetDomainSuggestions**で を使用する

次のサンプルコードは、GetDomainSuggestions を使用する方法を説明しています。

アクション例は、より大きなプログラムからのコードの抜粋であり、コンテキスト内で実行する必要があります。次のコード例で、このアクションのコンテキストを確認できます。

- 基本を学ぶ

.NET

SDK for .NET

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
    /// <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;
    }
```

- API の詳細については、「AWS SDK for .NET API リファレンス」の「GetDomainSuggestions」を参照してください。

CLI

AWS CLI

推奨されるドメイン名のリストを取得するには

次の get-domain-suggestions コマンドは、ドメイン名 example.com に基づいて推奨されるドメイン名のリストを表示します。レスポンスには、利用可能なドメイン名のみが含まれます。このコマンドは us-east-1 リージョンでのみ実行されます。デフォルトのリージョンが us-east-1 に設定されている場合は、region パラメータを省略できます。

```
aws route53domains get-domain-suggestions \
    --region us-east-1 \
    --domain-name example.com \
    --suggestion-count 10 \
    --only-available
```

出力:

```
{
    "SuggestionsList": [
        {
            "DomainName": "egzaampal.com",
            "Availability": "AVAILABLE"
        },
        {
            "DomainName": "examplelaw.com",
            "Availability": "AVAILABLE"
        },
        {
            "DomainName": "examplehouse.net",
```

```
            "Availability": "AVAILABLE"
        },
        {
            "DomainName": "homeexample.net",
            "Availability": "AVAILABLE"
        },
        {
            "DomainName": "examplelist.com",
            "Availability": "AVAILABLE"
       },
        {
            "DomainName": "examplenews.net",
            "Availability": "AVAILABLE"
        },
        {
            "DomainName": "officeexample.com",
            "Availability": "AVAILABLE"
        },
        {
            "DomainName": "exampleworld.com",
            "Availability": "AVAILABLE"
        },
        {
            "DomainName": "exampleart.com",
            "Availability": "AVAILABLE"
        }
    ]
}
```

- API の詳細については、「AWS CLI コマンドリファレンス」の「GetDomainSuggestions」を参照してください。

Java

SDK for Java 2.x

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
   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);
       }
   }
```

- API の詳細については、「AWS SDK for Java 2.x API リファレンス」の「GetDomainSuggestions」を参照してください。

Kotlin

SDK for Kotlin

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
suspend fun listDomainSuggestions(domainSuggestion: String?) {
```

```
    val suggestionsRequest =
        GetDomainSuggestionsRequest {
            domainName = domainSuggestion
            suggestionCount = 5
            onlyAvailable = true
        }
    Route53DomainsClient.fromEnvironment { 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(" ")
        }
    }
}
```

- API の詳細については、「AWS API リファレンス」の「GetDomainSuggestions」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK での Route 53 の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

AWS SDK または CLI **GetOperationDetail**で を使用する

次のサンプルコードは、GetOperationDetail を使用する方法を説明しています。

アクション例は、より大きなプログラムからのコードの抜粋であり、コンテキスト内で実行する必要があります。次のコード例で、このアクションのコンテキストを確認できます。

- 基本を学ぶ

.NET

SDK for .NET

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
    /// <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}.";
        }
```

```
    }
```

- API の詳細については、「AWS SDK for .NET API リファレンス」の「GetOperationDetail」を参照してください。

CLI

AWS CLI

オペレーションの現在のステータスを取得するには

一部のドメイン登録オペレーションは非同期的に動作し、完了する前にレスポンスを返します。これらのオペレーションは、現在のステータスを取得するために使用できるオペレーション ID を返します。次の get-operation-detail コマンドは、指定されたオペレーションのステータスを返します。

このコマンドは us-east-1 リージョンでのみ実行されます。デフォルトのリージョンが us-east-1 に設定されている場合は、region パラメータを省略できます。

```
aws route53domains get-operation-detail \
    --region us-east-1 \
    --operation-id edbd8d63-7fe7-4343-9bc5-54033example
```

出力:

```
{
    "OperationId": "edbd8d63-7fe7-4343-9bc5-54033example",
    "Status": "SUCCESSFUL",
    "DomainName": "example.com",
    "Type": "DOMAIN_LOCK",
    "SubmittedDate": 1573749367.864
}
```

- API の詳細については、「AWS CLI コマンドリファレンス」の「GetOperationDetail」を参照してください。

Java

SDK for Java 2.x

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
   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);
       }
   }
```

- API の詳細については、AWS SDK for Java 2.x API リファレンスの「GetOperationDetail」を参照してください。

Kotlin

SDK for Kotlin

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
suspend fun getOperationalDetail(opId: String?) {
    val detailRequest =
        GetOperationDetailRequest {
            operationId = opId
        }
    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
 { route53DomainsClient ->
        val response = route53DomainsClient.getOperationDetail(detailRequest)
        println("Operation detail message is ${response.message}")
    }
}
```

- API の詳細については、AWS SDK for Kotlin API リファレンスの「GetOperationDetail」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK での Route 53 の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

AWS SDK または CLI **ListDomains**で を使用する

次のサンプルコードは、ListDomains を使用する方法を説明しています。

アクション例は、より大きなプログラムからのコードの抜粋であり、コンテキスト内で実行する必要があります。次のコード例で、このアクションのコンテキストを確認できます。

- 基本を学ぶ

.NET

SDK for .NET

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
/// <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;
}
```

- API の詳細については、「AWS SDK for .NET API リファレンス」の「ListDomains」を参照してください。

CLI

AWS CLI

現在の AWS アカウントに登録されているドメインを一覧表示するには

次の `list-domains` コマンドは、現在の AWS アカウントに登録されているドメインに関する概要情報を一覧表示します。

このコマンドは us-east-1 リージョンでのみ実行されます。デフォルトのリージョンが us-east-1 に設定されている場合は、region パラメータを省略できます。

```
aws route53domains list-domains
    --region us-east-1
```

出力:

```
{
    "Domains": [
        {
            "DomainName": "example.com",
            "AutoRenew": true,
            "TransferLock": true,
            "Expiry": 1602712345.0
        },
        {
            "DomainName": "example.net",
            "AutoRenew": true,
            "TransferLock": true,
            "Expiry": 1602723456.0
        },
        {
            "DomainName": "example.org",
            "AutoRenew": true,
            "TransferLock": true,
            "Expiry": 1602734567.0
        }
    ]
}
```

- API の詳細については、「AWS CLI コマンドリファレンス」の「ListDomains」を参照してください。

Java

SDK for Java 2.x

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
    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);
        }
    }
```

- API の詳細については、「AWS SDK for Java 2.x API リファレンス」の「ListDomains」を参照してください。

Kotlin

SDK for Kotlin

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
suspend fun listDomains() {
```

```
    Route53DomainsClient.fromEnvironment { 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}")
            }
    }
}
```

- API の詳細については、「AWS SDK for Kotlin API リファレンス」の「ListDomains」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK での Route 53 の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

AWS SDK または CLI **ListOperations**で を使用する

次のサンプルコードは、ListOperations を使用する方法を説明しています。

アクション例は、より大きなプログラムからのコードの抜粋であり、コンテキスト内で実行する必要があります。次のコード例で、このアクションのコンテキストを確認できます。

- 基本を学ぶ

.NET

SDK for .NET

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
    /// <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;
    }
```

- API の詳細については、「AWS SDK for .NET API リファレンス」の「ListOperations」を参照してください。

CLI

AWS CLI

オペレーション ID を返すオペレーションのステータスを一覧表示するには

一部のドメイン登録オペレーションは非同期的に実行され、完了する前にレスポンスを返します。これらのオペレーションは、現在のステータスを取得するために使用できるオペレーション ID を返します。次の `list-operations` コマンドは、現在のドメイン登録オペレーションに関するステータスを含む概要情報を一覧表示します。

このコマンドは `us-east-1` リージョンでのみ実行されます。デフォルトのリージョンが `us-east-1` に設定されている場合は、`region` パラメータを省略できます。

```
aws route53domains list-operations
    --region us-east-1
```

出力:

```
{
    "Operations": [
        {
            "OperationId": "aab9822f-1da0-4bf3-8a15-fd4e0example",
            "Status": "SUCCESSFUL",
            "Type": "DOMAIN_LOCK",
            "SubmittedDate": 1455321739.986
        },
        {
            "OperationId": "c24379ed-76be-42f8-bdad-9379bexample",
            "Status": "SUCCESSFUL",
            "Type": "UPDATE_NAMESERVER",
            "SubmittedDate": 1468960475.109
        },
        {
            "OperationId": "f47e1297-ef9e-4c2b-ae1e-a5fcbexample",
            "Status": "SUCCESSFUL",
            "Type": "RENEW_DOMAIN",
            "SubmittedDate": 1473561835.943
        },
        {
            "OperationId": "75584f23-b15f-459e-aed7-dc6f5example",
            "Status": "SUCCESSFUL",
            "Type": "UPDATE_DOMAIN_CONTACT",
            "SubmittedDate": 1547501003.41
        }
    ]
}
```

出力には、オペレーション ID を返し、現在の AWS アカウントを使用して登録したすべてのドメインで実行したすべてのオペレーションが含まれます。指定した日付以降に送信したオペレーションのみを取得する場合は、submitted-since パラメータを含めて、Unix 形式と協定世界時 (UTC) で日付を指定できます。次のコマンドは、2020 年 1 月 1 日の UTC 午前 12 時以降に送信されたすべてのオペレーションのステータスを取得します。

```
aws route53domains list-operations \
    --submitted-since 1577836800
```

- API の詳細については、「AWS CLI コマンドリファレンス」の「ListOperations」を参照してください。

Java

SDK for Java 2.x

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
   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);
       }
   }
```

- API の詳細については、「AWS SDK for Java 2.x API リファレンス」の「ListOperations」を参照してください。

Kotlin

SDK for Kotlin

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
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.fromEnvironment { 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}")
            }
    }
}
```

- API の詳細については、「AWS SDK for Kotlin API リファレンス」の「ListOperations」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK での Route 53 の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

AWS SDK **ListPrices**で を使用する

次のサンプルコードは、ListPrices を使用する方法を説明しています。

アクション例は、より大きなプログラムからのコードの抜粋であり、コンテキスト内で実行する必要があります。次のコード例で、このアクションのコンテキストを確認できます。

- 基本を学ぶ

.NET

SDK for .NET

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
    /// <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();
    }
```

- API の詳細については、「AWS SDK for .NET API リファレンス」の「ListPrices」を参照してください。

Java

SDK for Java 2.x

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
   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);
```

```
        }
    }
```

- API の詳細については、「AWS SDK for Java 2.x API リファレンス」の「ListPrices」を参照してください。

Kotlin

SDK for Kotlin

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
suspend fun listAllPrices(domainType: String?) {
    val pricesRequest =
        ListPricesRequest {
            tld = domainType
        }

    Route53DomainsClient.fromEnvironment { 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}")
            }
    }
}
```

- API の詳細については、「AWS SDK for Kotlin API リファレンス」の「ListPrices」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK での Route 53 の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

AWS SDK または CLI **RegisterDomain**で を使用する

次のサンプルコードは、RegisterDomain を使用する方法を説明しています。

アクション例は、より大きなプログラムからのコードの抜粋であり、コンテキスト内で実行する必要があります。次のコード例で、このアクションのコンテキストを確認できます。

- 基本を学ぶ

.NET

SDK for .NET

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
    /// <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;
        }
    }
```

- API の詳細については、「AWS SDK for .NET API リファレンス」の「RegisterDomain」を参照してください。

CLI

AWS CLI

ドメインを登録するには

次の `register-domain` コマンドはドメインを登録し、JSON 形式のファイルからすべてのパラメータ値を取得します。

このコマンドは `us-east-1` リージョンでのみ実行されます。デフォルトのリージョンが `us-east-1` に設定されている場合は、`region` パラメータを省略できます。

```
aws route53domains register-domain \
    --region us-east-1 \
    --cli-input-json file://register-domain.json
```

register-domain.json の内容:

```
{
    "DomainName": "example.com",
    "DurationInYears": 1,
    "AutoRenew": true,
    "AdminContact": {
        "FirstName": "Martha",
        "LastName": "Rivera",
        "ContactType": "PERSON",
        "OrganizationName": "Example",
        "AddressLine1": "1 Main Street",
        "City": "Anytown",
        "State": "WA",
        "CountryCode": "US",
        "ZipCode": "98101",
        "PhoneNumber": "+1.8005551212",
        "Email": "mrivera@example.com"
    },
    "RegistrantContact": {
        "FirstName": "Li",
        "LastName": "Juan",
        "ContactType": "PERSON",
        "OrganizationName": "Example",
        "AddressLine1": "1 Main Street",
        "City": "Anytown",
        "State": "WA",
        "CountryCode": "US",
        "ZipCode": "98101",
        "PhoneNumber": "+1.8005551212",
        "Email": "ljuan@example.com"
    },
    "TechContact": {
        "FirstName": "Mateo",
        "LastName": "Jackson",
        "ContactType": "PERSON",
        "OrganizationName": "Example",
        "AddressLine1": "1 Main Street",
        "City": "Anytown",
```

```
        "State": "WA",
        "CountryCode": "US",
        "ZipCode": "98101",
        "PhoneNumber": "+1.8005551212",
        "Email": "mjackson@example.com"
    },
    "PrivacyProtectAdminContact": true,
    "PrivacyProtectRegistrantContact": true,
    "PrivacyProtectTechContact": true
}
```

出力:

```
{
    "OperationId": "b114c44a-9330-47d1-a6e8-a0b11example"
}
```

オペレーションが成功したことを確認するには、`get-operation-detail` を実行します。詳細については、「get-operation-detail」を参照してください。

詳細については、「Amazon Route 53 デベロッパーガイド」の「新しいドメインの登録」を参照してください。

`ExtraParams` の最上位ドメイン (TLD) に必要な値と有効な値については「Amazon Route 53 API リファレンス」の「ExtraParam」を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス」の「RegisterDomain」を参照してください。

Java

SDK for Java 2.x

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
    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 "";
    }
```

- API の詳細については、「AWS SDK for Java 2.x API リファレンス」の「RegisterDomain」を参照してください。

Kotlin

SDK for Kotlin

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
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.fromEnvironment { region = "us-east-1" }.use
 { route53DomainsClient ->
        val response = route53DomainsClient.registerDomain(domainRequest)
        println("Registration requested. Operation Id: ${response.operationId}")
        return response.operationId
    }
}
```

- API の詳細については、「AWS SDK for Kotlin API リファレンス」の「RegisterDomain」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK での Route 53 の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

AWS SDK または CLI **ViewBilling**で を使用する

次のサンプルコードは、ViewBilling を使用する方法を説明しています。

アクション例は、より大きなプログラムからのコードの抜粋であり、コンテキスト内で実行する必要があります。次のコード例で、このアクションのコンテキストを確認できます。

- 基本を学ぶ

.NET

SDK for .NET

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
    /// <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;
    }
```

- API の詳細については、「AWS SDK for .NET API リファレンス」の「ViewBilling」を参照してください。

CLI

AWS CLI

現在の AWS アカウントのドメイン登録料金の請求情報を取得するには

次の `view-billing` コマンドは、2018 年 1 月 1 日 (Unix 時間で 1514764800) から 2019 年 12 月 31 日深夜 (Unix 時間で 1577836800) までの間、現在のアカウントのすべてのドメイン関連の請求レコードを返します。

このコマンドは `us-east-1` リージョンでのみ実行されます。デフォルトのリージョンが `us-east-1` に設定されている場合は、`region` パラメータを省略できます。

```
aws route53domains view-billing \
    --region us-east-1 \
    --start-time 1514764800 \
    --end-time 1577836800
```

出力:

```
{
    "BillingRecords": [
        {
            "DomainName": "example.com",
            "Operation": "RENEW_DOMAIN",
            "InvoiceId": "149962827",
            "BillDate": 1536618063.181,
            "Price": 12.0
        },
        {
            "DomainName": "example.com",
            "Operation": "RENEW_DOMAIN",
            "InvoiceId": "290913289",
            "BillDate": 1568162630.884,
            "Price": 12.0
        }
    ]
}
```

詳細については、「Amazon Route 53 API リファレンス」の「ViewBilling」を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス」の「ViewBilling」を参照してください。

Java

SDK for Java 2.x

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
   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);
       }
   }
```

- API の詳細については、「AWS SDK for Java 2.x API リファレンス」の「ViewBilling」を参照してください。

Kotlin

SDK for Kotlin

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
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.fromEnvironment { 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}")
            }
    }
}
```

- API の詳細については、「AWS SDK for Kotlin API リファレンス」の「ViewBilling」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK での Route 53 の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

Amazon Route 53 でのセキュリティ

でのクラウドセキュリティが最優先事項 AWS です。お客様は AWS 、セキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャを活用できます。

セキュリティは、 AWS お客様とお客様の間の責任共有です。責任共有モデルでは、これをクラウドのセキュリティおよびクラウド内のセキュリティとして説明しています。

- クラウドのセキュリティ – AWS クラウドで AWS サービスを実行するインフラストラクチャを保護する AWS 責任があります。 AWS また、 では、安全に使用できるサービスも提供しています。「AWS 」 コンプライアンスプログラムの一環として、サードパーティーの監査が定期的にセキュリティの有効性をテストおよび検証しています。Amazon Route 53 に適用されるコンプライアンスプログラムの詳細については、コンプライアンスプログラムによるAWS 対象範囲内のサービスを参照してください。
- クラウドのセキュリティ – お客様の責任は、使用する AWS サービスによって決まります。また、お客様は、お客様のデータの機密性、企業の要件、および適用可能な法律および規制などの他の要因についても責任を担います。

このドキュメントは、Route 53 を使用する際に責任共有モデルを適用する方法を理解するのに役立ちます。以下のトピックでは、セキュリティおよびコンプライアンスの目的を達成するために Route 53 を設定する方法を示します。また、Route 53 リソースのモニタリングや保護に役立つ他の AWS サービスの使用方法についても説明します。

トピック

- Route 53 でのデータ保護
- Amazon Route 53 での Identity and Access Management
- Amazon Route 53 でのログ記録とモニタリング
- Amazon Route 53 のコンプライアンス検証
- Amazon Route 53 での耐障害性
- Amazon Route 53 でのインフラストラクチャセキュリティ

Route 53 でのデータ保護

責任共有モデル、Amazon Route AWS 53 でのデータ保護に適用されます。このモデルで説明されているように、 AWS はすべての を実行するグローバルインフラストラクチャを保護する責任があります AWS クラウド。ユーザーは、このインフラストラクチャでホストされるコンテンツに対する管理を維持する責任があります。また、使用する「 AWS のサービス 」のセキュリティ設定と管理タスクもユーザーの責任となります。データプライバシーの詳細については、「Data Privacy FAQChina」を参照してください。 欧州におけるデータ保護に関する情報については、General Data Protection Regulation (GDPR) Center を参照してください。

データ保護の目的で、認証情報を保護し AWS アカウント 、 AWS IAM アイデンティティセンターまたは AWS Identity and Access Management (IAM) を使用して個々のユーザーを設定することをお勧めします。この方法により、それぞれのジョブを遂行するために必要な権限のみが各ユーザーに付与されます。また、次の方法でデータを保護することもお勧めします:

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して AWS リソースと通信します。TLS 1.2 は必須ですが、TLS 1.3 を推奨します。
- で API とユーザーアクティビティのログ記録を設定します AWS CloudTrail。CloudTrail 証跡を使用して AWS アクティビティをキャプチャする方法については、「 AWS CloudTrail ユーザーガイド」のCloudTrail 証跡の使用」を参照してください。
- AWS 暗号化ソリューションと、その中のすべてのデフォルトのセキュリティコントロールを使用します AWS のサービス。
- Amazon Macie などの高度な管理されたセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- コマンドラインインターフェイスまたは API AWS を介して にアクセスするときに FIPS 140-3 検証済み暗号化モジュールが必要な場合は、FIPS エンドポイントを使用します。利用可能な FIPS エンドポイントの詳細については、「連邦情報処理規格 (FIPS) 140-3」を参照してください。

お客様の E メールアドレスなどの極秘または機密情報を、タグ、または [名前] フィールドなどの自由形式のテキストフィールドに含めないことを強くお勧めします。これは、コンソール、API、または SDK を使用して Route 53 AWS CLIまたは他の AWS のサービス を使用する場合も同様です。AWS SDKs タグ、または名前に使用される自由記述のテキストフィールドに入力したデータは、請求または診断ログに使用される場合があります。外部サーバーに URL を提供する場合、そのサーバーへのリクエストを検証できるように、認証情報を URL に含めないことを強くお勧めします。

Route 53 でのダングリング委任レコードからの保護

Route 53 を使用すると、顧客は example.com などのホストゾーンを作成して、DNS レコードをホストできます。各ホストゾーンには「委託セット」が付属しています。これは、顧客が親ドメインで NS レコードを設定するために使用できる 4 つのネームサーバーのセットです。これらの NS レコードは、「委託 NS レコード」または「委任レコード」と呼ばれます。

example.com Route 53 ホストゾーンを権威あるものにするには、example.com ドメインの正当な所有者がドメインレジストラを通じて「.com」親ドメインに委任レコードを設定する必要があります。関連付けられたホストゾーンが削除されるなど、お客様が親ドメインに設定された 4 つのネームサーバーにアクセスできなくなった場合、攻撃者が悪用するリスクが発生する可能性があります。これは「ダングリング委任レコード」リスクと呼ばれます。

ホストゾーンが削除された場合、Route 53 によりダングリング委任レコードのリスクから保護されます。削除後、同じドメイン名で新しいホストゾーンが作成されている場合、Route 53 は、削除されたホストゾーンを指す委任レコードが親ドメインにまだ存在するかどうかを確認します。存在する場合、Route 53 は重複するネームサーバーが割り当てられないようにします。これは次の例のシナリオ 1 です。

ただし、次の例のシナリオ 2 から 5 で説明されているように、Route 53 が保護できないダングリング委任レコードリスクは他にもあります。より広範なこのリスクセットからユーザーを保護するには、親 NS レコードが Route 53 ホストゾーンの委任セットと一致していることを確認してください。ホストゾーンの委任セットは、Route 53 コンソールまたは で確認できます AWS CLI。詳細については、「レコードの一覧表示」または「get-hosted-zone」を参照してください。

さらに、Route 53 ホストゾーンの DNSSEC 署名を有効にすると、上述のベストプラクティスを超えた保護の別のレイヤーとして機能することができます。DNSSEC は DNS の回答が信頼できる送信元からのものであることを認証し、このリスクを効果的に防止します。詳細については、「Amazon Route 53 での DNSSEC 署名の設定」を参照してください。

例

次の例では、ドメイン example.com とその子ドメイン child.example.com があると仮定します。さまざまなシナリオでダングリング委任レコードを作成する方法、Route 53 がドメインを悪用から保護する方法、およびダングリング委任レコードに関連するリスクを効果的に軽減する方法を説明します。

シナリオ 1:

4 個のネームサーバー <ns1>、<ns2>、<ns3>、および <ns4> を使用してホストゾーン child.example.com を作成します。ホストゾーン example.com で委任を適切に設定し、4 つのネームサーバー <ns1>、<ns2>、<ns3>、および <ns4> を使用して child.example.com の委任 NS レコードを作成します。example.com の委任 NS レコードを削除せずに child.example.com ホストゾーンが削除されると、Route 53 は、<ns1>、<ns2>、<ns3>、および <ns4> が同じドメイン名で新しく作成されたホストゾーンに割り当てられないようにすることで、ダングリング委任レコードのリスクから child.example.com を保護します。

シナリオ 2:

シナリオ 1 と同様ですが、今回は子ホストゾーンと、ホストゾーン example.com の委任 NS レコードを削除します。ただし、子ホストゾーンを作成せずに、委任 NS レコード <ns1>、<ns2>、<ns3>、および <ns4> を再度追加します。ここでは、<ns1>、<ns2>、<ns3>、および <ns4> はダングリング委任レコードです。Route 53 は保留が削除されるため、<ns1>、<ns2>、<ns3>、および <ns4> が割り当てられなくなり、新しく作成されたホストゾーンがネームサーバー上で使用できるようになりました。リスクを軽減するには、委任レコードから <ns1>、<ns2>、<ns3>、<ns4> を削除し、子ホストゾーンの作成後にのみそれらを追加します。

シナリオ 3:

このシナリオでは、ネームサーバー <ns1>、<ns2>、<ns3>、および <ns4> を使用して Route 53 の再利用可能な委託セットを作成します。次に、親ドメイン .com 内のこれらのネームサーバーにドメイン example.com を委任します。ただし、再利用可能な委託セットには example.com のホストゾーンをまだ作成していません。ここでは、<ns1>、<ns2>、<ns3>、および <ns4> は、ダングリング委任レコードです。リスクを軽減するには、ネームサーバー <ns1>、<ns2>、<ns3>、および <ns4> で再利用可能な委託セットを使用してホストゾーンを作成します。

シナリオ 4:

ホストゾーンは、child.example.comネームサーバー <ns1>、<ns2>、<ns3>、<ns4> と、grandchild.child.example.comネームサーバー <ns5>、<ns6>、<ns7>、<ns8> の両方で作成します。ただし、両方をexample.comゾーンに直接委任すると、ダングリング委任リスクが発生します。委任が適切な DNS 階層に従うようにするには、直接の親ゾーンを介してサブドメインのみを委任します。たとえば、 を委任する場合grandchild.child.example.com: 最初にexample.comゾーンchild.example.com内のネームサーバー <ns1>、<ns2>、<ns3>、<ns4> で委任し、次にchild.example.comゾーン内

のネームサーバー <ns5>、<ns6>、<ns7>、<ns8> grandchild.child.example.comで委任し、example.comゾーンgrandchild.child.example.comから の直接委任を削除します。

シナリオ 5:

対応するホストゾーンを作成する前に、ドメインまたはサブドメインを Route 53 ネームサーバーに委任すると、ダングリング委任レコードが作成されます。これはシナリオ 3 の場合と似ていますが、再利用可能な委任セットが作成されない場合にもリスクが適用されます。たとえば、親ドメイン のネームサーバー <ns1>、<ns2>、<ns3>、<ns4> example.comにドメインを委任しますが.com、これらのネームサーバーが をホストしたことはありませんexample.com。Route 53 は、そのドメイン名のネームサーバーに保留を確立するためのホストゾーンが存在しないため、これから保護できません。リスクを軽減するには、自分が管理するパブリックホストゾーンに属する Route 53 ネームサーバーにのみ委任します。

Amazon Route 53 での Identity and Access Management

(AWS Identity and Access Management IAM) では、ドメインの登録やレコードの更新など、Amazon Route 53 リソースに対してオペレーションを実行するには、承認された AWS ユーザーであることを認証する必要があります。Route 53 コンソールを使用している場合は、 AWS ユーザー名およびパスワードを指定して、自分の ID を認証します。

ID を認証すると、IAM は、オペレーションを実行し、リソースにアクセスするためのアクセス許可があること AWS を確認して、 へのアクセスを制御します。アカウント管理者である場合、IAM を使用して、アカウントに関連付けられたリソースへの他のユーザーのアクセスをコントロールできます。

この章では、IAM および Route 53 を使ってリソースを保護する方法について説明します。

トピック

- アイデンティティを使用した認証
- アクセスコントロール
- のサービスにリンクされたロールの使用 Amazon Route 53 Resolver
- AWS Amazon Route 53 の マネージドポリシー
- 詳細に設定されたアクセスコントロールのための IAM ポリシー条件の使用
- Amazon Route 53 API のアクセス許可: アクション、リソース、条件のリファレンス

アイデンティティを使用した認証

認証とは、ID 認証情報 AWS を使用して にサインインする方法です。、IAM ユーザー AWS アカウントのルートユーザー、または IAM ロールを引き受けることで認証される必要があります。

AWS IAM アイデンティティセンター (IAM Identity Center)、シングルサインオン認証、Google/Facebook 認証情報などの ID ソースからの認証情報を使用して、フェデレーティッド ID としてサインインできます。サインインの詳細については、「AWS サインイン ユーザーガイド」の「AWS アカウントにサインインする方法」を参照してください。

プログラムによるアクセスの場合、 は SDK と CLI AWS を提供してリクエストを暗号化して署名します。詳細については、「IAM ユーザーガイド」の「API リクエストに対するAWS 署名バージョン 4」を参照してください。

AWS アカウント ルートユーザー

を作成するときは AWS アカウント、すべての AWS のサービス および リソースへの完全なアクセス権を持つ AWS アカウント ルートユーザーと呼ばれる 1 つのサインインアイデンティティから始めます。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザー認証情報を必要とするタスクについては、「IAM ユーザーガイド」の「ルートユーザー認証情報が必要なタスク」を参照してください。

フェデレーテッドアイデンティティ

ベストプラクティスとして、人間のユーザーが一時的な認証情報 AWS のサービス を使用して にアクセスするには、ID プロバイダーとのフェデレーションを使用する必要があります。

フェデレーティッド ID は、エンタープライズディレクトリ、ウェブ ID プロバイダー、または ID Directory Service ソースの認証情報 AWS のサービス を使用して にアクセスするユーザーです。フェデレーテッドアイデンティティは、一時的な認証情報を提供するロールを引き受けます。

アクセスを一元管理する場合は、 AWS IAM アイデンティティセンターをお勧めします。詳細については、「AWS IAM アイデンティティセンター ユーザーガイド」の「IAM アイデンティティセンターとは」を参照してください。

IAM ユーザーとグループ

IAM ユーザーは、特定の個人やアプリケーションに対する特定のアクセス許可を持つアイデンティティです。長期認証情報を持つ IAM ユーザーの代わりに一時的な認証情報を使用することをお勧めします。詳細については、IAM ユーザーガイドの「ID プロバイダーとのフェデレーションを使用して にアクセスする必要がある AWS」を参照してください。

IAM グループは、IAM ユーザーの集合を指定し、大量のユーザーに対するアクセス許可の管理を容易にします。詳細については、「IAM ユーザーガイド」の「IAM ユーザーに関するユースケース」を参照してください。

IAM ロール

IAM ロールは、特定のアクセス許可を持つアイデンティであり、一時的な認証情報を提供します。ユーザーから IAM ロール (コンソール) に切り替えるか、 または API オペレーションを呼び出すことで、ロールを引き受けることができます。 AWS CLI AWS 詳細については、「IAM ユーザーガイド」の「ロールを引き受けるための各種方法」を参照してください。

IAM ロールは、フェデレーションユーザーアクセス、一時的な IAM ユーザーのアクセス許可、クロスアカウントアクセス、クロスサービスアクセス、および Amazon EC2 で実行するアプリケーションに役立ちます。詳細については、IAM ユーザーガイド の IAM でのクロスアカウントリソースアクセス を参照してください。

アクセスコントロール

Amazon Route 53 リソースを作成、更新、削除、またはリストするには、オペレーションを実行するアクセス許可と、対応するリソースにアクセスするアクセス許可が必要です。

以下のセクションでは、Route 53 のアクセス許可を管理する方法について説明します。最初に概要のセクションを読むことをお勧めします。

トピック

- Amazon Route 53 リソースに対するアクセス許可の管理の概要
- Amazon Route 53 での ID ベースのポリシー (IAM ポリシー) の使用

Amazon Route 53 リソースに対するアクセス許可の管理の概要

すべての AWS リソースは AWS アカウントによって所有され、リソースを作成またはアクセスするためのアクセス許可はアクセス許可ポリシーによって管理されます。

> **Note**
>
> アカウント管理者 (または管理者ユーザー) は、管理者権限を持つユーザーです。管理者の詳細については、IAM ユーザーガイドの「IAM ベストプラクティス」を参照してください。

アクセス許可を付与するときは、アクセス許可を取得するユーザー、アクセス許可を取得する対象のリソース、およびアクセス許可を取得して実行するアクションを決定します。

ユーザーが の AWS 外部とやり取りする場合は、プログラムによるアクセスが必要です AWS マネジメントコンソール。プログラムによるアクセスを許可する方法は、 がアクセスするユーザーのタイプによって異なります AWS。

ユーザーにプログラムによるアクセス権を付与するには、以下のいずれかのオプションを選択します。

プログラムによるアクセス権を必要とするユーザー	目的	方法
IAM	(推奨) コンソール認証情報を一時的な認証情報として使用して AWS CLI、、 AWS SDKs、または AWS APIs。	使用するインターフェイスの指示に従ってください。 • については AWS CLI、AWS Command Line Interface「 ユーザーガイド」のAWS「ローカル開発のためのログイン」を参照してください。 • AWS SDKs「 SDK およびツールリファレンスガイド」の「Login for AWS local development」を参照してください。 AWS SDKs
ワークフォースアイデンティティ (IAM アイデンティティセンターで管理されているユーザー)	一時的な認証情報を使用して AWS CLI、、 AWS SDKs、または AWS APIs。	使用するインターフェイスの指示に従ってください。 • については AWS CLI、AWS Command Line Interface ユーザーガイドの「 を使用する AWS CLI ための の設定 AWS IAM アイデンティティセンター」を参照してください。

プログラムによるアクセス権を必要とするユーザー	目的	方法
		• AWS SDKs、ツール、API AWS APIs「 SDK およびツールリファレンスガイド」の「IAM アイデンティティセンター認証」を参照してください。 AWS SDKs
IAM	一時的な認証情報を使用して AWS CLI、、 AWS SDKs、または AWS APIs。	「IAM ユーザーガイド」の「 AWS リソースでの一時的な認証情報の使用」の手順に従います。
IAM	(非推奨) 長期認証情報を使用して、AWS CLI、 AWS SDKs、または AWS APIs。	使用するインターフェイスの指示に従ってください。 • については AWS CLI、「 AWS Command Line Interface ユーザーガイド」の「IAM ユーザー認証情報を使用した認証」を参照してください。 • AWS SDKs「 SDK とツールリファレンスガイド」の「長期認証情報を使用した認証」を参照してください。 AWS SDKs • API AWS APIs「IAM ユーザーガイド」の「IAM ユーザーのアクセスキーの管理」を参照してください。

トピック

- Amazon Route 53 リソースの ARN

- リソース所有権についての理解
- リソースへのアクセスの管理
- ポリシー要素の指定: リソース、アクション、効果、プリンシパル
- ポリシーでの条件を指定する

Amazon Route 53 リソースの ARN

Amazon Route 53 は、DNS、ヘルスチェック、ドメイン登録用にさまざまなリソースタイプをサポートしています。ポリシーでは、ARN の * を使用して、以下のリソースへのアクセスを許可したり、拒否することができます。

- ヘルスチェック
- ホストゾーン
- 再利用可能な委託セット
- リソースレコードセット変更バッチのステータス (API のみ)
- トラフィックポリシー (トラフィックフロー)
- トラフィックポリシーのインスタンス (トラフィックフロー)

すべての Route 53 リソースでアクセス許可がサポートされているわけではありません。次のリソースへのアクセスを許可したり拒否したりすることはできません。

- ドメイン
- 個々のレコード
- ドメインのタグ
- ヘルスチェックのタグ
- ホストゾーンのタグ

Route 53 には、これらの各タイプのリソースで使用できる API アクションが用意されています。詳細については、「Amazon Route 53 API リファレンス」を参照してください。各アクションを使用するアクセス許可を付与または拒否するために指定するアクションおよび ARN のリストについては、「Amazon Route 53 API のアクセス許可: アクション、リソース、条件のリファレンス」を参照してください。

リソース所有権についての理解

AWS アカウントは、リソースを作成したユーザーに関係なく、アカウントで作成されたリソースを所有します。具体的には、リソース所有者は、リソース作成リクエストを認証するプリンシパルエンティティ (ルートアカウント、または IAM ロール) AWS のアカウントです。

次の例は、この仕組みを示しています。

- AWS アカウントのルートアカウントの認証情報を使用してホストゾーンを作成する場合、 AWS アカウントはリソースの所有者です。
- AWS アカウントにユーザーを作成し、そのユーザーにホストゾーンを作成するアクセス許可を付与すると、そのユーザーはホストゾーンを作成できます。ただし、ユーザーが属する AWS アカウントはホストゾーンリソースを所有しています。
- AWS アカウントにホストゾーンを作成するアクセス許可を持つ IAM ロールを作成すると、ロールを引き受けることのできるすべてのユーザーがホストゾーンを作成できます。ロールが属する AWS アカウントは、ホストゾーンリソースを所有します。

リソースへのアクセスの管理

アクセス許可のポリシーでは、誰が何にアクセスできるかを指定します。このセクションでは、Amazon Route 53 のアクセス許可ポリシーを作成するために使用可能なオプションについて説明します。IAM ポリシー構文の概説については、IAM ユーザーガイドの AWS IAM ポリシーリファレンスを参照してください。

IAM ID にアタッチされたポリシーは ID ベースのポリシー (IAM ポリシー) と呼ばれ、リソースにアタッチされたポリシーはリソースベースのポリシーと呼ばれます。Route 53 では、ID ベースのポリシー (IAM ポリシー) のみサポートされます。

トピック

- アイデンティティベースのポリシー (IAM ポリシー)
- リソースベースのポリシー

アイデンティティベースのポリシー (IAM ポリシー)

ポリシーを IAM アイデンティティにアタッチできます。例えば、次の操作を実行できます。

- アカウントのユーザーまたはグループにアクセス許可ポリシーをアタッチする – アカウント管理者は、特定のユーザーに関連付けられるアクセス許可ポリシーを使用して、そのユーザーに Amazon Route 53 リソースの作成を許可するアクセス許可を付与することができます。
- アクセス許可ポリシーをロールにアタッチする (クロスアカウントアクセス許可を付与する) – 別の AWS アカウントによって作成されたユーザーに Route 53 アクションを実行するアクセス許可を付与できます。そのためには、IAM ロールにアクセス許可ポリシーをアタッチし、他のアカウントのユーザーがそのロールを引き受けられるようにします。次の例では、これがアカウント A とアカウント B の 2 つの AWS アカウントでどのように機能するかを説明します。
  1. アカウント A の管理者は、IAM ロールを作成して、アカウント A が所有するリソースの作成や操作をするアクセス許可を付与するアクセス許可ポリシーをロールにアタッチします。
  2. アカウント A の管理者は、ロールに信頼ポリシーをアタッチします。信頼ポリシーは、ロールを引き受けることのできるプリンシパルとしてアカウント B を識別します。
  3. 次に、アカウント B の管理者は、ロールを引き受けるアクセス許可をアカウント B のユーザーまたはグループに委任できます。これにより、アカウント B のユーザーはアカウント A でリソースを作成したり、リソースにアクセスしたりできます。

  別の AWS アカウントのユーザーに権限を委任する方法の詳細については、IAM ユーザーガイドの「アクセス管理」を参照してください。

次のポリシー例では、ユーザーが CreateHostedZone アクションを実行し、 AWS アカウントのパブリックホストゾーンを作成できるようにします。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53:CreateHostedZone"
            ],
            "Resource":"*"
        }
    ]
}
```

プライベートホストゾーンにもポリシーを適用する場合、次の例に示すように、Route 53 AssociateVPCWithHostedZone アクションと 2 つの Amazon EC2 アクション (DescribeVpcs と DescribeRegion) を使用するためのアクセス許可を付与する必要があります。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53:CreateHostedZone",
                "route53:AssociateVPCWithHostedZone"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs",
                "ec2:DescribeRegions"
            ],
            "Resource": "*"
        }
    ]
}
```

Route 53 の ID へのポリシーのアタッチの詳細については、「Amazon Route 53 での ID ベースのポリシー (IAM ポリシー) の使用」を参照してください。ユーザー、グループ、ロール、アクセス権限の詳細については、「IAM ユーザーガイド」の「ID (ユーザー、グループ、ロール)」を参照してください。

リソースベースのポリシー

Amazon S3 などの他のサービスでは、リソースへのアクセス許可ポリシーのアタッチもサポートされています。例えば、ポリシーを S3 バケットにアタッチして、そのバケットに対するアクセス許可を管理できます。Amazon Route 53 では、リソースへのポリシーのアタッチはサポートされません。

ポリシー要素の指定: リソース、アクション、効果、プリンシパル

Amazon Route 53 には、各 Route 53 リソース (Amazon Route 53 リソースの ARN 参照) で使用できる API アクション (「Amazon Route 53 API リファレンス」参照) が含まれています。これらのアクションの一部またはすべてを実行するアクセス許可を、ユーザーまたはフェデレーティッドユーザーに付与できます。ドメインの登録など、一部の API アクションでは複数のアクションを実行する権限が必要な点に注意してください。

以下は、基本的なポリシーの要素です。

- リソース - Amazon リソースネーム (ARN) を使用して、ポリシーを適用するリソースを識別します。詳細については、「Amazon Route 53 リソースの ARN」を参照してください。
- アクション - アクションのキーワードを使用して、許可または拒否するリソースオペレーションを識別します。例えば、指定された `Effect` に応じて、`route53:CreateHostedZone` アクセス許可によって Route 53 `CreateHostedZone` アクションの実行がユーザーに許可または拒否されます。
- 効果 - ユーザーが指定されたリソースでアクションの実行を試みた場合の、許可または拒否の効果を指定します。アクションへのアクセスを明示的に許可していない場合、アクセスは暗黙的に拒否されます。また、明示的にリソースへのアクセスを拒否すると、別のポリシーによってアクセスが許可されている場合でも、ユーザーはそのリソースにアクセスできなくなります。
- プリンシパル - ID ベースのポリシー (IAM ポリシー) で、ポリシーがアタッチされているユーザーが黙示的なプリンシパルとなります。リソースベースのポリシーでは、権限 (リソースベースのポリシーにのみ適用) を受け取りたいユーザー、アカウント、サービス、またはその他のエンティティを指定します。Route 53 では、リソースベースのポリシー はサポートされていません。

IAM ポリシー構文の詳細と説明については、IAM ユーザーガイドのAWS IAM ポリシーリファレンスを参照してください。

適用する Route 53 API オペレーションやリソースがすべて表示されているのリストについては、「Amazon Route 53 API のアクセス許可: アクション、リソース、条件のリファレンス」を参照してください。

ポリシーでの条件を指定する

アクセス許可を付与するとき、IAM ポリシー言語を使用して、いつポリシーが有効になるかを指定できます。例えば、特定の日付の後にのみ適用されるポリシーが必要になる場合があります。ポリシー言語での条件の指定の詳細については、「IAM ユーザーガイド」の「IAM JSON ポリシー要素: Condition」を参照してください。

条件を表すには、あらかじめ定義された条件キーを使用します。Route 53 に固有の条件キーはありません。ただし、必要に応じて使用できる AWS 幅広い条件キーがあります。 AWS ワイドキーの完全なリストについては、IAM ユーザーガイドの「条件に使用可能なキー」を参照してください。

Amazon Route 53 での ID ベースのポリシー (IAM ポリシー) の使用

このトピックでは、アカウント管理者が IAM アイデンティティに許可ポリシーをアタッチし、そうすることによって Amazon Route 53 リソースで操作を実行する許可を付与する方法を示す、アイデンティティベースのポリシーの例を提供します。

> **Important**
>
> 初めに、Route 53 リソースへのアクセスを管理するための基本概念とオプションについて説明する概要トピックをお読みになることをお勧めします。詳細については、「Amazon Route 53 リソースに対するアクセス許可の管理の概要」を参照してください。

> **Note**
>
> アクセスを許可する場合、ホストゾーンと Amazon VPC は同じパーティションに属している必要があります。パーティションは のグループです AWS リージョン。各 AWS アカウント は 1 つのパーティションにスコープされます。
> サポートされているパーティションは以下のとおりです。
>
> - aws - AWS リージョン
> - aws-cn - 中国リージョン
> - aws-us-gov - AWS GovCloud (US) Region
>
> 詳細については、「AWS 一般参照」の「アクセス管理」と「Amazon Route 53 エンドポイントとクォータ」を参照してください。

トピック

- Amazon Route 53 コンソールを使用するために必要なアクセス許可
- ドメインレコード所有者のアクセス許可の例
- DNSSEC 署名に必要な Route 53 カスタマー管理キーアクセス許可

- カスタマーマネージドポリシーの例

以下の例に示しているのは、アクセス許可ポリシーです。Sid (ステートメント ID) はオプションです。

JSON

```
{
    "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": "*"
        }
```

```
    ]
}
```

ポリシーには、2 つのステートメントが含まれています。

- 最初のステートメントでは、パブリックホストゾーンとそのレコードの作成と管理に必要なアクションに対する権限が付与されます。Amazon リソースネーム (ARN) のワイルドカード文字 (*) は、現在の AWS アカウントが所有するすべてのホストゾーンへのアクセスを許可します。
- 2 番目のステートメントでは、ヘルスチェックの作成と管理に必要なすべてのアクションに対する権限が付与されます。

各アクションを使用するアクセス許可を付与または拒否するために指定するアクションおよび ARN のリストについては、「Amazon Route 53 API のアクセス許可: アクション、リソース、条件のリファレンス」を参照してください。

Amazon Route 53 コンソールを使用するために必要なアクセス許可

Amazon Route 53 コンソールへのフルアクセスを許可するには、次のアクセス許可ポリシーでアクセス許可を付与します。

JSON

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Effect":"Allow",
            "Action":[
                "route53:*",
                "route53domains:*",
                "tag:*",
                "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"
        }
    ]
}
```

アクセス許可が必要な理由は次のとおりです。

route53:*

以下を除くすべての Route 53 アクションを実行できます。

- [エイリアス先] の値が CloudFront ディストリビューション、Elastic Load Balancing ロードバランサー、Elastic Beanstalk 環境、または Amazon S3 バケットであるエイリアスレコードを作成および更新する。(これらの権限があると、[Alias Target] (エイリアス先) の値が同じホストゾーン内の別のレコードであるエイリアスレコードを作成できます)
- プライベートホストゾーンを操作する。

- ドメインを操作する。
- CloudWatch アラームを作成、削除、および表示する。
- Route 53 コンソールで CloudWatch メトリクスをレンダリングします。

`route53domains:*`

ドメインの操作を許可します。

> **Important**
>
> `route53` のアクションを個別にリストする場合は、`route53:CreateHostedZone` を含めてドメインを操作する必要があります。ドメインを登録すると同時にホストゾーンも作成されるため、ドメインを登録する権限を含むポリシーにはホストゾーンを作成する権限も必要です

(ドメイン登録について、Route 53 は個別のリソースへのアクセス許可の付与または拒否をサポートしていません)。

`route53resolver:*`

Route 53 VPC Resolver を操作できます。

`ssm:GetParametersByPath`

新しいエイリアスレコード、プライベートホストゾーン、ヘルスチェックを作成するときに、公開されているリージョンを取得できます。

`cloudfront:ListDistributions`

[Alias Target] (エイリアス先) の値が CloudFront ディストリビューションとなるエイリアスレコードを作成および更新できます。

Route 53 コンソールを使用していない場合、これらのアクセス許可は必要ありません。Route 53 は、ディストリビューションのリストを取得してコンソールに表示する場合のみ、これを使用します。

`elasticloadbalancing:DescribeLoadBalancers`

[Alias Target(エイリアス先)] の値が ELB ロードバランサーとなるエイリアスレコードを作成および更新できます。

Route 53 コンソールを使用していない場合、これらのアクセス許可は必要ありません。Route 53 は、ロードバランサーのリストを取得してコンソールに表示する場合のみ、これを使用します。

elasticbeanstalk:DescribeEnvironments

[Alias Target] (エイリアス先) の値が Elastic Beanstalk 環境となるエイリアスレコードを作成および更新できます。

Route 53 コンソールを使用していない場合、これらのアクセス許可は必要ありません。Route 53 は、環境のリストを取得してコンソールに表示する場合のみ、これを使用します。

s3:ListAllMyBuckets、**s3:GetBucketLocation**、および **s3:GetBucketWebsite**

[Alias Target] (エイリアス先) の値が Amazon S3 バケットとなるエイリアスレコードを作成および更新できます。(Amazon S3 バケットのエイリアスは、バケットがウェブサイトエンドポイントとして設定されている場合のみ作成できます。`s3:GetBucketWebsite` は必要な設定情報を取得します)。

Route 53 コンソールを使用していない場合、これらのアクセス許可は必要ありません。Route 53 は、バケットのリストを取得してコンソールに表示する場合のみ、これを使用します。

ec2:DescribeVpcs: 、および **ec2:DescribeRegions**

プライベートホストゾーンの操作を許可します。

すべてのリストされている **ec2** アクセス許可

Route 53 VPC Resolver を操作できます。

sns:ListTopics, **sns:ListSubscriptionsByTopic**, **sns:CreateTopic**, **cloudwatch:DescribeAlarms**, **cloudwatch:PutMetricAlarm**, **cloudwatch:DeleteAlarms**

CloudWatch アラームを作成、削除、および表示できます。

cloudwatch:GetMetricStatistics

CloudWatch メトリクスヘルスチェックを作成することができます。

Route 53 コンソールを使用していない場合、これらのアクセス許可は必要ありません。Route 53 は、統計を取得してコンソールに表示する場合のみ、これを使用します。

apigateway:GET

[エイリアス先] の値が Amazon API Gateway の API であるエイリアスレコードを作成および更新できます。

Route 53 コンソールを使用していない場合、このアクセス許可は必要ありません。Route 53 は、API のリストを取得してコンソールに表示する場合のみ、これを使用します。

`kms:*`

を使用して DNSSEC 署名 AWS KMS を有効にできます。

ドメインレコード所有者のアクセス許可の例

リソースレコードセットのアクセス許可を使用すると、 AWS ユーザーが更新または変更できる内容を制限する詳細なアクセス許可を設定できます。詳細については、「詳細に設定されたアクセスコントロールのための IAM ポリシー条件の使用」を参照してください。

場合によっては、ホストゾーンの所有者がホストゾーンの全体的な管理を担当し、組織内の別のユーザーがそれらのタスクのサブセットを担当することがあります。例えば、DNSSEC 署名を有効にしたホストゾーンの所有者は、他のユーザーがホストゾーンの Resource Set Records (RR) を追加および削除するためのアクセス許可などを含む IAM ポリシーを作成したい場合があります。ホストゾーン所有者がレコード所有者または他のユーザーに対して有効にする特定のアクセス許可は、組織のポリシーによって異なります。

以下は、レコード所有者に RR、トラフィックポリシー、ヘルスチェックの変更を許可する IAM ポリシーの例です。このポリシーを持つレコード所有者は、ゾーンの作成と削除、クエリログの有効化または無効化、再利用可能な委任セットの作成と削除、DNSSEC 設定の変更など、ゾーンレベルの操作を実行できません。

```
{
      "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 署名に必要な Route 53 カスタマー管理キーアクセス許可

Route 53 の DNSSEC 署名を有効にすると、Route 53 は AWS Key Management Service () のカスタマーマネージドキーに基づいてキー署名キー (KSK) を作成しますAWS KMS。DNSSEC 署名をサポートしている既存のカスタマー管理キーを使用することも、新しいカスタマー管理キーを作成することもできます。Route 53 は、KSK を作成できるようにカスタマー管理キーにアクセスするアクセス許可を持っている必要があります。

Route 53 がカスタマー管理キーにアクセスできるようにするには、カスタマー管理キーポリシーに次のステートメントが含まれていることを確認します。

```
{
            "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
                }
            }
        }
```

混乱した使節の問題は、アクションを実行するためのアクセス許可を持たないエンティティが、自分より特権があるエンティティにアクションの実行を強制できてしまう状況が発生するセキュリティ上の問題です。 AWS KMS から保護するには、オプションで、 aws:SourceAccount と aws:SourceArn条件 (両方または 1 つ) の組み合わせを指定することで、サービスがリソースベースのポリシーで持つアクセス許可をリソースに制限できます。 aws:SourceAccountはホストゾーンの所有者の AWS アカウント ID です。 はホストゾーンの ARN aws:SourceArnです。

以下の内容は追加できる許可の例を 2 つ示したものです:

```
{
    "Sid": "Allow Route 53 DNSSEC Service",
    …
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "111122223333"
        },
        "ArnEquals": {
            "aws:SourceArn": "arn:aws:route53:::hostedzone/HOSTED_ZONE_ID"
        }
    }
},
```

- または -

```
{
    "Sid": "Allow Route 53 DNSSEC Service",
    …
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": ["1111-2222-3333","4444-5555-6666"]
        },
        "ArnLike": {
            "aws:SourceArn": "arn:aws:route53:::hostedzone/*"
        }
    }
},
```

詳細については、IAM ユーザーガイド の 混乱した代理問題 を参照してください。

カスタマーマネージドポリシーの例

独自のカスタム IAM ポリシーを作成して、Route 53 アクションにアクセス許可を付与することもできます。これらのカスタムポリシーは、指定された許可を必要とする IAM グループにアタッチできます。これらのポリシーは、Route 53 API、 AWS SDKs、または AWS CLI を使用している場合に機能します。次の例では、いくつかの一般的ユースケースのアクセス許可を示します。Route 53 へのフルアクセスをユーザーに許可するポリシーについては、「Amazon Route 53 コンソールを使用するために必要なアクセス許可」を参照してください。

例

- 例 1: すべてのホストゾーンへの読み取りアクセスを許可する
- 例 2: ホストゾーンの作成と削除を許可する
- 例 3: すべてのドメインに対するフルアクセスを許可する (パブリックホストゾーンのみ)
- 例 4: インバウンドおよびアウトバウンドの Route 53 VPC Resolver エンドポイントの作成を許可する

例 1: すべてのホストゾーンへの読み取りアクセスを許可する

以下の権限ポリシーは、すべてのホストゾーンをリストし、ホストゾーン内のすべてのレコードを表示するユーザー権限を付与します。

JSON

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Effect":"Allow",
            "Action":[
                "route53:GetHostedZone",
                "route53:ListResourceRecordSets"
            ],
            "Resource":"*"
        },
        {
            "Effect":"Allow",
            "Action":["route53:ListHostedZones"],
            "Resource":"*"
        }
```

```
    ]
}
```

例 2: ホストゾーンの作成と削除を許可する

次の権限ポリシーは、ホストゾーンの作成と削除、および変更の進行状況の追跡をユーザーに許可します。

JSON

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Effect":"Allow",
            "Action":["route53:CreateHostedZone"],
            "Resource":"*"
        },
        {
            "Effect":"Allow",
            "Action":["route53:DeleteHostedZone"],
            "Resource":"*"
        },
        {
            "Effect":"Allow",
            "Action":["route53:GetChange"],
            "Resource":"*"
        }
    ]
}
```

例 3: すべてのドメインに対するフルアクセスを許可する (パブリックホストゾーンのみ)

次の権限ポリシーは、ドメインの登録権限やホストゾーンの作成権限など、ドメイン登録に関するすべてのアクションの実行をユーザーに許可します。

JSON

```
{
```

```
    "Version":"2012-10-17",
    "Statement":[
        {
            "Effect":"Allow",
            "Action":[
                "route53domains:*",
                "route53:CreateHostedZone"
            ],
            "Resource":"*"
        }
    ]
}
```

ドメインを登録すると同時にホストゾーンも作成されるため、ドメインを登録する権限を含むポリシーにはホストゾーンを作成する権限も必要です (ドメイン登録について、Route 53 は個別のリソースへのアクセス許可の付与をサポートしていません)。

プライベートホストゾーンを操作するために必要なアクセス許可については、「Amazon Route 53 コンソールを使用するために必要なアクセス許可」を参照してください。

例 4: インバウンドおよびアウトバウンドの Route 53 VPC Resolver エンドポイントの作成を許可する

次のアクセス許可ポリシーは、ユーザーが Route 53 コンソールを使用して Resolver のインバウンドおよびアウトバウンドエンドポイントを作成することを許可します。

これらのアクセス許可の一部は、コンソールでエンドポイントを作成するためにのみ必要です。インバウンドおよびアウトバウンドエンドポイントのみをプログラムで作成するアクセス許可を付与する場合は、これらのアクセス許可を省略できます。

- `route53resolver:ListResolverEndpoints` では、インバウンドまたはアウトバウンドエンドポイントのリストが表示されるため、ユーザーはエンドポイントが作成されたことを確認できます。
- `DescribeAvailabilityZones` は、アベイラビリティーゾーンのリストを表示するために必要です。
- `DescribeVpcs` は VPC のリストを表示するために必要です。

JSON

```
{
    "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": "*"
        }
    ]
}
```

のサービスにリンクされたロールの使用 Amazon Route 53 Resolver

Route 53 VPC Resolver は AWS Identity and Access Management (IAM) サービスにリンクされたロールを使用します。サービスにリンクされたロールは、VPC Resolver に直接リンクされた一意のタイプの IAM ロールです。サービスにリンクされたロールは VPC Resolver によって事前定義されており、サービスがユーザーに代わって他の AWS サービスを呼び出すために必要なすべてのアクセス許可が含まれています。

サービスにリンクされたロールを使用すると、必要なアクセス許可を手動で追加する必要がなくなるため、VPC リゾルバーの設定が簡単になります。VPC Resolver は、サービスにリンクされたロールのアクセス許可を定義します。特に定義されている場合を除き、VPC Resolver のみがそのロールを引き受けることができます。定義される許可には、信頼ポリシーと許可ポリシーが含まれており、その許可ポリシーを他のIAM エンティティに添付することはできません。

サービスにリンクされたロールを削除するには、まずその関連リソースを削除します。これにより、VPC Resolver リソースへのアクセス許可が誤って削除されないため、VPC Resolver リソースが保護されます。

サービスにリンクされたロールをサポートする他のサービスについては、「IAM と連携するAWS のサービス」を参照して、サービスにリンクされたロール列がはいになっているサービスを探してください。サービスにリンクされた役割に関するドキュメントをサービスで表示するには[はい] リンクを選択してください。

トピック

- VPC リゾルバーのサービスにリンクされたロールのアクセス許可
- VPC リゾルバーのサービスにリンクされたロールの作成
- VPC リゾルバーのサービスにリンクされたロールの編集
- VPC リゾルバーのサービスにリンクされたロールの削除
- VPC Resolver のサービスにリンクされたロールでサポートされているリージョン

VPC リゾルバーのサービスにリンクされたロールのアクセス許可

VPC Resolver は、**AWSServiceRoleForRoute53Resolver**サービスにリンクされたロールを使用して、ユーザーに代わってクエリログを配信します。

ロールのアクセス許可ポリシーにより、VPC Resolver はリソースに対して次のアクションを実行できます。

JSON

```
{
  "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": "*"
```

```
    }
  ]
}
```

サービスリンクロールの作成、編集、削除を IAM エンティティ (ユーザー、グループ、ロールなど) に許可するにはアクセス許可を設定する必要があります。詳細については、「IAM ユーザーガイド」の「サービスリンクロールの許可」を参照してください。

VPC リゾルバーのサービスにリンクされたロールの作成

サービスリンクロールを手動で作成する必要はありません。Amazon Route 53 コンソール、、 AWS CLIまたは AWS API でリゾルバークエリログ設定の関連付けを作成すると、VPC Resolver によってサービスにリンクされたロールが作成されます。

> **Important**
>
> このサービスリンクロールはこのロールでサポートされている機能を使用する別のサービスでアクションが完了した場合にアカウントに表示されます。また、サービスにリンクされたロールのサポートを開始した 2020 年 8 月 12 日より前に VPC Resolver サービスを使用している場合、VPC Resolver はアカウントに`AWSServiceRoleForRoute53Resolver`ロールを作成しました。詳細については、「IAM アカウントに新しいロールが表示される」を参照してください。

このサービスリンクロールを削除した後で再度作成する必要が生じた場合は、同じ手順でアカウントにロールを再作成できます。新しい Resolver クエリログ設定の関連付けを作成すると、`AWSServiceRoleForRoute53Resolver` というサービスにリンクされたロールが再度作成されます。

VPC リゾルバーのサービスにリンクされたロールの編集

VPC Resolver では、`AWSServiceRoleForRoute53Resolver`サービスにリンクされたロールを編集することはできません。サービスリンクロールの作成後は、さまざまなエンティティがロールを参照する可能性があるため、ロール名を変更することはできません。ただし、IAM を使用してロールの説明を編集することはできます。詳細については、「IAM ユーザーガイド」の「サービスリンクロールの編集」を参照してください。

VPC リゾルバーのサービスにリンクされたロールの削除

サービスリンクロールを必要とする機能やサービスが不要になった場合は、ロールを削除することをお勧めします。そうすることで、積極的にモニタリングまたは保守されていない未使用のエンティティを排除できます。ただし、手動で削除する前に、サービスリンクロールのリソースをクリーンアップする必要があります。

> **Note**
>
> リソースを削除しようとしたときに VPC Resolver サービスがロールを使用している場合、削除が失敗する可能性があります。失敗した場合は数分待ってから操作を再試行してください。

で使用される VPC Resolver リソースを削除するには **`AWSServiceRoleForRoute53Resolver`**

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. Route 53 コンソールのメニューを展開します。コンソールの左上隅にある 3 本の水平バー (☰) アイコンを選択します。
3. Resolver メニューから、[Query logging (クエリログ記録)] を選択します。
4. クエリログ設定の名前の横にあるチェックボックスをオンにし、[Delete (削除)]を選択します。
5. [Delete query logging configuration (クエリログ記録設定を削除)] テキストボックスで [Stop logging queries (クエリログ記録を停止)] を選択します。

   これにより、VPC から設定の関連付けが解除されます。また、クエリログ設定の関連付けをプログラムで解除することもできます。詳細については、「disassociate-resolver-query-log-config」を参照してください。
6. クエリのログ記録が停止した後、オプションでフィールドに **`delete`** を入力し、[Delete (削除)] を選択してクエリログ設定を削除できます。ただし、`AWSServiceRoleForRoute53Resolver` で使用されるリソースを削除する場合、これは必要ありません。

サービスリンクロールを IAM で手動削除するには

IAM コンソール、 AWS CLI、または AWS API を使用して、AWSServiceRoleForRoute53Resolverサービスにリンクされたロールを削除します。詳細については、「IAM ユーザーガイド」の「サービスリンクロールの削除」を参照してください。

VPC Resolver のサービスにリンクされたロールでサポートされているリージョン

VPC Resolver は、サービスが利用可能なすべてのリージョンでサービスにリンクされたロールの使用をサポートしているわけではありません。以下のリージョンでは、AWSServiceRoleForRoute53Resolver ロールを使用できます。

リージョン名	リージョン識別子	VPC Resolver でのサポート
米国東部 (バージニア北部)	us-east-1	はい
米国東部 (オハイオ)	us-east-2	はい
米国西部 (北カリフォルニア)	us-west-1	はい
米国西部 (オレゴン)	us-west-2	はい
アジアパシフィック (ムンバイ)	ap-south-1	はい
アジアパシフィック (大阪)	ap-northeast-3	はい
アジアパシフィック (ソウル)	ap-northeast-2	はい
アジアパシフィック (シンガポール)	ap-southeast-1	はい
アジアパシフィック (シドニー)	ap-southeast-2	はい
アジアパシフィック (東京)	ap-northeast-1	はい
カナダ (中部)	ca-central-1	はい
欧州 (フランクフルト)	eu-central-1	はい
欧州 (アイルランド)	eu-west-1	はい
欧州 (ロンドン)	eu-west-2	はい

リージョン名	リージョン識別子	VPC Resolver でのサポート
欧州 (パリ)	eu-west-3	はい
南米 (サンパウロ)	sa-east-1	はい
中国 (北京)	cn-north-1	はい
中国 (寧夏)	cn-northwest-1	はい
AWS GovCloud (US)	us-gov-east-1	はい
AWS GovCloud (US)	us-gov-west-1	はい

AWS Amazon Route 53 の マネージドポリシー

AWS 管理ポリシーは、 によって作成および管理されるスタンドアロンポリシーです AWS。 AWS 管理ポリシーは、多くの一般的なユースケースにアクセス許可を付与するように設計されているため、ユーザー、グループ、ロールにアクセス許可の割り当てを開始できます。

AWS 管理ポリシーは、すべての AWS お客様が使用できるため、特定のユースケースに対して最小特権のアクセス許可を付与しない場合があることに注意してください。ユースケースに固有のカスタマー管理ポリシーを定義して、アクセス許可を絞り込むことをお勧めします。

AWS 管理ポリシーで定義されているアクセス許可は変更できません。が AWS 管理ポリシーで定義されたアクセス許可 AWS を更新すると、ポリシーがアタッチされているすべてのプリンシパル ID (ユーザー、グループ、ロール) に影響します。 AWS は、新しい が起動されるか、新しい API オペレーション AWS のサービス が既存のサービスで使用できるようになったときに、 AWS 管理ポリシーを更新する可能性が高くなります。

詳細については、「IAM ユーザーガイド」の「AWS マネージドポリシー」を参照してください。

AWS マネージドポリシー: AmazonRoute53FullAccess

`AmazonRoute53FullAccess` ポリシーは IAM アイデンティティにアタッチできます。

このポリシーは、ドメイン登録やヘルスチェックなど、Route 53 リソースへのフルアクセスを許可しますが、VPC Resolver は除きます。

アクセス許可の詳細

このポリシーには以下のアクセス許可が含まれています。

- `route53:*` - 以下を除くすべての Route 53 アクションを実行できます。
  - [エイリアス先] の値が CloudFront ディストリビューション、Elastic Load Balancing ロードバランサー、Elastic Beanstalk 環境、または Amazon S3 バケットであるエイリアスレコードを作成および更新する。(これらの権限があると、[Alias Target] (エイリアス先) の値が同じホストゾーン内の別のレコードであるエイリアスレコードを作成できます)
  - プライベートホストゾーンを操作する。
  - ドメインを操作する。
  - CloudWatch アラームを作成、削除、および表示する。
  - Route 53 コンソールで CloudWatch メトリクスをレンダリングします。
- `route53domains:*` - ドメインの操作を行うことができます。
- `cloudfront:ListDistributions` - [Alias Target (エイリアス先)] の値が CloudFront ディストリビューションであるエイリアスレコードを作成および更新できます。

  Route 53 コンソールを使用していない場合、このアクセス許可は必要ありません。Route 53 は、ディストリビューションのリストを取得してコンソールに表示する場合のみ、これを使用します。
- `cloudfront:GetDistributionTenantByDomain` – CloudFront マルチテナントディストリビューションを取得して、エイリアスターゲットの値が CloudFront ディストリビューションテナントであるエイリアスレコードを作成および更新するために使用されます。
- `cloudfront:GetConnectionGroup` – CloudFront マルチテナントディストリビューションを取得して、エイリアスターゲットの値が CloudFront ディストリビューションテナントであるエイリアスレコードを作成および更新するために使用されます。
- `cloudwatch:DescribeAlarms` – `sns:ListTopics` および `sns:ListSubscriptionsByTopic` と併用して、CloudWatch アラームを作成、削除、表示できます。
- `cloudwatch:GetMetricStatistics` - CloudWatch メトリクスヘルスチェックを作成することができます。

  Route 53 コンソールを使用していない場合、これらのアクセス許可は必要ありません。Route 53 は、統計を取得してコンソールに表示する場合のみ、これを使用します。
- `cloudwatch:GetMetricData` – CloudWatch ヘルスチェックメトリクスのステータスを表示できます。

- `ec2:DescribeVpcs` — VPC のリストを表示できます。
- `ec2:DescribeVpcEndpoints` — VPC エンドポイントのリストを表示できます。
- `ec2:DescribeRegions` — アベイラビリティーゾーンのリストを表示できます。
- `elasticloadbalancing:DescribeLoadBalancers` - [Alias Target (エイリアス先)] の値が Elastic Load Balancing となるエイリアスレコードを作成および更新できます。

  Route 53 コンソールを使用していない場合、これらのアクセス許可は必要ありません。Route 53 は、ロードバランサーのリストを取得してコンソールに表示する場合のみ、これを使用します。
- `elasticbeanstalk:DescribeEnvironments` - [Alias Target (エイリアス先)] の値が Elastic Beanstalk 環境となるエイリアスレコードを作成および更新できます。

  Route 53 コンソールを使用していない場合、これらのアクセス許可は必要ありません。Route 53 は、環境のリストを取得してコンソールに表示する場合のみ、これを使用します。
- `es:ListDomainNames` – アクティブリージョン内で現在のユーザーが所有するすべての Amazon OpenSearch Service ドメイン名を表示できます。
- `es:DescribeDomains` – 指定された Amazon OpenSearch Service ドメインのドメイン設定を取得できます。
- `lightsail:GetContainerServices` – Lightsail コンテナサービスを使用して、エイリアスターゲットの値が Lightsail ドメインであるエイリアスレコードを作成および更新できます。
- `s3:ListBucket`、`s3:GetBucketLocation`、`s3:GetBucketWebsite` - [Alias Target] (エイリアスのターゲット) の値が Amazon S3 バケットとなるエイリアスレコードを作成および更新できます。(Amazon S3 バケットのエイリアスは、バケットがウェブサイトエンドポイントとして設定されている場合のみ作成できます。`s3:GetBucketWebsite` は必要な設定情報を取得します)。

  Route 53 コンソールを使用していない場合、これらのアクセス許可は必要ありません。Route 53 は、バケットのリストを取得してコンソールに表示する場合のみ、これを使用します。
- `sns:ListTopics`、`sns:ListSubscriptionsByTopic`、`cloudwatch:DescribeAlarms` – CloudWatch アラームを作成、削除、表示できます。
- `tag:GetResources` – リソース内のタグを表示できます。例えば、ヘルスチェックの名前などです。
- `apigateway:GET` - [Alias Target (エイリアス先)] の値が Amazon API Gateway のAPI であるエイリアスレコードを作成および更新できます。

アクセス許可の詳細については、「Amazon Route 53 API のアクセス許可: アクション、リソース、条件のリファレンス」を参照してください。

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "route53:*",
    "route53domains:*",
    "cloudfront:ListDistributions",
    "cloudfront:GetDistributionTenantByDomain",
    "cloudfront:GetConnectionGroup",
    "cloudwatch:DescribeAlarms",
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:GetMetricData",
    "ec2:DescribeVpcs",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeRegions",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticbeanstalk:DescribeEnvironments",
    "es:ListDomainNames",
    "es:DescribeDomains",
    "lightsail:GetContainerServices",
    "s3:ListBucket",
    "s3:GetBucketLocation",
    "s3:GetBucketWebsite",
    "sns:ListTopics",
    "sns:ListSubscriptionsByTopic",
    "tag:GetResources"
   ],
   "Resource": "*"
  },
  {
   "Effect": "Allow",
   "Action": "apigateway:GET",
   "Resource": "arn:aws:apigateway:*::/domainnames"
  }
 ]
}
```

AWS マネージドポリシー: AmazonRoute53ReadOnlyAccess

`AmazonRoute53ReadOnlyAccess` ポリシーは IAM アイデンティティにアタッチできます。

このポリシーは、ドメイン登録やヘルスチェックなど、Route 53 リソースへの読み取り専用アクセスを許可しますが、VPC Resolver は除きます。

アクセス許可の詳細

このポリシーには以下のアクセス許可が含まれています。

- `route53:Get*` — Route 53 リソースを取得します。
- `route53:List*` - Route 53 リソースを一覧表示します。
- `route53:TestDNSAnswer` — DNS リクエストに応答して Route 53 が返す値を取得します。

アクセス許可の詳細については、「Amazon Route 53 API のアクセス許可: アクション、リソース、条件のリファレンス」を参照してください。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53:Get*",
                "route53:List*",
                "route53:TestDNSAnswer"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWS マネージドポリシー: AmazonRoute53DomainsFullAccess

`AmazonRoute53DomainsFullAccess` ポリシーは IAM アイデンティティにアタッチできます。

このポリシーは、Route 53 ドメイン登録リソースへのフルアクセスを付与します。

アクセス許可の詳細

このポリシーには以下のアクセス許可が含まれています。

- `route53:CreateHostedZone` — Route 53 ホストゾーンを作成できます。
- `route53domains:*` — ドメイン名を登録し、関連する操作を実行できます。

アクセス許可の詳細については、「Amazon Route 53 API のアクセス許可: アクション、リソース、条件のリファレンス」を参照してください。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53:CreateHostedZone",
                "route53domains:*"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWS マネージドポリシー: AmazonRoute53DomainsReadOnlyAccess

`AmazonRoute53DomainsReadOnlyAccess` ポリシーは IAM アイデンティティにアタッチできます。

このポリシーは、Route 53 ドメイン登録リソースへの読み取り専用アクセスを付与します。

アクセス許可の詳細

このポリシーには以下のアクセス許可が含まれています。

- `route53domains:Get*` — Route 53 からドメインのリストを取得できます。
- `route53domains:List*` — Route 53 ドメインのリストを表示できます。

アクセス許可の詳細については、「Amazon Route 53 API のアクセス許可: アクション、リソース、条件のリファレンス」を参照してください。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53domains:Get*",
                "route53domains:List*"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWS マネージドポリシー: AmazonRoute53ResolverFullAccess

`AmazonRoute53ResolverFullAccess` ポリシーは IAM アイデンティティにアタッチできます。

このポリシーは、Route 53 VPC Resolver リソースへのフルアクセスを許可します。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- `route53resolver:*` – Route 53 コンソールで VPC Resolver リソースを作成および管理できます。
- `ec2:DescribeSubnets` — Amazon VPC サブネットを一覧表示できVます。
- `ec2:CreateNetworkInterface`、`ec2:DeleteNetworkInterface`、`ec2:ModifyNetworkInterf` — ネットワークインターフェイスを作成、変更、削除できます。

- ec2:DescribeNetworkInterfaces — ネットワークインターフェイスのリストを表示します。
- ec2:DescribeSecurityGroups — すべてのセキュリティグループのリストを表示できます。
- ec2:DescribeVpcs — VPC のリストを表示できます。
- ec2:DescribeAvailabilityZones — 使用可能なゾーンを一覧表示します。

アクセス許可の詳細については、「Amazon Route 53 API のアクセス許可: アクション、リソース、条件のリファレンス」を参照してください。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AmazonRoute53ResolverFullAccess",
            "Effect": "Allow",
            "Action": [
                "route53resolver:*",
                "ec2:DescribeSubnets",
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeVpcs",
                "ec2:DescribeAvailabilityZones"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWS マネージドポリシー: AmazonRoute53ResolverReadOnlyAccess

AmazonRoute53ResolverReadOnlyAccess ポリシーは IAM アイデンティティにアタッチできます。

このポリシーは、Route 53 VPC Resolver リソースへの読み取り専用アクセスを許可します。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- `route53resolver:Get*` – VPC Resolver リソースを取得します。
- `route53resolver:List*` – VPC Resolver リソースのリストを表示できます。
- `ec2:DescribeNetworkInterfaces` — ネットワークインターフェイスのリストを表示します。
- `ec2:DescribeSecurityGroups` — すべてのセキュリティグループのリストを表示できます。

アクセス許可の詳細については、「Amazon Route 53 API のアクセス許可: アクション、リソース、条件のリファレンス」を参照してください。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AmazonRoute53ResolverReadOnlyAccess",
            "Effect": "Allow",
            "Action": [
                "route53resolver:Get*",
                "route53resolver:List*",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWS マネージドポリシー: Route53ResolverServiceRolePolicy

IAM エンティティに `Route53ResolverServiceRolePolicy` をアタッチすることはできません。このポリシーは、Route 53 VPC Resolver が VPC Resolver によって使用または管理されるサービスとリソースにアクセス AWS できるようにするサービスにリンクされたロールにアタッチされます。詳細については、「のサービスにリンクされたロールの使用 Amazon Route 53 Resolver」を参照してください。

AWS マネージドポリシー: AmazonRoute53ProfilesFullAccess

`AmazonRoute53ProfilesReadOnlyAccess` ポリシーを IAM アイデンティティにアタッチできます。

このポリシーは、Amazon Route 53 プロファイルリソースへのフルアクセス権を付与します。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- `route53profiles` — Route 53 コンソールでプロファイルリソースを作成および管理できます。
- `ec2` – プリンシパルが VPC に関する情報を取得するのを許可します。

アクセス許可の詳細については、「Amazon Route 53 API のアクセス許可: アクション、リソース、条件のリファレンス」を参照してください。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AmazonRoute53ProfilesFullAccess",
            "Effect": "Allow",
            "Action": [
                "route53profiles:AssociateProfile",
                "route53profiles:AssociateResourceToProfile",
                "route53profiles:CreateProfile",
                "route53profiles:DeleteProfile",
                "route53profiles:DisassociateProfile",
                "route53profiles:DisassociateResourceFromProfile",
```

```
                "route53profiles:UpdateProfileResourceAssociation",
                "route53profiles:GetProfile",
                "route53profiles:GetProfileAssociation",
                "route53profiles:GetProfileResourceAssociation",
                "route53profiles:GetProfilePolicy",
                "route53profiles:ListProfileAssociations",
                "route53profiles:ListProfileResourceAssociations",
                "route53profiles:ListProfiles",
                "route53profiles:PutProfilePolicy",
                "route53profiles:ListTagsForResource",
                "route53profiles:TagResource",
                "route53profiles:UntagResource",
                "route53resolver:GetFirewallConfig",
                "route53resolver:GetFirewallRuleGroup",
                "route53resolver:GetResolverConfig",
                "route53resolver:GetResolverDnssecConfig",
                "route53resolver:GetResolverQueryLogConfig",
                "route53resolver:GetResolverRule",
                "ec2:DescribeVpcs",
                "route53:GetHostedZone"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWS マネージドポリシー: AmazonRoute53ProfilesReadOnlyAccess

`AmazonRoute53ProfilesReadOnlyAccess` ポリシーを IAM アイデンティティにアタッチできます。

このポリシーは、すべての Amazon Route 53 プロファイルリソースへの読み取り専用アクセス権を付与します。

アクセス許可の詳細

アクセス許可の詳細については、「Amazon Route 53 API のアクセス許可: アクション、リソース、条件のリファレンス」を参照してください。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AmazonRoute53ProfilesReadOnlyAccess",
            "Effect": "Allow",
            "Action": [
                "route53profiles:GetProfile",
                "route53profiles:GetProfileAssociation",
                "route53profiles:GetProfileResourceAssociation",
                "route53profiles:GetProfilePolicy",
                "route53profiles:ListProfileAssociations",
                "route53profiles:ListProfileResourceAssociations",
                "route53profiles:ListProfiles",
                "route53profiles:ListTagsForResource",
                "route53resolver:GetFirewallConfig",
                "route53resolver:GetResolverConfig",
                "route53resolver:GetResolverDnssecConfig",
                "route53resolver:GetResolverQueryLogConfig"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWS 管理ポリシーへの Route 53 の更新

このサービスがこれらの変更の追跡を開始してからの Route 53 の AWS マネージドポリシーの更新に関する詳細を表示します。このページの変更に関する自動通知については、Route 53 の [ドキュメントの履歴] ページの RSS フィードを購読してください。

マネージドポリシーの変更履歴

変更	説明	日付
AmazonRoute53FullAccess – 更新されたポリシー	`cloudwatch:GetMetricData` 、`tag:GetResources` 、`es:ListDomainNames` 、`es:DescribeDomains` 、`cloudfront:GetDistributionTenantByDomain` 、`cloudfront:GetConnectionGroup` 、`lightsail:GetContainerServices` のアクセス許可を追加します。これらのアクセス許可により、最大 500 個の CloudWatch ヘルスチェックメトリクス、最大 100 個のヘルスチェックの名前を取得し、指定された Amazon OpenSearch Service ドメインのドメイン設定を取得し、アクティブなリージョンの現在のユーザーが所有するすべての Amazon OpenSearch Service ドメインの名前を一覧表示し、CloudFront マルチテナントディストリビューションを取得し、Lightsailコンテナサービスを取得できます。	2025 年 6 月 1 日
AmazonRoute53ProfilesFullAccess – 更新されたポリシー	`GetProfilePolicy` と `PutProfilePolicy` のアクセス許可を追加します。これらはアクセス許可のみの IAM	2024 年 8 月 27 日

変更	説明	日付
	アクションです。IAM プリンシパルにこれらのアクセス許可が付与されていない場合、AWS RAM サービスを使用してプロファイルを共有しようとするとエラーが発生します。	
AmazonRoute53ProfilesReadOnlyAccess – 更新されたポリシー	`GetProfilePolicy` にアクセス許可を追加します。これはアクセス許可のみの IAM アクションです。IAM プリンシパルにこのアクセス許可が付与されていない場合、 AWS RAM サービスを使用してプロファイルのポリシーにアクセスしようとするとエラーが発生します。	2024 年 8 月 27 日
AmazonRoute53ResolverFullAccess – 更新されたポリシー	ポリシーを一意に識別するためのステートメント ID (Sid) を追加しました。	2024 年 8 月 5 日
AmazonRoute53ResolverReadOnlyAccess – 更新されたポリシー	ポリシーを一意に識別するためのステートメント ID (Sid) を追加しました。	2024 年 8 月 5 日
AmazonRoute53ProfilesFullAccess – 新しいポリシー	Amazon Route 53 は、Amazon Route 53 プロファイルリソースへのフルアクセスを許可する新しいポリシーを追加しました。	2024 年 4 月 22 日

変更	説明	日付
AmazonRoute53ProfilesReadOnlyAccess – 新しいポリシー	Amazon Route 53 は、Amazon Route 53 プロファイルリソースへの読み取り専用アクセスを許可する新しいポリシーを追加しました。	2024 年 4 月 22 日
Route53ResolverServiceRolePolicy – 新しいポリシー	Amazon Route 53 は、VPC Resolver が Resolver によって使用または管理される AWS サービスとリソースにアクセスできるようにするサービスにリンクされたロールにアタッチされた新しいポリシーを追加しました。	2021 年 7 月 14 日
AmazonRoute53ResolverReadOnlyAccess – 新しいポリシー	Amazon Route 53 は、VPC Resolver リソースへの読み取り専用アクセスを許可する新しいポリシーを追加しました。	2021 年 7 月 14 日
AmazonRoute53ResolverFullAccess – 新しいポリシー	Amazon Route 53 は、VPC Resolver リソースへのフルアクセスを許可する新しいポリシーを追加しました。	2021 年 7 月 14 日
AmazonRoute53DomainsReadOnlyAccess – 新しいポリシー	Amazon Route 53 は、Route 53 ドメインリソースへの読み取り専用アクセスを許可する新しいポリシーを追加しました。	2021 年 7 月 14 日

変更	説明	日付
AmazonRoute53DomainsFullAccess – 新しいポリシー	Amazon Route 53 は、Route 53 ドメインリソースへのフルアクセスを許可する新しいポリシーを追加しました。	2021 年 7 月 14 日
AmazonRoute53ReadOnlyAccess – 新しいポリシー	Amazon Route 53 は、Route 53 リソースへの読み取り専用アクセスを許可する新しいポリシーを追加しました。	2021 年 7 月 14 日
AmazonRoute53FullAccess – 新しいポリシー	Amazon Route 53 は、Route 53 リソースへのフルアクセスを許可する新しいポリシーを追加しました。	2021 年 7 月 14 日
Route 53 で、変更追跡のサポート開始	Route 53 は AWS 、管理ポリシーの変更の追跡を開始しました。	2021 年 7 月 14 日

詳細に設定されたアクセスコントロールのための IAM ポリシー条件の使用

Route 53 では、IAM ポリシーを使用してアクセス許可を付与するときに条件を指定できます (「アクセスコントロール」参照)。例えば、以下のことが可能です:

- 単一のリソースレコードセットへのアクセスを許可する。
- ホストゾーン内の特定の DNS レコードタイプ (A レコードや AAAA レコードなど) のすべてのリソースレコードセットへのアクセスを許可する。
- 名前に特定の文字列が含まれるリソースレコードセットへのアクセスをユーザーに許可する。
- Route 53 コンソール上で、あるいは ChangeResourceRecordSets API 使用時に、`CREATE | UPSERT | DELETE` アクションの一部のみの実行をユーザーに許可する。
- 特定の VPC からプライベートホストゾーンを関連付けたり、関連付けを解除できるアクセス許可をユーザーに付与します。

- 特定の VPC に関連付けられたホストゾーンを一覧表示できるアクセス許可をユーザーに付与します。
- 新しいプライベートホストゾーンを作成し、特定の VPC に関連付けることができるアクセス許可をユーザーに付与します。
- VPC 関連付け認可を作成または削除できるアクセス許可をユーザーに付与します。
- Route 53 プロファイルで特定のリソースタイプのみをユーザーが管理 (associate/disassociate/update) できるようにするアクセス許可を付与します。
- ユーザーが Route 53 プロファイルで特定のリソース ARNs のみを管理 (associate/disassociate/update) できるようにするアクセス許可を付与します。
- 特定のホストゾーンドメインのみを Route 53 プロファイルで管理 (associate/disassociate/update) できるようにするアクセス許可を付与します。
- 特定のリゾルバールールドメインのみを Route 53 プロファイルで管理 (associate/disassociate/update) することをユーザーに許可するアクセス許可を付与します。
- Route 53 プロファイル内の特定の優先度範囲のファイアウォールルールグループの管理 (associate/disassociate/update) をユーザーに許可するアクセス許可を付与します。
- Route 53 プロファイルを特定の VPCs。

また、任意のきめ細かなアクセス許可を組み合わせたアクセス許可を作成することもできます。

Route 53 コンディションキー値の正規化

ポリシー条件に入力する値は、次のようにフォーマット (正規化) する必要があります。

`route53:ChangeResourceRecordSetsNormalizedRecordNames` の場合

- すべての文字を小文字にする必要があります。
- DNS 名は末尾のドットなしにする必要があります。
- a ~ z、0 ~ 9、- (ハイフン)、_ (アンダースコア)、. (ラベル間の区切り文字としてのピリオド) 以外の文字は、\ に 3 桁の 8 進コードを続けた形式のエスケープコードを使用する必要があります。例えば、`\052` は文字 * の 8 進コードです。

`route53:ChangeResourceRecordSetsActions` では、値には次のいずれかを指定でき、大文字にする必要があります。

- CREATE

- UPSERT
- DELETE

route53:ChangeResourceRecordSetsRecordTypes の場合:

- 値は大文字である必要があり、Route 53 がサポートするどの DNS レコードタイプでもかまいません。詳細については、「サポートされる DNS レコードタイプ」を参照してください。

route53:VPCs の場合:

- 値は、VPCId=<vpc-id>,VPCRegion=<region> 形式である必要があります。
- <vpc-id> と <region> の値は、VPCId=vpc-123abc や VPCRegion=us-east-1 などの小文字にする必要があります。
- コンテキストキーと値では大文字と小文字が区別されます。

> **Important**
>
> アクセス許可で意図したとおりにアクションを許可または制限するには、次の規則に従う必要があります。この条件キーでは VPCId および VPCRegion要素のみが受け入れられ、 などの他の AWS リソース AWS アカウントはサポートされていません。

の場合**route53profiles:ResourceTypes**、値は次のいずれかであり、大文字と小文字が区別されます。

- HostedZone
- FirewallRuleGroup
- ResolverQueryLoggingConfig
- ResolverRule
- VPCEndpoint

route53profiles:ResourceArns の場合:

- 値は、 などの有効な AWS リソース ARN である必要がありますarn:aws:route53:::hostedzone/Z12345。

- ARN 値を比較するときは、 ArnEqualsまたは ArnLike条件演算子を使用します。

route53profiles:HostedZoneDomains の場合:

- 値は、 などの有効なドメイン名である必要がありますexample.com。
- ドメイン名には末尾のドットを含めないでください。
- これらの値は大文字と小文字が区別されます。

route53profiles:ResolverRuleDomains の場合:

- 値は、 などの有効なドメイン名である必要がありますexample.com。
- ドメイン名には末尾のドットを含めないでください。
- これらの値は大文字と小文字が区別されます。

route53profiles:FirewallRuleGroupPriority の場合:

- 値は、ファイアウォールルールグループの優先度を表す数値である必要があります。
- NumericEquals、、 などの数値条件演算子NumericLessThanEqualsを使用して、優先度値を比較したりNumericGreaterThanEquals、優先度範囲を定義したりできます。

route53profiles:ResourceIds の場合:

- 値は、 などの有効な VPC ID である必要がありますvpc-1a2b3c4d5e6f。
- これらの値は大文字と小文字が区別されます。

「IAM ユーザーガイド」の「Access Analyzer」または「Policy Simulator」を使用して、ポリシーで想定どおりにアクセス許可が付与または制限されていることを検証できます。IAM ポリシーをテストユーザーまたはロールに適用して Route 53 オペレーションを実行することで、アクセス許可を検証することもできます。

条件の指定: 条件キーの使用

AWS は、アクセスコントロールのために IAM をサポートするすべての AWS サービスに対して、事前定義された一連の条件キー (AWS全体の条件キー) を提供します。たとえば、aws:SourceIp 条件キーを使用して、リクエスタの IP アドレスを確認してから、アクションの実行を許可できます。

詳細について、および AWS全体を対象とするキーのリストについては、「IAM ユーザーガイド」の「Available Keys for Conditions」(条件に使用可能なキー) を参照してください。

> **Note**
>
> Route 53 では、タグベースの条件キーはサポートされていません。

以下の表では、Route 53 に適用される Route 53 サービス固有の条件キーを示しています。

Route 53 条件キー	API オペレーション	値の型	説明
`route53:ChangeResourceRecordSetsNormalizedRecordNames`	ChangeResourceRecordSets	複数値	ChangeResourceRecordSets のリクエストに含まれる DNS レコード名のリストを表します。想定どおりの動作を実現するには、IAM ポリシーの DNS 名を次のように正規化する必要があります。 • すべての文字を小文字にする必要があります。 • DNS 名は末尾のドットなしにする必要があります。 • a ~ z、0 ~ 9、- (ハイフン)、_ (アンダースコア)、. (ラベル間の区切り文字としてのピリオド) 以外の文字は、\ に 3 桁の 8 進コードを続けた形式のエスケープコードを使用する必要があります。
`route53:ChangeResourceRecordSetsRecordTypes`	ChangeResourceRecordSets	複数値	`ChangeResourceRecordSets` のリクエストに含まれる DNS レコードタイプのリストを表します。 `ChangeResourceRecordSetsRecordTypes` は、Route 53 でサポートされている DNS レコードタイプのどれでもかまいませ

Route 53 条件キー	API オペレーション	値の型	説明
			ん。詳細については、「サポートされる DNS レコードタイプ」を参照してください。ポリシーではすべて大文字で入力する必要があります。
route53:ChangeResourceRecordSetsActions	ChangeResourceRecordSets	複数値	ChangeResourceRecordSets のリクエストに含まれるアクションのリストを表します。 ChangeResourceRecordSetsActions は、次の値のどれでもかまいません (大文字である必要があります)。 • CREATE • UPSERT • DELETE

Route 53 条件キー	API オペレーション	値の型	説明
route53:VPCs	AssociateVPCWithHostedZone DisassociateVPCFromHostedZone ListHostedZonesByVPC CreateHostedZone CreateVPCAssociationAuthorization DeleteVPCAssociationAuthorization	複数値	AssociateVPCWithHostedZone 、DisassociateVPCFromHostedZone 、ListHostedZonesByVPC 、CreateHostedZone 、CreateVPCAssociationAuthorization 、DeleteVPCAssociationAuthorization のリクエスト内の VPC のリストを、「VPCId=<vpc-id>,VPCRegion=<region>」の形式で表します

Route 53 条件キー	API オペレーション	値の型	説明
`route53profiles:ResourceTypes`	AssociateResourceToProfile DisassociateResourceFromProfile UpdateProfileResourceAssociation	String	特定のリソースタイプでアクセスをフィルタリングします。 `route53profiles:ResourceTypes` には、次のいずれかの値を指定できます (大文字と小文字が区別されます) 。 • HostedZone • FirewallRuleGroup • ResolverQueryLoggingConfig • ResolverRule • VPCEndpoint
`route53profiles:ResourceArns`	AssociateResourceToProfile DisassociateResourceFromProfile	ARN	特定のリソース ARNs。

Route 53 条件キー	API オペレーション	値の型	説明
`route53profiles:HostedZoneDomains`	AssociateResourceToProfile DisassociateResourceFromProfile UpdateProfileResourceAssociation	String	ホストゾーンドメインでアクセスをフィルタリングします。予想される動作を取得するには、IAM ポリシーのドメイン名を次のように正規化する必要があります。 • ドメイン名には末尾のドットを含めないでください。 • これらの値は大文字と小文字が区別されます。
`route53profiles:ResolverRuleDomains`	AssociateResourceToProfile DisassociateResourceFromProfile UpdateProfileResourceAssociation	String	リゾルバールールドメインでアクセスをフィルタリングします。予想される動作を取得するには、IAM ポリシーのドメイン名を次のように正規化する必要があります。 • ドメイン名には末尾のドットを含めないでください。 • これらの値は大文字と小文字が区別されます。

Route 53 条件キー	API オペレーション	値の型	説明
route53profiles:FirewallRuleGroupPriority	AssociateResourceToProfile DisassociateResourceFromProfile UpdateProfileResourceAssociation	数値	ファイアウォールルールグループの優先度範囲によってアクセスをフィルタリングします。
route53profiles:ResourceIds	AssociateProfile DisassociateProfile	String	指定された VPCs。

ポリシー例: きめ細かなアクセスのための条件の使用

このセクションのそれぞれの例では、Effect 句を Allow に設定し、許可されるアクション、リソース、およびパラメータのみを指定します。IAM ポリシーで明示的に指定されたものへのアクセスだけが許可されます。

場合によっては、拒否ベースとなるようにこのポリシーを書き直すことができます。つまり、Effect 句を Deny に設定して、ポリシーのすべてのロジックを逆にします。ただし、拒否ベースのポリシーを使用しないことをお勧めします。このようなポリシーは、許可ベースのポリシーと比べて、正しく記述することが難しいためです。テキストの正規化が必要なため、これは特に Route 53 に当てはまります。

特定の名前の DNS レコードへのアクセスを制限するアクセス許可を付与する

次のアクセス許可ポリシーでは、example.com および marketing.example.com のホストゾーン Z12345 での ChangeResourceRecordSets アクションを許可する。このポリシーでは route53:ChangeResourceRecordSetsNormalizedRecordNames 条件キーを使用して、指定した名前に一致するレコードに対してのみにユーザーアクションを制限します。

JSON

```
{
    "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 は、複数値のキーに適用される IAM 条件演算子です。上記のポリシーの条件では、ChangeResourceRecordSets のすべての変更が example.com の DNS 名を持つ場合にのみオペレーションが許可されます。詳細については、「IAM ユーザーガイド」の「IAM condition operators」(IAM 条件演算子) と「IAM condition with multiple keys or values」(複数のキーまたは値を含む IAM 条件) 参照してください。

特定のサフィックスを含む名前に一致するアクセス許可を実装するには、条件演算子 StringLike または StringNotLike を含むポリシーで IAM ワイルドカード (*) を使用します。次のポリシーでは、ChangeResourceRecordSets オペレーションのすべての変更の DNS 名が「-beta.example.com」で終わる場合、オペレーションが許可されます。

JSON

```
{
    "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 ワイルドカードはドメイン名ワイルドカードとは異なります。ドメイン名でワイルドカードを使用する方法については、次の例を参照してください。

ワイルドカードを含むドメイン名と一致する DNS レコードへのアクセスを制限するアクセス許可を付与する

次のアクセス許可ポリシーでは、example.com のホストゾーン Z12345 での `ChangeResourceRecordSets` アクションを許可する。このポリシーでは `route53:ChangeResourceRecordSetsNormalizedRecordNames` を使用してユーザーアクションを *.example.com と一致するレコードのみに制限します。

JSON

```
{
    "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 は DNS 名の文字 * の 8 進コードで、\ に含まれる \052 は JSON 構文に従ってエスケープされて \\ になります。

特定の DNS レコードへのアクセスを制限するアクセス許可を付与する

次のアクセス許可ポリシーでは、example.com のホストゾーン Z12345 での ChangeResourceRecordSets アクションを許可する。3 つの条件キーの組み合わせを使用してユーザーアクションを制限し、特定の DNS 名とタイプの DNS レコードの作成または編集のみを許可します。

JSON

```
{
    "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"]
                }
            }
          }
        ]
}
```

指定されたタイプの DNS レコードのみの作成と編集にアクセスを制限するアクセス許可を付与する

次のアクセス許可ポリシーでは、example.com のホストゾーン Z12345 での ChangeResourceRecordSets アクションを許可する。このポリシーでは route53:ChangeResourceRecordSetsRecordTypes 条件キーを使用して、指定したタイプ (A および AAAA) に一致するレコードに対してのみにユーザーアクションを制限します。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "route53:ChangeResourceRecordSets",
            "Resource": "arn:aws:route53:::hostedzone/Z11111112222222333333",
            "Condition": {
                "ForAllValues:StringEquals":{
                    "route53:ChangeResourceRecordSetsRecordTypes": ["A", "AAAA"]
                }
            }
          }
        ]
}
```

IAM プリンシパルで操作できる VPC を指定するアクセス許可を付与する

次のアクセス許可ポリシーは、vpc-id で指定された VPC の AssociateVPCWithHostedZone、DisassociateVPCFromHostedZone、ListHostedZonesByVPC、アクションを許可するアクセス許可を付与します。

> **Important**
>
> 条件値は VPCId=<vpc-id>,VPCRegion=<region> の形式である必要があります。条件値に VPC ARN を指定した場合、条件キーは有効になりません。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Action": [
                "route53:*"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringLike": {
                    "route53:VPCs": [
                        "VPCId=<vpc-id>,VPCRegion=<region>"
                    ]
                }
            }
        },
        {
            "Sid": "Statement2",
            "Effect": "Allow",
            "Action": "ec2:DescribeVpcs",
            "Resource": "*"
        }
    ]
}
```

Important

`route53profiles` 条件キーは、me-central-1 と me-south-1 を除き、Route 53 Route53Profiles が利用可能なすべての AWS リージョン で使用できます。

Route 53 Profiles の特定のリソースタイプへのリソースの関連付けを制限するアクセス許可を付与する

次のアクセス許可ポリシーは、リソースタイプがホストゾーンの場合にのみ AssociateResourceToProfile および DisassociateResourceFromProfileアクションを許可するアクセス許可を付与します。route53profiles:ResourceTypes 条件キーを使用して、プロファイルに関連付けることができるリソースタイプを制限します。

```
{
    "Effect": "Allow",
    "Action": [
        "route53profiles:AssociateResourceToProfile",
        "route53profiles:DisassociateResourceFromProfile"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "route53profiles:ResourceTypes": "HostedZone"
        }
    }
}
```

Route 53 Profiles の特定のリソース ARNs へのリソースの関連付けを制限するアクセス許可を付与する

次のアクセス許可ポリシーは、指定されたリソース ARN に対してのみ AssociateResourceToProfile および DisassociateResourceFromProfileアクションを許可するアクセス許可を付与します。route53profiles:ResourceArns 条件キーを使用して、プロファイルに関連付けることができるリソースを制限します。

```
{
    "Effect": "Allow",
    "Action": [
        "route53profiles:AssociateResourceToProfile",
        "route53profiles:DisassociateResourceFromProfile"
    ],
    "Resource": "*",
    "Condition": {
        "ArnEquals": {
            "route53profiles:ResourceArns": "arn:aws:route53:::hostedzone/Z12345"
        }
    }
}
```

Route 53 Profiles の特定のホストゾーンドメインへのリソースの関連付けを制限するアクセス許可を付与する

次のアクセス許可ポリシーはAssociateResourceToProfile、ホストゾーンドメインが指定された値と一致する場合にのみ、、DisassociateResourceFromProfile、およびUpdateProfileResourceAssociationアクションを許可するアクセス許可を付与します。route53profiles:HostedZoneDomains 条件キーを使用して、プロファイルに関連付けることができるホストゾーンドメインを制限します。

```
{
    "Effect": "Allow",
    "Action": [
        "route53profiles:AssociateResourceToProfile",
        "route53profiles:DisassociateResourceFromProfile",
        "route53profiles:UpdateProfileResourceAssociation"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "route53profiles:HostedZoneDomains": "example.com"
        }
    }
}
```

Route 53 プロファイルの特定のリゾルバールールドメインへのリソースの関連付けを制限するアクセス許可を付与する

次のアクセス許可ポリシーはAssociateResourceToProfile、リゾルバールールドメインが指定された値と一致する場合にのみ、、DisassociateResourceFromProfile、および UpdateProfileResourceAssociationアクションを許可するアクセス許可を付与します。route53profiles:ResolverRuleDomains 条件キーを使用して、プロファイルに関連付けることができるリゾルバールールドメインを制限します。

```
{
    "Effect": "Allow",
    "Action": [
        "route53profiles:AssociateResourceToProfile",
        "route53profiles:DisassociateResourceFromProfile",
        "route53profiles:UpdateProfileResourceAssociation"
    ],
    "Resource": "*",
```

```
    "Condition": {
        "StringEquals": {
            "route53profiles:ResolverRuleDomains": "example.com"
        }
    }
}
```

Route 53 プロファイルの特定の優先度範囲へのファイアウォールルールグループの関連付けを制限するアクセス許可を付与する

次のアクセス許可ポリシーはAssociateResourceToProfile、ファイアウォールルールグループの優先度が指定された範囲内にある場合にのみ、、DisassociateResourceFromProfile、および UpdateProfileResourceAssociationアクションを許可するアクセス許可を付与します。route53profiles:FirewallRuleGroupPriority 条件キーを使用して、使用できる優先度値を制限します。

```
{
    "Effect": "Allow",
    "Action": [
        "route53profiles:AssociateResourceToProfile",
        "route53profiles:DisassociateResourceFromProfile",
        "route53profiles:UpdateProfileResourceAssociation"
    ],
    "Resource": "*",
    "Condition": {
        "NumericGreaterThanEquals": {
            "route53profiles:FirewallRuleGroupPriority": "100"
        }
    }
}
```

Route 53 プロファイルVPCs へのプロファイルの関連付けを制限するアクセス許可を付与する

次のアクセス許可ポリシーは、指定された VPC に対してのみ AssociateProfile および DisassociateProfileアクションを許可するアクセス許可を付与します。route53profiles:ResourceIds 条件キーを使用して、プロファイルを関連付けることができる VPCsを制限します。

```
{
    "Effect": "Allow",
    "Action": [
        "route53profiles:AssociateProfile",
```

```
            "route53profiles:DisassociateProfile"
        ],
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "route53profiles:ResourceIds": "vpc-1a2b3c4d5e6f"
            }
        }
}
```

Amazon Route 53 API のアクセス許可: アクション、リソース、条件のリファレンス

IAM ID にアタッチできるアクセス許可ポリシー (アイデンティティベースのポリシー) を設定アクセスコントロールして記述する場合、Route 53 のアクション、リソース、および条件キー、VPC リゾルバーの Route 53 ドメインのアクション、リソース、および条件キー、および Amazon Route 53 プロファイルのアクション、リソース、および条件キーのリストを使用して、サービス認可リファレンスVPCs と DNS 設定を共有できます。 https://docs.aws.amazon.com/service-authorization/latest/reference/list_amazonroute53resolver.html ページには、各 Amazon Route 53 API アクション、アクセス許可を付与する必要があるアクション、アクセス許可を付与する必要がある AWS リソースが含まれます。ポリシーの `Action` フィールドでアクションを指定し、ポリシーの `Resource` フィールドでリソースの値を指定します。

Route 53 ポリシーで AWS全体の条件キーを使用して、条件を表現できます。 AWS全体のキーの完全なリストについては、IAM ユーザーガイドの「使用可能なキー」を参照してください。

> **Note**
>
> アクセスを許可する場合、ホストゾーンと Amazon VPC は同じパーティションに属している必要があります。パーティションは のグループです AWS リージョン。各 AWS アカウント は 1 つのパーティションにスコープされます。
> サポートされているパーティションは以下のとおりです。
>
> - `aws` - AWS リージョン
> - `aws-cn` - 中国リージョン
> - `aws-us-gov` - AWS GovCloud (US) Region
>
> 詳細については、AWS 全般のリファレンスの「アクセス管理」を参照してください。

> **Note**
>
> アクションを指定するには、次のように、該当するプレフィックス (route53、route53domains、route53resolver など) に続けて API オペレーション名を使用します。
>
> - route53:CreateHostedZone
> - route53domains:RegisterDomain
> - route53resolver:CreateResolverEndpoint

Amazon Route 53 でのログ記録とモニタリング

Amazon Route 53 は、DNS クエリログ記録と、ヘルスチェックを使用してリソースをモニタリングする機能を提供しています。さらに、Route 53 は他の AWS サービスと統合して、追加のログ記録とモニタリングを提供します。

DNS クエリのログ記録

Route 53 が受信するクエリに関する情報を記録するように Route 53 を設定できます。情報とは、リクエストされたドメインまたはサブドメイン、リクエストの日時、DNS レコードタイプ (例: A、AAAA) などです。

詳細については、「パブリック DNS クエリのログ記録」を参照してください。

を使用してコンソールとプログラムによるアクション AWS CloudTrail を ログに記録する

CloudTrail は、ユーザー、ロール、または AWS のサービスによって実行された Route 53 アクションの記録を提供します。CloudTrail によって収集された情報を使用して、発行されたリクエスト、リクエスト発行元の IP アドレス、リクエストの発行者、発行日時、その他の詳細を追跡できます。詳細については、「を使用した Amazon Route 53 API コールのログ記録 AWS CloudTrail」を参照してください。

ドメイン登録のモニタリング

この Route 53 ダッシュボードでは、ドメイン移管のステータスや、有効期限が近づいているドメインなど、ドメイン登録の状態に関する詳細情報が提供されます。

詳細については、「ドメイン登録のモニタリング」を参照してください。

Route 53 ヘルスチェックおよび Amazon CloudWatch を使用したリソースのモニタリング

Route 53 のヘルスチェックを作成してリソースをモニタリングできます。ヘルスチェックでは、CloudWatch を使用して生データを収集し、読み取り可能なほぼリアルタイムのメトリクスに加工します。

詳細については、「Amazon Route 53 のヘルスチェックと Amazon CloudWatch を使用したリソースのモニタリング」を参照してください。

Amazon CloudWatch を使用して Route 53 VPC Resolver エンドポイントをモニタリングする

CloudWatch を使用して、 エンドポイントによって転送される DNS クエリの数をモニタリングできます。

詳細については、「Amazon CloudWatch による Route 53 VPC Resolver エンドポイントのモニタリング」を参照してください。

の使用 AWS Trusted Advisor

Trusted Advisor は、 AWS 顧客へのサービス提供から学んだベストプラクティスを活用します。は AWS 環境 Trusted Advisor を検査し、コスト削減、システムの可用性とパフォーマンスの向上、セキュリティギャップの解消に役立つ機会があれば、レコメンデーションを行います。すべての AWS お客様は 5 つの Trusted Advisor チェックにアクセスできます。ビジネスまたはエンタープライズサポートプランをご利用のお客様は、すべての Trusted Advisor チェックを表示できます。

詳細については、「Trusted Advisor」を参照してください。

Amazon Route 53 のコンプライアンス検証

サードパーティーの監査者は、複数のコンプライアンスプログラムの一環として Amazon Route 53 のセキュリティと AWS コンプライアンスを評価します。これらのプログラムには、SOC、PCI、FedRAMP、HIPAA などがあります。

特定のコンプライアンスプログラムの対象となる AWS サービスのリストについては、AWS「コンプライアンスプログラムによる対象範囲内のサービス」を参照してください。一般的な情報については、「AWS コンプライアンスプログラム」を参照してください。

を使用して、サードパーティーの監査レポートをダウンロードできます AWS Artifact。詳細については、AWS「Artifact でのレポートのダウンロード」を参照してください。

Route 53 を使用する際のお客様のコンプライアンス責任は、お客様のデータの機密性や貴社のコンプライアンス目的、適用可能な法律および規制によって決定されます。Route 53 の使用が HIPAA、PCI、FedRAMP などの標準への準拠の対象である場合、 は以下に役立つリソース AWS を提供します。

- セキュリティとコンプライアンスのクイックスタートガイド – これらのデプロイガイドでは、アーキテクチャ上の考慮事項について説明し、セキュリティとコンプライアンスに重点を置いたベースライン環境をデプロイする手順について説明します AWS。
- HIPAA セキュリティおよびコンプライアンスのためのアーキテクチャ設計ホワイトペーパー - このホワイトペーパーは、企業が AWS を使用して HIPAA に準拠するアプリケーションを構築する方法を説明します。
- AWS コンプライアンスリソース – このワークブックとガイドのコレクションは、お客様の業界や地域に適用される場合があります。
- AWS Config – この AWS サービスは、リソース設定が内部プラクティス、業界ガイドライン、および規制にどの程度準拠しているかを評価します。
- AWS Security Hub CSPM – この AWS サービスは、 内のセキュリティ状態を包括的に把握 AWS し、セキュリティ業界標準とベストプラクティスへの準拠を確認するのに役立ちます。

Amazon Route 53 での耐障害性

AWS グローバルインフラストラクチャは、 AWS リージョンとアベイラビリティーゾーンを中心に構築されています。 AWS リージョンは、低レイテンシー、高スループット、冗長性の高いネットワークで接続された、物理的に分離された複数のアベイラビリティーゾーンを提供します。アベイラビリティーゾーンでは、アベイラビリティーゾーン間で中断せずに、自動的にフェイルオーバーするアプリケーションとデータベースを設計および運用することができます。アベイラビリティーゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性、耐障害性、およびスケーラビリティが優れています。

Route 53 の機能は、コントロールとデータプレーンに分割されています。Route 53 のサービスは、多くの AWS と同様、リソースの作成、更新、削除などの管理操作を実行するためのコントロールプレーンと、サービスの中核的な機能を提供するためのデータプレーンで構成されています。Route 53 でのコントロールプレーンとデータプレーンの詳細については、「コントロールプレーンとデータプレーンの概念」を参照してください。

Route 53 は主にグローバルサービスですが、以下の機能は AWS リージョンをサポートしています。

- Route 53 VPC Resolver を使用してハイブリッド設定をセットアップする場合は、選択した AWS リージョンにエンドポイントを作成し、複数のアベイラビリティーゾーンで IP アドレスを指定します。アウトバウンドエンドポイントについては、エンドポイントを作成したのと同じリージョン内でルールを作成します。詳細については、「Route 53 VPC Resolver とは」を参照してください。
- Amazon EC2 インスタンスや Elastic Load Balancing ロードバランサーなど、特定のリージョンで作成するリソースのヘルスを確認するよう Route 53 ヘルスチェックを設定できます。
- エンドポイントをモニタリングするヘルスチェックを作成するときは、オプションで Route 53 がヘルスチェックを実行するリージョンを指定できます。

AWS リージョンとアベイラビリティーゾーンの詳細については、AWS 「 グローバルインフラストラクチャ」を参照してください。

Amazon Route 53 でのインフラストラクチャセキュリティ

マネージドサービスである Amazon Route 53 は、 AWS グローバルネットワークセキュリティで保護されています。 AWS セキュリティサービスと がインフラストラクチャ AWS を保護する方法については、AWS 「 クラウドセキュリティ」を参照してください。インフラストラクチャセキュリティのベストプラクティスを使用して環境を AWS 設計するには、「Security Pillar AWS Well-Architected Framework」の「Infrastructure Protection」を参照してください。

AWS 公開された API コールを使用して、ネットワーク経由で Route 53 にアクセスします。クライアントは次をサポートする必要があります。

- Transport Layer Security (TLS)。TLS 1.2 が必須で、TLS 1.3 をお勧めします。
- DHE (楕円ディフィー・ヘルマン鍵共有) や ECDHE (楕円曲線ディフィー・ヘルマン鍵共有) などの完全前方秘匿性 (PFS) による暗号スイート。これらのモードは、Java 7 以降など、最近のほとんどのシステムでサポートされています。

Resolver DNS Firewall から Security Hub CSPM に検出結果を送信する

AWS Security Hub CSPM は、 のセキュリティ状態を包括的に把握 AWS し、セキュリティ業界標準とベストプラクティスに照らして環境をチェックするのに役立ちます。Security Hub CSPM は AWS アカウント AWS のサービス、 全体、およびサポートされているサードパーティーパートナー製品からセキュリティデータを収集し、セキュリティの傾向を分析し、最も優先度の高いセキュリティ問題を特定するのに役立ちます。

Resolver DNS Firewall を Security Hub CSPM と統合することで、DNS Firewall から Security Hub CSPM に検出結果を送信できます。Security Hub CSPM は、セキュリティ体制の分析にこれらの検出結果を含めます。

目次

- Security Hub CSPM での検出結果の仕組み
  - DNS Firewall が送信する検出結果のタイプ
  - Security Hub CSPM が使用できない場合の再試行
  - Security Hub CSPM の既存の検出結果を更新する
- DNS Firewall からの一般的な検出結果
- 統合の有効化と構成
- Security Hub CSPM への検出結果の配信の停止

Security Hub CSPM での検出結果の仕組み

Security Hub CSPM では、検出結果は、セキュリティチェックまたはセキュリティ関連の検出の監視可能なレコードです。一部の検出結果は、他の AWS のサービス またはサードパーティーパートナーによって検出された問題から発生します。Security Hub CSPM には、セキュリティの問題を検出して検出結果を生成するために使用される独自のセキュリティコントロールもあります。

Security Hub CSPM には、これらすべてのソースからの検出結果を管理するためのツールが用意されています。検出結果の一覧を表示およびフィルタリングして、検出結果の詳細を表示できます。詳細については、AWS Security Hub 「 ユーザーガイド」の「Security Hub CSPM での検出結果の詳細と検出結果履歴の確認」を参照してください。検出結果を自動的に更新したり、カスタムアクションに送信したりすることもできます。詳細については、「 AWS Security Hub ユーザーガイド」

の「Security Hub CSPM の検出結果を自動的に変更してアクションを実行する」を参照してください。

Security Hub CSPM のすべての検出結果は、 AWS Security Finding Format (ASFF) と呼ばれる標準 JSON 形式を使用します。ASFF には、セキュリティ問題のソース、影響を受けるリソース、および検出結果の現在のステータスに関する詳細が含まれます。詳細については、AWS Security Hub ユーザーガイドの AWS Security Finding 形式 (ASFF) を参照してください。

DNS Firewall は、Security Hub CSPM に結果 AWS のサービス を送信する の 1 つです。

DNS Firewall が送信する検出結果のタイプ

DNS Firewall には次の統合があります。

- マネージドドメインリスト: AWS マネージドドメインリストに関連付けられたドメインに対してブロックまたはアラートが発生したクエリに関連するセキュリティ検出結果。
- カスタムドメインリスト: 顧客のドメインリストに関連付けられたドメインに対してブロックまたはアラートが発生したクエリに関連するセキュリティ検出結果。
- DNS Firewall Advanced: DNS Firewall Advanced によってブロックまたはアラートされたクエリに関連するセキュリティ検出結果。

Security Hub CSPM は、AWS Security Finding 形式 (ASFF) の DNS Firewall から検出結果を取り込みます。ASFF では、Types フィールドが検出結果タイプを提供します。DNS Firewall からの検出結果には、Types に対する次の値を指定できます。

- `TTPs/Impact/Impact:Runtime-MaliciousDomainRequest.Reputation`

Security Hub CSPM が使用できない場合の再試行

Security Hub CSPM が使用できない場合、DNS Firewall は結果を受信するまで結果の送信を再試行します。

Security Hub CSPM の既存の検出結果を更新する

同じ検出結果が再度観察された場合、DNS Firewall は既存の検出結果を更新します。

DNS Firewall からの一般的な検出結果

Security Hub CSPM は、AWS Security Finding 形式 (ASFF) で DNS Firewall の検出結果を取り込みます。

以下に、ASFF の DNS Firewall からの一般的な検出結果の例を示します。


```
{
            "SchemaVersion": "2018-10-08",
            "Id": "00000000-0000-0000-0000-example1",
            "ProductArn": "arn:aws:securityhub:us-east-1::product/amazon/route-53-
resolver-dns-firewall-aws-list",
            "ProductName": "Route 53 Resolver DNS Firewall - AWS List",
            "CompanyName": "Amazon",
            "Region": "us-east-1",
            "GeneratorId": "arn:aws:route53resolver:us-east-1:000000000000:firewall-
rule-group/rslvr-frg-example1",
            "AwsAccountId": "000000000000",
            "Types": [
                "TTPs/Impact/Impact:Runtime-MaliciousDomainRequest.Reputation"
            ],
            "FirstObservedAt": "2024-12-06T19:58:49.000Z",
            "LastObservedAt": "2024-12-06T19:58:49.000Z",
            "CreatedAt": "2024-12-06T19:58:49.000Z",
            "UpdatedAt": "2024-12-06T19:58:49.000Z",
            "Severity": {
                "Label": "HIGH",
                "Normalized": 70
            },
            "Title": "DNS Firewall ALERT generated for domain example1.com. from VPC
 vpc-example1",
            "Description": "DNS Firewall ALERT",
            "ProductFields": {
                "aws/route53resolver/dnsfirewall/queryName": "example1.com.",
                "aws/route53resolver/dnsfirewall/firewallRuleGroupId": "rslvr-frg-
example1",
                "aws/route53resolver/dnsfirewall/queryType": "A",
                "aws/route53resolver/dnsfirewall/queryClass": "IN",
                "aws/route53resolver/dnsfirewall/firewallDomainListId": "rslvr-fdl-
example1",
                "aws/route53resolver/dnsfirewall/transport": "UDP",
                "aws/route53resolver/dnsfirewall/firewallRuleAction": "ALERT",
```

```
                "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/
amazon/route-53-resolver-dns-firewall-aws-list/00000000-0000-0000-0000-example1",
                "aws/securityhub/ProductName": "Route 53 Resolver DNS Firewall - AWS
 List",
                "aws/securityhub/CompanyName": "Amazon"
            },
            "Resources": [
                {
                    "Type": "Other",
                    "Id": "rslvr-in-example1",
                    "Partition": "aws",
                    "Region": "us-east-1",
                    "Details": {
                        "Other": {
                            "ResourceType": "ResolverEndpoint",
                            "EndpointId": "rslvr-in-example1"
                        }
                    }
                },
                {
                    "Type": "Other",
                    "Id": "rni-example1",
                    "Partition": "aws",
                    "Region": "us-east-1",
                    "Details": {
                        "Other": {
                            "NetworkInterfaceId": "rni-example1",
                            "ResourceType": "ResolverNetworkInterface"
                        }
                    }
                }
            ],
            "WorkflowState": "NEW",
            "Workflow": {
                "Status": "NEW"
            },
            "RecordState": "ACTIVE",
            "FindingProviderFields": {
                "Severity": {
                    "Label": "HIGH"
                },
                "Types": [
                    "TTPs/Impact/Impact:Runtime-MaliciousDomainRequest.Reputation"
                ]
```

```
            },
            "ProcessedAt": "2024-12-11T19:33:35.494Z"
        }
```

統合の有効化と構成

DNS Firewall を Security Hub CSPM と統合するには、まず Security Hub CSPM を有効にする必要があります。Security Hub CSPM の有効化については、AWS Security Hub 「 ユーザーガイド」の「Security Hub CSPM の有効化」を参照してください。

Security Hub CSPM への検出結果の配信の停止

Security Hub CSPM への DNS Firewall の検出結果の送信を停止するには、Security Hub CSPM コンソールまたは Security Hub CSPM API を使用できます。

その方法については、「AWS Security Hub ユーザーガイド」の「統合先からの検出結果のフローの無効化」を参照してください。

Amazon Route 53 のモニタリング

モニタリングは、 AWS ソリューションの信頼性、可用性、パフォーマンスを維持する上で重要な部分です。マルチポイント障害が発生した場合は、その障害をより簡単にデバッグできるように、AWS ソリューションのすべての部分からモニタリングデータを収集する必要があります。ただし、モニタリングを開始する前に、以下の質問に対する回答を反映したモニタリング計画を作成する必要があります。

- どのような目的でモニタリングしますか?
- どのリソースをモニタリングしますか?
- どのくらいの頻度でこれらのリソースをモニタリングしますか?
- どのモニタリングツールを利用しますか?
- 誰がモニタリングタスクを実行しますか?
- 問題が発生したときに誰が通知を受け取りますか?

トピック

- パブリック DNS クエリのログ記録
- リゾルバーでのクエリのログ記録
- ドメイン登録のモニタリング
- Amazon Route 53 のヘルスチェックと Amazon CloudWatch を使用したリソースのモニタリング
- Amazon CloudWatch を使用したホストゾーンのモニタリング
- Amazon CloudWatch による Route 53 VPC Resolver エンドポイントのモニタリング
- Amazon CloudWatch を使用した Resolver DNS Firewall ルールグループのモニタリング
- を使用したリゾルバー DNS ファイアウォールイベントの管理 Amazon EventBridge
- を使用した Amazon Route 53 API コールのログ記録 AWS CloudTrail

パブリック DNS クエリのログ記録

Route 53 が受信するパブリック DNS クエリに関する次のような情報を口グ記録するように、Amazon Route 53 を設定できます。

- リクエストされたドメインまたはサブドメイン

- リクエストの日付と時刻
- DNS レコードタイプ (A や AAAA など)
- DNS クエリに応答した Route 53 エッジロケーション
- DNS レスポンスコード (`NoError` や `ServFail` など)

クエリログ記録を設定すると、Route 53 は CloudWatch Logs にログを送信します。CloudWatch Logs ツールを使用してクエリログにアクセスします。

クエリログには、DNS リゾルバーが Route 53 に転送したクエリのみが含まれます。DNS リゾルバーが既にクエリ (example.com のロードバランサーの IP アドレスなど) への応答をキャッシュしている場合、リゾルバーは Route 53 へのクエリの送信は行わず、対応するレコードの TTL の有効期限が切れるまで、キャッシュされた応答を返信し続けます。

クエリログは、すべての DNS クエリをキャプチャしない場合があります。ログに記録されるクエリの数は、ドメイン名 (example.com) またはサブドメイン名 (www.example.com) に対して送信されるクエリの数、ユーザーが使用するリゾルバー、およびレコードの TTL によって異なります。場合によっては、ログには数千件ごとに 1 つのクエリのみが含まれます。DNS の仕組みについては、「ウェブサイトやウェブアプリケーションへのインターネットトラフィックのルーティング」を参照してください。

詳細なログ情報が必要ない場合は、Amazon CloudWatch メトリクスを使用すると、ホストゾーンのために Route 53 が応答している DNS クエリの総数を確認できます。詳細については、「パブリックホストゾーンの DNS クエリメトリクスの表示」を参照してください

トピック

- DNS クエリのログ記録の設定
- Amazon CloudWatch を使用して DNS クエリログにアクセスする
- ログの保持期間の変更と Amazon S3 へのログのエクスポート
- クエリログ記録の停止
- DNS クエリログに表示される値
- クエリログの例

DNS クエリのログ記録の設定

特定のホストゾーンでの DNS クエリのログ記録を開始するには、Amazon Route 53 コンソールで以下のタスクを実行します。

- Route 53 がログを発行する先の CloudWatch Logs ロググループを選択するか、新しいロググループを作成します。

> **Note**
>
> ロググループは、米国東部 (バージニア北部) リージョンに置かれる必要があります。

- [Create (作成)] を選択して終了します。

> **Note**
>
> ユーザーがドメイン宛ての DNS クエリを送信すると、クエリログ記録の設定を作成してから数分以内にログ内にクエリが表示されるはずです。

DNS クエリのログ記録を設定するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [Hosted zones] を選択します。
3. クエリのログ記録を設定するホストゾーンを選択します。
4. [Hosted zone details] ペインで、[クエリログ記録の設定] を選択します。
5. 既存のロググループを選択するか、もしくは新しいロググループを作成します。
6. 許可に関するアラートを受け取った場合 (これは、新しいコンソールでのクエリログ記録の設定が完了していない場合に発生します)、次のいずれかの操作を行います。

   - 既に 10 個のリソースポリシーがある場合、それ以上ポリシーを作成することはできません。リソースポリシーのいずれかを選択し、[Edit (編集)] を選択します。編集することで、ロググループにログを書き込む許可が Route 53 に与えられます。[Save] を選択します。アラートが消え、次のステップに進むことが可能になります。
   - 以前にクエリのログ記録を設定したことがない場合 (または、リソースポリシーをまだ 10 個まで作成していない場合) は、CloudWatch Logs グループにログを書き込むためのアクセス許可を、Route 53 に付与する必要があります。[Grant permissions (アクセス許可の付与)] を選択します。アラートが消え、次のステップに進むことが可能になります。

7. [アクセス許可 – オプション] を選択してテーブルを表示し、リソースポリシーが CloudWatch ロググループに一致しているか、CloudWatch にログを発行するためのアクセス許可が Route 53 に付与されているかを確認します。
8. [Create (作成)] を選択します。

Amazon CloudWatch を使用して DNS クエリログにアクセスする

Amazon Route 53 では、クエリログは直接 CloudWatch Logs に送信されます。Route 53 経由でログにアクセスすることはできません。代わりに CloudWatch Logs を使用することで、ほぼリアルタイムでのログの表示、データの検索とフィルタリング、および Amazon S3 へのログのエクスポートが行えます。

Route 53 は、指定されたホストゾーンの DNS クエリに応答するための Route 53 エッジロケーションごとに、1 つの CloudWatch Logs ログストリームを作成し、クエリログを適切なログストリームに送信します。各ログストリームの名前の形式は *hosted-zone-id*/*edge-location-ID* (例: Z1D633PJN98FT9/DFW3) です。

各エッジロケーションは、3 文字コードと、割り当てられた任意の数字で識別されます (例: DFW3)。通常、この 3 文字コードは、エッジロケーションの近くにある空港の、国際航空運送協会の空港コードに対応します (これらの略語は今後変更される可能性があります。) エッジロケーションの一覧については、Route 53 製品の詳細ページの「Route 53 グローバルネットワーク」を参照してください。

> **Note**
>
> 上記の規則に従わないプレフィックスやサフィックスが表示される場合があります。これらのエンコード属性は、内部使用に限定されます。

詳細については、該当するドキュメントを参照してください。

- Amazon CloudWatch Logs ユーザーガイド
- Amazon CloudWatch Logs API リファレンス
- コマンドリファレンスの CloudWatch Logs AWS CLI セクション
- DNS クエリログに表示される値

ログの保持期間の変更と Amazon S3 へのログのエクスポート

デフォルトでは、CloudWatch Logs のクエリログの保持期限に制限はありません。必要に応じて保持期間を指定することで、 この期間よりも古いログを CloudWatch Logs が削除するようにできます。詳細については、Amazon CloudWatch ユーザーガイドの「CloudWatch Logs でのログデータ保持期間の変更」を参照してください。

ログデータを保持しながら、そのデータを CloudWatch Logs ツールにより確認および分析する必要がないという場合は、ログをAmazon S3 にエクスポートすることでストレージコストを削減できます。詳細については、「Amazon S3 へのログデータのエクスポート」を参照してください。

料金表の詳細については、該当の料金表ページを参照してください。

- CloudWatch 料金表ページの「Amazon CloudWatch Logs」
- Amazon S3 料金

> **Note**
>
> Route 53 で DNS クエリを ログ記録するように設定する場合には、利用料金は発生しません。

クエリログ記録の停止

CloudWatch Logs に対するクエリログの送信を、Amazon Route 53 に停止させる場合は、以下の手順を実行しクエリログ記録の設定を削除します。

クエリログ記録設定を削除するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [Hosted zones] を選択します。
3. クエリログ記録の設定を削除するホストゾーンの名前を選択します。
4. [Hosted zone details (ホストゾーンの詳細)] ペインで、[Delete query logging configuration (クエリログ記録の設定を削除)] を選択します。
5. [Delete] を選択して確定します。

DNS クエリログに表示される値

各ログファイルには、対応するエッジロケーションで Amazon Route 53 が DNS リゾルバーから受信した DNS クエリごとに、それぞれ 1 つのログエントリが記述されています。各ログエントリには、以下の値が記述されています。

ログ形式バージョン

クエリログのバージョン番号。ログにフィールドを追加したり既存のフィールドの形式を変更した場合、この値を増分します。

クエリのタイムスタンプ

Route 53 がリクエストに応答した日時。ISO 8601 形式の協定世界時 (UTC) (例: `2017-03-16T19:20:25.177Z`) です。

ISO 8601 形式については、Wikipedia の記事「ISO 8601」を参照してください。UTC については、Wikipedia の記事「協定世界時」を参照してください。

ホストゾーン ID

このログのすべての DNS クエリに関連付けられるホストゾーンの ID。

クエリ名

リクエストで指定されたドメインまたはサブドメイン。

クエリタイプ

リクエストで指定された DNS レコードタイプ、または ANY のいずれか。Route 53 でサポートされるタイプについては、「サポートされる DNS レコードタイプ」を参照してください。

Response Code (レスポンスコード)

DNS クエリに応答して Route 53 が返した DNS レスポンスコード。

レイヤー 4 プロトコル

クエリの送信に使用されたプロトコル (TCP または UDP)。

Route 53 エッジロケーション

クエリに応答した Route 53 エッジロケーション。各エッジロケーションは、3 文字コードと、任意の数字で識別されます (例: DFW3)。通常、この 3 文字コードは、エッジロケーションの近くにある空港の、国際航空運送協会の空港コードに対応します (これらの略語は今後変更される可能性があります。)

エッジロケーションの一覧については、Route 53 製品の詳細ページの「Amazon Route 53 のグローバルネットワーク」を参照してください。

リゾルバー IP アドレス

Route 53 にリクエストを送信した DNS リゾルバーの IP アドレス。

EDNS クライアントサブネット

リクエストを発信したクライアントの IP アドレスの一部 (DNS リゾルバーから取得できる場合)。

詳細については、IETF ドラフトの「Client Subnet in DNS Requests」を参照してください。

クエリログの例

クエリログの例を次のように表示します (リージョンはプレースホルダーです):

```
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 -
```

リゾルバーでのクエリのログ記録

次の DNS クエリをログ記録できます。

- 指定した Amazon Virtual Private Cloud VPC で発生するクエリ、およびこれらの DNS クエリに対する応答。
- インバウンドの Resolver エンドポイントを使用する、オンプレミスのリソースからのクエリ。
- 再帰的な DNS 解決にアウトバウンド Resolver のエンドポイントを使用するクエリ。
- Resolver DNS Firewall ルールを使用してドメインリストをブロック、許可、またはモニタリングするクエリ。

VPC Resolver クエリログには、次のような値が含まれます。

- VPC が作成された AWS リージョン
- クエリの発信元である VPC の ID
- クエリの発信元であるインスタンスの IP アドレス
- クエリの発信元であるリソースのインスタンス ID
- クエリが最初に作成された日時
- リクエストされた DNS 名 (prod.example.com など)
- DNS レコードタイプ (A や AAAA など)
- DNS レスポンスコード (`NoError` や `ServFail` など)
- DNS 応答データ (DNS クエリに応答して返される IP アドレスなど)
- DNS Firewall ルールのアクションに対する応答

ログに記録されるすべての値の詳細なリストと、その例については、「VPC Resolver クエリログに表示される値」を参照してください。

> **Note**
>
> DNS リゾルバーの標準と同様に、リゾルバーはその有効期限 (TTL) に定義されている期間、DNS クエリをキャッシュします。Route 53 VPC Resolver はVPCs で発生したクエリをキャッシュし、可能な限りキャッシュから応答してレスポンスを高速化します。VPC Resolver クエリログ記録は、VPC Resolver がキャッシュから応答できるクエリではなく、一意のクエリのみをログに記録します。
> 例えば、クエリのログ記録の設定が機能している VPC の 1 つにある EC2 インスタンスが、accounting.example.com に対しリクエストを送信するとします。VPC Resolver は、そのクエリへのレスポンスをキャッシュし、クエリをログに記録します。同じインスタンスの Elastic Network Interface が VPC Resolver のキャッシュの TTL 内で accounting.example.com に対してクエリを実行すると、VPC Resolver はキャッシュからクエリに応答します。この 2 番目のクエリはログに記録されません。

ログは、次のいずれかの AWS リソースに送信できます。

- Amazon CloudWatch Logs (CloudWatch Logs) のロググループ
- Amazon S3 (S3) バケット

- Firehose 配信ストリーム

詳細については、「AWS VPC Resolver クエリログを送信できる リソース」を参照してください。

トピック

- AWS VPC Resolver クエリログを送信できる リソース
- Resolver のクエリログ記録の設定の管理

AWS VPC Resolver クエリログを送信できる リソース

> **Note**
>
> 1 秒あたりのクエリ数 (QPS) が高いワークロードのクエリをログに記録する場合は、Amazon S3 を使用して、宛先に書き込むときにクエリログがスロットリングされないようにする必要があります。Amazon CloudWatch を使用している場合は、`PutLogEvents` オペレーションのために、1 秒あたりのリクエスト数の上限を引き上げることができます。CloudWatch の制限の引き上げの詳細については、Amazon CloudWatch ユーザーガイドの「CloudWatch Logs のクォータ」を参照してください。

VPC Resolver クエリログは、次の AWS リソースに送信できます。

Amazon CloudWatch Logs (Amazon CloudWatch Logs) のロググループ

Logs Insights を使用すると、ログの分析やメトリクスとアラームの作成が可能です。

詳細については、 Amazon CloudWatch Logs ユーザーガイドを参照してください。

Amazon S3 (S3) バケット

長期間にわたるログのアーカイブには、S3 バケットの使用が経済的です。通常は、高いレイテンシーが得られます。

すべての S3 サーバー側の暗号化オプションがサポートされています。詳細については、「Amazon S3 ユーザーガイド」の「サーバー側の暗号化によるデータの保護」を参照してください。

AWS KMS キーによるサーバー側の暗号化 (SSE-KMS) を選択した場合は、ログ配信アカウントが Amazon S3 バケットに書き込めるように、カスタマーマネージドキーのキーポリシーを

更新する必要があります。SSE-KMS での使用に必要なキーポリシーについては、「Amazon CloudWatch ユーザーガイド」の「Amazon S3 バケットのサーバー側の暗号化」を参照してください。

自分が所有するアカウント内に S3 バケットがある場合、必要なアクセス許可がバケットポリシーに自動的に追加されます。自身で所有していないアカウントの S3 バケットにログを送信する場合は、その S3 バケットの所有者が、バケットポリシーの中に必要なアクセス許可を追加する必要があります。次に例を示します。

JSON

```
{
    "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/*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "your_caller_account"
                }
            }
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::your_bucket_name",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "your_caller_account"
                }
            }
        },
        {
```

```
            "Effect": "Allow",
            "Principal": {
                "AWS": "iam_user_arn_or_account_number_for_root"
            },
            "Action": "s3:ListBucket",
            "Resource": "arn:aws:s3:::your_bucket_name"
        }
    ]
}
```

> **Note**
>
> 組織の中心的な S3 バケットにログを保存する場合は、(中心的バケットへの書き込みに必要なアクセス許可を持つ) 中央のアカウントからクエリログ記録を設定した上で、RAM を使用しながら、アカウント全体でその構成を共有することをお勧めします。

詳細については、Amazon Simple Storage Service ユーザーガイドを参照してください。

Firehose 配信ストリーム

Amazon OpenSearch Service、Amazon Redshift、またはその他のアプリケーションに対し、リアルタイムでログのストリーミングが可能です。

詳細については、「Amazon Data Firehose デベロッパーガイド」を参照してください。

Resolver でのクエリのログ記録の料金については、Amazon CloudWatch の料金表を参照してください。

CloudWatch Vended Logs 料金は、ログが Amazon S3 に直接公開されている場合でも、VPC Resolver ログを使用する場合に適用されます。詳細については、「Logs pricing at Amazon CloudWatch pricing」を参照してください。

Resolver のクエリログ記録の設定の管理

の設定 (VPC Resolver クエリログ記録)

VPC Resolver クエリのログ記録は、次の 2 つの方法で設定できます。

- 直接 VPC の関連付け - VPCsに直接関連付けます。

- プロファイルの関連付け - クエリログ記録設定を Route 53 プロファイルに関連付けます。これにより、そのプロファイルに関連付けられているすべての VPCs にログ記録が適用されます。詳細については、「VPC Resolver クエリログ設定を Route 53 プロファイルに関連付ける」を参照してください。

VPC で発生する DNS クエリのログ記録は、Amazon Route 53 コンソールで以下のタスクを実行することで開始できます。

Resolver のクエリログ記録を設定するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. Route 53 コンソールのメニューを展開します。コンソールの左上隅にある 3 本の水平バー (☰) アイコンを選択します。
3. Resolver メニューから、[Query logging (クエリログ記録)] を選択します。
4. リージョンセレクターで、クエリログ記録設定を作成する AWS リージョンを選択します。これは、DNS クエリを記録する VPC が作成されているリージョンと同じリージョンでなければなりません。VPC が複数のリージョンに存在する場合は、リージョンごとにクエリログ記録の設定を少なくとも 1 つ作成する必要があります。
5. [クエリログ記録の設定] を選択します。
6. 次の値を指定します。

   クエリログ記録設定の名前

   クエリログ記録の設定に使用する名前を入力します。この名前は、コンソールのクエリログ記録の設定リストに表示されます。この設定では、後で検索する際に便利な名前を入力します。

   クエリログの保存先

   VPC Resolver がクエリログを送信する AWS リソースのタイプを選択します。各オプション (CloudWatch Logs ロググループ、S3 バケット、および Firehose 配信ストリーム) から選択する方法については、「AWS VPC Resolver クエリログを送信できる リソース」を参照してください。

リソースのタイプを選択したら、そのタイプの別のリソースを作成するか、現在の AWS アカウントによって作成された既存のリソースを選択できます。

> **Note**
>
> ステップ 4 で選択した AWS リージョン (クエリログ記録の設定を作成するリージョン) で作成されたリソースのみを選択できます。新しいリソースを作成することを選択した場合、そのリソースは同じリージョンに作成されます。

クエリを口グに記録する VPC

このクエリログ記録の設定では、選択した VPC で発生した DNS クエリが口グに記録されます。VPC Resolver がクエリを口グに記録する現在のリージョンの各 VPC のチェックボックスをオンにし、選択を選択します。

代替: VPCs を直接関連付ける代わりに、このクエリログ記録設定を Route 53 プロファイルに関連付けることができます。これにより、そのプロファイルに関連付けられたすべての VPCs に口グ記録が適用されます。詳細については、「VPC Resolver クエリログ設定を Route 53 プロファイルに関連付ける」を参照してください。

> **Note**
>
> VPC 口グの配信は、特定の送信先タイプに対して 1 回だけ有効にすることができます。口グを同じタイプの複数の送信先に配信することはできません。例えば、VPC 口グを Amazon S3 にある 2 つの送信先に配信することはできません。

7. [クエリログ記録の設定] を選択します。

> **Note**
>
> クエリログ記録の設定が正常に作成されてから数分以内に、VPC 内のリソースによって作成された DNS クエリが口グ内に表示されるようになります。

VPC Resolver クエリログに表示される値

各ログファイルには、対応するエッジロケーションで Amazon Route 53 が DNS リゾルバーから受信した DNS クエリごとに、それぞれ 1 つのログエントリが記述されています。各ログエントリには、以下の値が記述されています。

バージョン

クエリログ形式のバージョン番号。現在のバージョンは `1.1` です。

バージョンの値には、**`major_version.minor_version`** の形式でメジャーおよびマイナーのバージョンが含まれています。例えば、`version` の値が `1.7` の場合には、`1` がメジャーバージョンを示し、`7` がマイナーバージョンを示します。

ログ構造に後方互換性のない変更が加えられた場合、Route 53 により、メジャーバージョンが増分されます。これには、既に存在する JSON フィールドの削除や、フィールドのコンテンツの表現方法 (日付形式など) の変更が含まれます。

変更によってログファイルに新しいフィールドが追加されると、Route 53 はマイナーバージョンを増分します。この処理は、VPC 内の既存の DNS クエリの一部またはすべてにおいて、新しい情報が利用可能になった時点で発生します。

account_id

VPC を作成した AWS アカウントの ID。

リージョン

VPC を作成した AWS リージョン。

vpc_id | resource_id

- `vpc_id` – クエリの送信元の VPC の ID。クエリログ記録設定が Route 53 プロファイルを通じて適用される場合、VPC ID は含まれません。
- `resource_id` – クエリログ記録設定が関連付けられている Route 53 プロファイルの ID。設定が Route 53 プロファイルに関連付けられている場合にのみ含まれます。

query_timestamp

クエリが送信された日時を、ISO 8601 形式の協定世界時 (UTC) で表します (例: `2017-03-16T19:20:17Z`) 。

ISO 8601 形式については、Wikipedia の記事「ISO 8601」を参照してください。UTC については、Wikipedia の記事「協定世界時」を参照してください。

query_name

クエリで指定されたドメイン名 (example.com) またはサブドメイン名 (www.example.com)。

query_type

リクエストで指定された DNS レコードタイプ、または ANY のいずれか。Route 53 でサポートされるタイプについては、「サポートされる DNS レコードタイプ」を参照してください。

query_class

クエリのクラス。

rcode

VPC Resolver が DNS クエリに応答して返した DNS レスポンスコード。応答コードは、クエリが有効であったかどうかを示します。最も一般的な応答コードは、クエリが有効であったことを意味する NOERROR です。レスポンスが有効でない場合、Resolver はその理由を示す応答コードを返します。使用される応答コードのリストについては、IANA ウェブサイトで「DNS RCODES」を参照してください。

answer_type

VPC Resolver がクエリに応答して返す値の DNS レコードタイプ (A、MX、CNAME など)。Route 53 でサポートされるタイプについては、「サポートされる DNS レコードタイプ」を参照してください。

rdata

VPC Resolver がクエリに応答して返した値。例えば、A レコードの場合は、IPv4 形式の IP アドレスになります。CNAME レコードの場合には、CNAME レコード内のドメイン名です。

answer_class

クエリに対する VPC Resolver レスポンスのクラス。

srcaddr

クエリの発信元であるホストの IP アドレス。

srcport

クエリの発信元であるインスタンスのポート。

transport

DNS クエリを送信するために使用されたプロトコル。

srcids

`instance`、`resolver_endpoint`、および DNS クエリの発信元、またはそのクエリが通過した `resolver_network_interface`。

インスタンス

クエリの発信元であるインスタンスの ID。

> **Note**
>
> Route 53 VPC Resolver クエリログにインスタンス ID が表示されていて、アカウントに表示されない場合は、DNS クエリが AWS CloudShell、ユーザーが使用した AWS Lambda Amazon EKS、または Fargate コンソールのいずれかから発生した可能性があります。

resolver_endpoint

DNS クエリをオンプレミス DNS サーバーに渡すリゾルバーエンドポイントの ID。

> **Note**
>
> 異なるリゾルバーエンドポイントを使用して異なる転送ルール間で連鎖する CNAME レコードがある場合、クエリログにはチェーンで最後に使用されたリゾルバーエンドポイントの ID のみが表示されます。複数のエンドポイントを通じて完全な解決パスを追跡するには、さまざまなクエリログ記録設定間でログを関連付けることができます。

firewall_rule_group_id

クエリ内のドメイン名と一致した DNS Firewall ルールグループの ID。この情報は、アクションが alert または block に設定されているルールとの一致が、DNS Firewall により検出された場合にのみ挿入されます。

ファイアウォールルールグループの詳細については、「DNS Firewall のルールグループとルール」を参照してください。

firewall_rule_action

クエリ内のドメイン名に一致したルールが指定しているアクション。この情報は、アクションが alert または block に設定されているルールとの一致が、DNS Firewall により検出された場合にのみ挿入されます。

firewall_domain_list_id

クエリ内のドメイン名に一致したルールによって使用されるドメインリスト。この情報は、アクションが alert または block に設定されているルールとの一致が、DNS Firewall により検出された場合にのみ挿入されます。

additional_properties

ログ配信イベントの追加情報。is_delayed: ログの配信に遅延がある場合。

Route 53 VPC Resolver クエリログの例

Resolver のクエリログの例を次に示します。

```
{
  "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"
    }
```

Resolver クエリのログ記録設定を他の AWS アカウントと共有する

1 つの AWS アカウントを使用して作成したクエリログ記録設定を他の AWS アカウントと共有できます。設定を共有するには、Route 53 VPC Resolver コンソールを AWS Resource Access Manager と統合します。Resource Access Manager の詳細については、Resource Access Manager ユーザーガイドを参照してください。

次の点に注意してください。

共有されたクエリログ記録の設定と VPC との関連付け

別の AWS アカウントが 1 つ以上の設定をアカウントと共有している場合、VPC VPCs を作成した設定に関連付けるのと同じ方法でVPCsを設定に関連付けることができます。

設定の削除または共有解除

他のアカウントと設定を共有し、その設定を削除するか共有を停止し、1 つ以上の VPCs が設定に関連付けられている場合、Route 53 VPC Resolver はそれらの VPCs から発信される DNS クエリのログ記録を停止します。

1 つの構成で関連付けることができるクエリログ記録の設定と VPC の最大数

1 つのアカウントで作成した設定を他の単一または複数のアカウントと共有する場合、その設定に関連付けることができる VPC の最大数が各アカウントに適用されます。たとえば、組織内に 10,000 個のアカウントがある場合、中央アカウントにクエリログ記録設定を作成し、 を通じて共有して、組織アカウント AWS RAM と共有できます。その後、組織のアカウントは設定を各自の VPC に関連付けます。アカウントにおける AWS リージョン ごとのクエリログ設定の VPC 関連付けは上限が 100 件となっているため、関連付けはその範囲内で行われます。ただし、すべての VPC が単一のアカウントにある場合は、必要に応じてアカウントのサービス制限を引き上げます。

現在の VPC リゾルバーのクォータについては、「」を参照してくださいRoute 53 VPC リゾルバーのクォータ。

アクセス許可

ルールを別の AWS アカウントと共有するには、PutResolverQueryLogConfigPolicy アクションを使用するアクセス許可が必要です。

ルールが共有されている AWS アカウントの制限

ルールを共有するアカウントは、ルールを変更または削除できません。

タグ付け

ルールを作成したアカウントのみが、ルールのタグを追加、削除、または表示できます。

ルールの現在の共有ステータス (ルールを共有したアカウントやルールの共有先であるアカウントなど) を確認し、別のアカウントとルールを共有するには、以下の手順を実行します。

共有ステータスを表示し、クエリログ記録設定を別の AWS アカウントと共有するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペイン内で [Query Logging (クエリログ記録)] を選択します。
3. ナビゲーションバーで、転送ルールを作成したリージョンを選択します。

   [Sharing status (共有ステータス)] 列に、現在のアカウントで作成されたルールまたは現在のアカウントと共有されているルールの現在の共有ステータスが表示されます。

   - Not shared: 現在の AWS アカウントがルールを作成し、そのルールは他のアカウントと共有されません。
   - Shared by me (自分が共有): 現在のアカウントがルールを作成し、1 つ以上の他のアカウントと共有しています。
   - Shared with me (自分と共有): 別のアカウントがルールを作成し、現在のアカウントと共有しています。
4. 共有情報を表示するルールまたは別のアカウントと共有するルールの名前を選択します。

   [Rule: ***rule name*** (ルール: rule name)] ページで、[Owner (所有者)] の値として、ルールを作成したアカウントの ID が表示されます。これは現在のアカウントです。ただし、[Sharing status (共有ステータス)] の値が [Shared with me (自分と共有)] である場合を除きます。その場合の [Owner (所有者)] は、ルールを作成して現在のアカウントと共有しているアカウントです。

   共有ステータスも表示されます。
5. 共有設定を選択して AWS RAM コンソールを開きます。
6. 「AWS RAM ユーザーガイド」の「Creating a resource share in AWS RAM」のステップに従います。

> **Note**
>
> 共有設定を更新することはできません。以下のいずれかの設定を変更する場合は、新しい設定を使用してルールを共有し直し、古い共有設定を削除する必要があります。

ドメイン登録のモニタリング

Amazon Route 53 のダッシュボードでは、以下のようなドメイン登録の状態に関する詳細情報を提供します。

- 新しいドメイン登録の状態
- Route 53 へのドメイン移管の状態
- 有効期限に近づいているドメインのリスト

Route 53 コンソールのダッシュボードを定期的に確認することをお勧めします。特に、新しいドメインを登録したり、Route 53 にドメインを移管したりした後には、対処を要する問題がないことを確認してください。

また、ドメインの連絡先情報が最新であることを確認することをお勧めします。ドメインの有効期限が近づくと、Route 53 はドメインの登録者の連絡先に、ドメインの有効期限と更新方法に関する情報を E メールで送信します。

Amazon Route 53 のヘルスチェックと Amazon CloudWatch を使用したリソースのモニタリング

Amazon Route 53 のヘルスチェックを作成してリソースをモニタリングできます。ヘルスチェックでは、CloudWatch を使用して生データを収集し、ほぼリアルタイムの読み取り可能なメトリクスに加工します。これらの統計情報は、2 週間記録されるため、履歴情報にアクセスしてリソースの動作をより的確に把握できます。デフォルトでは、Route 53 のヘルスチェックからのメトリクスデータは、 1 分間隔で自動的に CloudWatch に送信されます。

Route 53 ヘルスチェックの詳細については、「CloudWatch を使用したヘルスチェックのモニタリング」を参照してください。CloudWatch の詳細については、Amazon CloudWatch ユーザーガイドの「Amazon CloudWatch とは」を参照してください。

Route 53 ヘルスチェックのメトリクスとディメンション

ヘルスチェックを作成すると、Amazon Route 53 は、指定したリソースに関するメトリクスとディメンションを毎分 1 回、 CloudWatch に対し送信し始めます。Route 53 コンソールでは、ヘルスチェックのステータスを表示できます。次の手順を使用して、CloudWatch コンソールでメトリクスを表示したり、 AWS Command Line Interface () を使用してメトリクスを表示したりすることもできますAWS CLI。

CloudWatch コンソールを使用してメトリクスを表示するには

1. CloudWatch コンソール (https://console.aws.amazon.com/cloudwatch/) を開きます。
2. ナビゲーションペインで [Metrics (メトリクス)] を選択してください。
3. [All Metrics] タブで、[Route 53] を選択します。
4. [Health Check Metrics] を選択します。

を使用してメトリクスを表示するには AWS CLI

- コマンドプロンプトで、次のコマンドを使用します。

```
aws cloudwatch list-metrics --namespace "AWS/Route53"
```

トピック

- Route 53 のヘルスチェックに関する CloudWatch メトリクス
- Route 53 ヘルスチェックでのメトリクスのディメンション

Route 53 のヘルスチェックに関する CloudWatch メトリクス

AWS/Route53 名前空間には、Route 53 のヘルスチェックに関する以下のメトリクスが含まれています。

ChildHealthCheckHealthyCount

計算されたヘルスチェックについて、正常なヘルスチェックの数。

有効な統計: Average (推奨)、Minimum、Maximum

単位: カウント

ConnectionTime

Route 53 のヘルスチェッカーがエンドポイントとの間で TCP 接続を確立するのにかかった平均時間 (ミリ秒)。ヘルスチェックの ConnectionTime は、すべてのリージョンまたは選択した地理的リージョンについて確認できます。

有効な統計: Average (推奨)、Minimum、Maximum

単位: ミリ秒

HealthCheckPercentageHealthy

選択されたエンドポイントの中で、正常である結果を返した Route 53 のヘルスチェッカーの割合。

有効な統計: Average、Minimum、Maximum

単位: パーセント

HealthCheckStatus

CloudWatch がチェックしているヘルスチェックエンドポイントのステータス。1 の場合は正常であることを、0 の場合は異常であることを示します。

有効な統計: 最小、平均、最大

単位: なし

SSLHandshakeTime

Route 53 のヘルスチェッカーが SSL ハンドシェイクを完了するまでにかかった平均時間 (ミリ秒)。ヘルスチェックの SSLHandshakeTime は、すべてのリージョンまたは選択した地理的リージョンについて確認できます。

有効な統計: Average (推奨)、Minimum、Maximum

単位: ミリ秒

TimeToFirstByte

Route 53 のヘルスチェッカーが、HTTP または HTTPS リクエストへの応答の先頭バイトを受け取るまでにかかった平均時間 (ミリ秒)。ヘルスチェックの TimeToFirstByte は、すべてのリージョンまたは選択した地理的リージョンについて確認できます。

有効な統計: Average (推奨)、Minimum、Maximum

単位: ミリ秒

Route 53 ヘルスチェックでのメトリクスのディメンション

ヘルスチェックのための Route 53 メトリクスは、AWS/Route53 名前空間を使用し、HealthCheckId のためのメトリクスを提供します。メトリクスを取得する場合は、HealthCheckId ディメンションを入力する必要があります。

さらに、ConnectionTime、SSLHandshakeTime、および TimeToFirstByte に対して、オプションとして Region も指定できます。Region を省略した場合、CloudWatch は、すべてのリージョンからのメトリクスを返します。Region を含めた場合は、指定したリージョンのみのメトリクスが CloudWatch から返されます。

詳細については、「CloudWatch を使用したヘルスチェックのモニタリング」を参照してください

Amazon CloudWatch を使用したホストゾーンのモニタリング

Amazon CloudWatch を使用して生データを収集し、ほぼリアルタイムで読み取り可能なメトリクスに加工することで、パブリックホストゾーンをモニタリングできます。メトリクスは、そのメトリクスが基づいている DNS クエリが Route 53 で受信された直後から利用できます。Route 53 ホストゾーンにおける CloudWatch メトリクスデータの詳細度は 1 分です。

詳細については、次のドキュメントを参照してください。

- Amazon CloudWatch コンソールでメトリクスを表示する方法、および AWS Command Line Interface (AWS CLI) を使用してメトリクスを取得する方法の概要と詳細については、パブリックホストゾーンの DNS クエリメトリクスの表示 を参照してください。
- メトリクスの保持期間の詳細については、Amazon CloudWatch API リファレンスの「GetMetricStatistics」を参照してください。
- CloudWatch の詳細については、Amazon CloudWatch ユーザーガイドの「Amazon CloudWatch とは」を参照してください。
- CloudWatch メトリクスの詳細については、Amazon CloudWatch ユーザーガイドの「Amazon CloudWatch メトリクスの使用」を参照してください。

トピック

- Route 53 パブリックホストゾーンの CloudWatch メトリクス

- Route 53 パブリックホストゾーンメトリクスの CloudWatch ディメンション

Route 53 パブリックホストゾーンの CloudWatch メトリクス

AWS/Route53 名前空間には、Route 53 ホストゾーンについての次のメトリクスが含まれます。

DNSQueries

ホストゾーンについて、指定された期間に Route 53 が応答している DNS クエリの数。

有効な統計: Sum、SampleCount

単位: カウント

リージョン: Route 53 はグローバルサービスです。ホストゾーンメトリクスを取得するには、リージョンに米国東部 (バージニア北部) を指定する必要があります。

DNSSECInternalFailure

ホストゾーン内に INTERNAL_FAILURE 状態のオブジェクトが存在する場合は、値が 1 になります。それ以外の場合は値は 0 です。

有効な統計: Sum

単位: カウント

ボリューム: 各ホストゾーンで 4 時間ごとに 1

リージョン: Route 53 はグローバルサービスです。ホストゾーンメトリクスを取得するには、リージョンに米国東部 (バージニア北部) を指定する必要があります。

DNSSECKeySigningKeysNeedingAction

(KMS の障害により) ACTION_NEED の状態になっているキー署名キー (KSK) の数。

有効な統計: Sum、SampleCount

単位: カウント

ボリューム: 各ホストゾーンで 4 時間ごとに 1

リージョン: Route 53 はグローバルサービスです。ホストゾーンメトリクスを取得するには、リージョンに米国東部 (バージニア北部) を指定する必要があります。

DNSSECKeySigningKeyMaxNeedingActionAge

キー署名キー (KSK) が ACTION_NEED 状態に設定されてからの経過時間。

有効な統計: 最大

単位: 秒

ボリューム: 各ホストゾーンで 4 時間ごとに 1

リージョン: Route 53 はグローバルサービスです。ホストゾーンメトリクスを取得するには、リージョンに米国東部 (バージニア北部) を指定する必要があります。

DNSSECKeySigningKeyAge

キー署名キー (KSK) が作成されてからの経過時間 (有効になってからではありません)。

有効な統計: 最大

単位: 秒

ボリューム: 各ホストゾーンで 4 時間ごとに 1

リージョン: Route 53 はグローバルサービスです。ホストゾーンメトリクスを取得するには、リージョンに米国東部 (バージニア北部) を指定する必要があります。

Route 53 パブリックホストゾーンメトリクスの CloudWatch ディメンション

ホストゾーンに関する Route 53 メトリクスは `AWS/Route53` 名前空間を使用し、`HostedZoneId` に関するメトリクスを提供します。DNS クエリの数を取得するには、`HostedZoneId` ディメンションでホストゾーンの ID を指定する必要があります。

Amazon CloudWatch による Route 53 VPC Resolver エンドポイントのモニタリング

Amazon CloudWatch を使用して、Route 53 VPC Resolver エンドポイントによって転送される DNS クエリの数をモニタリングできます。Amazon CloudWatch では、生データを収集し、ほぼリアルタイムの読み取り可能なメトリクスに加工します。これらの統計情報は、2 週間記録されるため、履歴

情報にアクセスしてリソースの動作をより的確に把握できます。デフォルトでは、Resolver エンドポイントのメトリクスデータは、5 分間隔で CloudWatch に自動的に送信されます。5 分間隔は、メトリクスデータを送信できる最小間隔でもあります。

VPC Resolver の詳細については、「」を参照してくださいRoute 53 VPC Resolver とは。CloudWatch の詳細については、「Amazon CloudWatch ユーザーガイド」の「Amazon CloudWatch とは」を参照してください。

Route 53 VPC Resolver のメトリクスとディメンション

DNS クエリをネットワークに転送するように VPC Resolver を設定すると、VPC Resolver は 5 分に 1 回、転送されるクエリの数に関するメトリクスとディメンションを CloudWatch に送信し始めます。次の手順を使用して、CloudWatch コンソールでメトリクスを表示するか、 AWS Command Line Interface () を使用してメトリクスを表示できますAWS CLI。

CloudWatch コンソールを使用して VPC Resolver メトリクスを表示するには

1. CloudWatch コンソールの https://console.aws.amazon.com/cloudwatch/ を開いてください。
2. ナビゲーションバーで、エンドポイントを作成したリージョンを選択します。
3. ナビゲーションペインで [Metrics (メトリクス)] を選択します。
4. [すべてのメトリクス] タブで、[Route 53 Resolver] を選択します。
5. 指定したエンドポイントに対するクエリの数を表示するには、[By Endpoint (エンドポイント別)] を選択します。次に、クエリ数を表示するエンドポイントを選択します。

   すべてのエンドポイントで を選択すると、現在の AWS アカウントによって作成されたすべてのインバウンドエンドポイントまたはすべてのアウトバウンドエンドポイントのクエリ数が表示されます。次に、[InboundQueryVolume] または [OutboundQueryVolume] を選択すると、必要な数が表示されます。

を使用してメトリクスを表示するには AWS CLI

- コマンドプロンプトで、次のコマンドを使用します。

```
aws cloudwatch list-metrics --namespace "AWS/Route53Resolver"
```

トピック

- Route 53 VPC リゾルバーの CloudWatch 基本メトリクス

- Route 53 VPC リゾルバーの CloudWatch 詳細メトリクス Route 53
- Route 53 VPC Resolver メトリクスのディメンション

Route 53 VPC リゾルバーの CloudWatch 基本メトリクス

AWS/Route53Resolver 名前空間には、Route 53 VPC Resolver エンドポイントと IP アドレスの基本的なメトリクスが無料で含まれています。

トピック

- Route 53 VPC Resolver エンドポイントのメトリクス
- Route 53 VPC Resolver の IP アドレスのメトリクス

Route 53 VPC Resolver エンドポイントのメトリクス

AWS/Route53Resolver 名前空間には、Route 53 VPC Resolver エンドポイントの次のメトリクスが含まれます。

EndpointHealthyENICount

OPERATIONAL ステータスの Elastic Network Interface の数です。(EndpointId が指定した) エンドポイントの Amazon VPC ネットワークインターフェイスが正しく設定されており、ネットワークと Resolver の間での、インバウンドまたはアウトバウンドの DNS クエリを通過させることができます。

有効な統計: Minimum、Maximum、Average

単位: カウント

EndpointUnhealthyENICount

AUTO_RECOVERING ステータスの Elastic Network Interface の数です。

Resolver は、(EndpointId が指定した) エンドポイントに関連付けられている 1 つ以上の Amazon VPC ネットワークインターフェイスを復旧しようとしています。復旧プロセス中は、エンドポイントは容量が制限された状態で機能し、復旧が完了するまで DNS クエリを処理できません。

有効な統計: Minimum、Maximum、Average

単位: カウント

InboundQueryVolume

インバウンドエンドポイントを対象とし、EndpointId で指定されたエンドポイントを介してネットワークから VPC に転送された DNS クエリの数。

有効な統計: Sum

単位: カウント

OutboundQueryVolume

アウトバウンドエンドポイントを対象とし、EndpointId で指定されたエンドポイントを介して VPC からネットワークに転送された DNS クエリの数。

有効な統計: Sum

単位: カウント

OutboundQueryAggregateVolume

アウトバウンドエンドポイントの場合、Amazon VPC からネットワークに転送された DNS クエリの総数 (以下を含む)。

- EndpointId で指定されたエンドポイントを介して VPC からネットワークに転送された DNS クエリの数。
- 現在のアカウントが他のアカウントと Resolver ルールを共有する場合、EndpointId によって指定されたエンドポイントを介してネットワークに転送される他のアカウントによって作成された VPC からのクエリ。

有効な統計: Sum

単位: カウント

ResolverEndpointCapacityStatus

Resolver エンドポイントの容量ステータス。このメトリクスは現在の容量使用率の状態を示します。これは、0 = OK (通常の運用容量）、1 = Warning (少なくとも 1 つの Elastic Network Interface が容量使用率 50% を超過）、2 = Critical (少なくとも 1 つの Elastic Network Interface が容量使用率 75% を超過) で示されます。

容量ステータスは、クエリボリューム、クエリレイテンシー、DNS プロトコル、DNS パケットサイズ、接続追跡ステータスなど、複数の要因によって決まります。

有効な統計: Maximum

単位: なし

VPC リゾルバーエンドポイント容量管理のベストプラクティス

容量の問題に対処するには、通常、Resolver エンドポイントの Elastic Network Interface の数を増やすことをお勧めします。ただし、特定のエンドポイントタイプには重要な考慮事項があります。

インバウンドエンドポイントの場合、トラフィックの負荷分散はお客様によって異なります。したがって、容量の警告や重大なアラートは、Elastic Network Interface のサブセットが不釣り合いに使用されている「ホットスポット」を示している可能性があります。

- 潜在的な負荷分散の問題を特定するには、各 Elastic Network Interface の InboundQueryVolume メトリクスを個別に調べます。

アウトバウンドエンドポイントの場合、トラフィックは Elastic Network Interface 間で自動的に分散されます。容量の問題は、ターゲットネームサーバーの問題、またはタイムアウトの高レイテンシークエリがリゾルバーネットワークインターフェイスを圧迫していることが原因である可能性があります。

- このような場合は、単に Elastic Network Interface を増やすだけでは効果がない可能性があるため、ターゲットネームサーバーを修正することをお勧めします。

Route 53 VPC Resolver の IP アドレスのメトリクス

`AWS/Route53Resolver` 名前空間には、Resolver のインバウンドエンドポイント、またはアウトバウンドエンドポイントに関連付けられた IP アドレスごとに、次のメトリクスが含まれています。(エンドポイントを指定すると、VPC Resolver は Amazon VPC Elastic Network Interface を作成します)。

InboundQueryVolume

インバウンドエンドポイントの IP アドレスごとに、ネットワークから、指定された IP アドレスに転送された DNS クエリの数。各 IP アドレスは、IP アドレス ID で識別されます。この値は Route 53 コンソールを使用して取得できます。該当するエンドポイントのページの [IP アドレス] セクションで、[IP アドレス ID] 列を参照してください。また、ListResolverEndpointIpAddresses を使用してプログラムで値を取得することもできます。

有効な統計: Sum

単位: カウント

OutboundQueryAggregateVolume

アウトバウンドエンドポイントの IP アドレスごとに、Amazon VPC からネットワークに転送された DNS クエリの総数 (以下を含む)。

- 指定された IP アドレスを使用して VPC からネットワークに転送された DNS クエリの数。
- 現在のアカウントが他のアカウントと Resolver ルールを共有する場合、指定された IP アドレスを介してネットワークに転送される他のアカウントによって作成された VPC からのクエリ。

各 IP アドレスは、IP アドレス ID で識別されます。この値は Route 53 コンソールを使用して取得できます。該当するエンドポイントのページの [IP アドレス] セクションで、[IP アドレス ID] 列を参照してください。また、ListResolverEndpointIpAddresses を使用してプログラムで値を取得することもできます。

有効な統計: Sum

単位: カウント

Route 53 VPC リゾルバーの CloudWatch 詳細メトリクス Route 53

Route 53 VPC Resolver は、エンドポイントのオプトイン機能として RNI Enhanced および Target Name Server メトリクスを提供します。これらのメトリクスは 1 分間隔で CloudWatch に送信されます。

> **Note**
>
> - 詳細なメトリクスはデフォルトでは有効になっていませんが、エンドポイントレベルで有効にすることができます。これらのメトリクスは、RniEnhancedMetricsEnabled フラグと TargetNameServerMetricsEnabled フラグを使用してエンドポイントを作成または更新するときにプログラムで有効にできます。詳細については、「CreateResolverEndpoint」および「UpdateResolverEndpoint」を参照してください。
> - Route 53 Resolver エンドポイントの詳細メトリクスの使用には、標準の CloudWatch 料金と料金が適用されます。詳細については、「Amazon CloudWatch 料金表」をご覧ください。

トピック

- RNI 拡張メトリクス
- ターゲットネームサーバーのメトリクス

RNI 拡張メトリクス

Route 53 Resolver は、RNI 拡張メトリクスを Amazon CloudWatch に公開して、Resolver エンドポイントと Resolver IP アドレスのパフォーマンスとヘルスをモニタリングします。`AWS/Route53Resolver` 名前空間には、、 `EndpointIdRniId`ディメンションの Route 53 Resolver インバウンドエンドポイントとアウトバウンドエンドポイントに関する次の RNI 拡張メトリクスが含まれます。

P90ResponseTime

Resolver エンドポイント (`RniId`) に関連付けられた Resolver IP () が受信した DNS クエリの 90 パーセンタイルレスポンスレイテンシー`EndpointId`

有効な統計: Maximum

単位: マイクロ秒

ServFailQueries

Resolver エンドポイントに関連付けられた Resolver IP (`RniId`) に送信された DNS クエリの SERVFAIL レスポンスの数 (`EndpointId`)

有効な統計: Sum

単位: カウント

NxDomainQueries

Resolver エンドポイントに関連付けられた Resolver IP (`RniId`) に送信された DNS クエリの NXDOMAIN レスポンスの数 (`EndpointId`)

有効な統計: Sum

単位: カウント

RefusedQueries

Resolver エンドポイントに関連付けられた Resolver IP (`RniId`) に送信された DNS クエリの REFUSED レスポンスの数 (`EndpointId`)

有効な統計: Sum

単位: カウント

FormErrorQueries

Resolver エンドポイントに関連付けられた Resolver IP (RniId) に送信された DNS クエリの FORMERR レスポンスの数 (EndpointId)

有効な統計: Sum

単位: カウント

TimeoutQueries

Resolver エンドポイントに関連付けられた Resolver IP (RniId) に送信された DNS クエリのタイムアウト数 (EndpointId)

有効な統計: Sum

単位: カウント

ターゲットネームサーバーのメトリクス

Route 53 Resolver は、Resolver エンドポイントに関連付けられたターゲットネームサーバーのパフォーマンスと可用性をモニタリングするために、ターゲットネームサーバーメトリクスを Amazon CloudWatch に発行します。AWS/Route53Resolver 名前空間には、、EndpointIDTargetNameServerIPディメンションの Route 53 Resolver アウトバウンドエンドポイントに関する以下の詳細なメトリクスが含まれます。

P90ResponseTime

Resolver エンドポイント (TargetNameServerIP) を介して送信される DNS クエリのターゲットネームサーバー IP (EndpointID) の 90 パーセンタイルレスポンスレイテンシー

有効な統計: Maximum

単位: マイクロ秒

RequestQueries

Resolver エンドポイント (TargetNameServerIP) を介してターゲットネームサーバー IP () に送信された DNS クエリの数EndpointID。

有効な統計: Sum

単位: カウント

TimeoutQueries

ターゲットネームサーバー IP (EndpointID) でタイムアウトしたリゾルバーエンドポイント () を介して送信された DNS クエリの数TargetNameServerIP。

有効な統計: Sum

単位: カウント

> **Note**
>
> 場合によっては、VPC Resolver メトリクス (ResolverEndpointCapacityStatus) と RNI 拡張メトリクスにギャップが見られることがあります。これらのギャップは、ネットワークインターフェイスが連続してスケジュールされたメンテナンスまたは更新を受けるときに発生する可能性があります。Route 53 がネットワークインターフェイスをサービスに返した後、サービスが運用データを収集し、これらのメトリクスを発行するまでに少なくとも 1 分かかります。これらのギャップは、VPC Resolver エンドポイントで停止が発生していることを示すものではありません。これらのメトリクスに対して CloudWatch アラームを設定する場合は、次のことをお勧めします。
>
> - アラームを「欠落データを無視として扱う」に設定する、または
> - アラームしきい値の評価期間を 5 分以上に設定します。
>
> これらの設定は、通常のメンテナンスアクティビティ中の誤アラームを減らすのに役立ちます。

Route 53 VPC Resolver メトリクスのディメンション

インバウンドエンドポイントとアウトバウンドエンドポイントの Route 53 VPC Resolver メトリクスは、 AWS/Route53Resolver名前空間を使用し、次のディメンションのメトリクスを提供します。

- EndpointId: EndpointIdディメンションの値を指定すると、CloudWatch は指定されたエンドポイントの DNS クエリの数を返します。を指定しない場合EndpointId、CloudWatch は現在の AWS アカウントによって作成されたすべてのエンドポイントの DNS クエリの数を返します。

- RniId ディメンションは、 OutboundQueryAggregateVolume および InboundQueryVolumeメトリクスでサポートされています。
- EndpointId、RniIdディメンションはP90ResponseTime、リゾルバーエンドポイントに関連付けられたリゾルバー IP アドレスTimeoutQueriesの ServFailQueriesNxDomainQueries、FormErrorQueries、、RefusedQueries、、およびでサポートされています。
- EndpointID、TargetNameServerIPディメンションはP90ResponseTime、リゾルバーエンドポイントに関連付けられたTimeoutQueriesターゲットネームサーバーの 、RequestQueries、および でサポートされています。

Amazon CloudWatch を使用した Resolver DNS Firewall ルールグループのモニタリング

Amazon CloudWatch を使用して、Resolver DNS Firewall ルールグループによってフィルタリングされた DNS クエリの数をモニタリングできます。Amazon CloudWatch では、生データを収集し、ほぼリアルタイムの読み取り可能なメトリクスに加工します。これらの統計情報は、2 週間記録されるため、履歴情報にアクセスしてリソースの動作をより的確に把握できます。デフォルトでは、DNS Firewall ルールグループについてのメトリクスデータは、5 分間隔で CloudWatch に対し自動的に送信されます。

DNS Firewallの詳細については、「DNS ファイアウォールを使用してアウトバウンド DNS トラフィックをフィルタリングする」 を参照してください。CloudWatch の詳細については、Amazon CloudWatch ユーザーガイドの「Amazon CloudWatch とは」を参照してください。

Resolver DNS Firewall のメトリクスとディメンション

Resolver DNS Firewall ルールグループを VPC に関連付けて DNS クエリをフィルタリングすると、DNS Firewall はフィルタリングするクエリに関するメトリクスとディメンションを 5 分ごとに CloudWatch に送信し始めます。DNS Firewall のメトリクスとディメンションの詳細については、「Resolver DNS Firewall の CloudWatch メトリクス」を参照してください。

次の手順を使用して、CloudWatch コンソールでメトリクスを表示するか、 AWS Command Line Interface () を使用してメトリクスを表示できますAWS CLI。

CloudWatch コンソールを使用して DNS Firewall のメトリクスを表示するには

1. CloudWatch コンソール (https://console.aws.amazon.com/cloudwatch/) を開きます。

2. ナビゲーションバーで、表示するリージョンを選択します。
3. ナビゲーションペインで [Metrics (メトリクス)] を選択してください。
4. すべてのメトリクスタブで、Route 53 VPC Resolver を選択します。
5. 目的のメトリクスを選択します。

を使用してメトリクスを表示するには AWS CLI

- コマンドプロンプトで、次のコマンドを使用します。

```
aws cloudwatch list-metrics --namespace "AWS/Route53Resolver"
```

トピック

- Resolver DNS Firewall の CloudWatch メトリクス

Resolver DNS Firewall の CloudWatch メトリクス

AWS/Route53Resolver 名前空間には、Resolver DNS Firewall ルールグループのメトリクスが含まれます。

トピック

- Resolver DNS Firewall ルールグループのメトリクス
- VPC に関するメトリクス
- ファイアウォールルールグループと VPC の関連付けに関するメトリクス
- ファイアウォールルールグループ内のドメインリストに関するメトリクス

Resolver DNS Firewall ルールグループのメトリクス

FirewallRuleGroupQueryVolume

ファイアウォールルールグループ (FirewallRuleGroupId で指定) と一致する DNS Firewall のクエリ数。

ディメンション: FirewallRuleGroupId

有効な統計: Sum

単位: カウント

VPC に関するメトリクス

VpcFirewallQueryVolume

VPC (`VpcId` で指定) からの DNS Firewall のクエリ数

ディメンション: `VpcId`

有効な統計: Sum

単位: カウント

ファイアウォールルールグループと VPC の関連付けに関するメトリクス

FirewallRuleGroupVpcQueryVolume

ファイアウォールルールグループ (`VpcId` で指定) と一致する、(`FirewallRuleGroupId` で指定された) VPC からの DNS Firewall のクエリ数

ディメンション: `FirewallRuleGroupId, VpcId`

有効な統計: Sum

単位: カウント

ファイアウォールルールグループ内のドメインリストに関するメトリクス

FirewallRuleQueryVolume

ファイアウォールルールグループ (`FirewallDomainListId` で指定) 内の、ファイアウォールドメインリスト (`FirewallRuleGroupId` で指定) と一致する DNS Firewall のクエリ数。

ディメンション: `FirewallRuleGroupId, FirewallDomainListId`

有効な統計: Sum

単位: カウント

トピック

- DNS Firewall データでの Amazon CloudWatch Contributor Insights の使用
- Amazon CloudWatch Logs Insights を使用した DNS Firewall ログの分析

DNS Firewall データでの Amazon CloudWatch Contributor Insights の使用

Amazon CloudWatch Contributor Insights はログデータを分析し、コントリビューターデータを表示する時系列を作成します。たとえば、最もブロックまたは許可された DNS クエリを生成するルールグループと VPCs を表示できます。このデータを使用して、最もフィルタリングされたトラフィックを生成するルールグループ、ドメイン、または VPCsを特定できます。詳細については、「Contributor Insights を使用した高カーディナリティデータの分析」を参照してください。

DNS Firewall データで Amazon CloudWatch Contributor Insights を使用するには

1. Contributor Insights では、分析する VPC の Route 53 VPC Resolver クエリログ記録が必要です。ターゲット VPC のクエリログ記録を有効にしていない場合は、次のステップを実行して有効にします。
2. Amazon VPC コンソールで、Route 53 VPC Resolver クエリログ記録ページを開き、クエリログ記録設定を作成します。送信先で、既存の CloudWatch Logs ロググループを選択するか、ロググループを作成します (クエリログ記録コンソールから直接ロググループを作成できます)。次に、設定をターゲット VPC に関連付けます。詳細については、「the section called “ 設定の管理”」を参照してください。
3. Amazon VPC DNS Firewall コンソールで、分析タブを開くか、Amazon CloudWatch Contributor Insights コンソールを開きます。

   > **Note**
   >
   > 分析タブから Contributor Insights と Logs Insights の両方にアクセスできます。関心のある個々のルールグループを選択して、その分析を表示することもできます。

4. Contributor Insights を選択し、ルールを作成します。詳細については、「Contributor Insights ルールを作成する」を参照してください。
5. [Rule type] (ルールタイプ) で、[Sample rule] (サンプルルール) を選択します。次に、サンプルルールの選択を選択し、Route 53 DNS Firewall Logs サンプルルールのいずれかを選択します。

> **Note**
>
> ファイアウォールルールグループ ID をルール名に含めて、ルールが適用されるルールグループを特定できるようにします。

6. サンプルルールを選択すると、CloudWatch はルールページのすべての必須フィールドを入力します。
7. 結果のメトリクスを表示するには、CloudWatch コンソールを開きます。メトリクス、次にすべてのメトリクス (クラシックメトリクス) を選択し、DNS Firewall メトリクスがすでに含まれている Route 53 VPC Resolver 名前空間を探します。

Amazon CloudWatch Logs Insights を使用した DNS Firewall ログの分析

Amazon CloudWatch Logs Insights を使用すると、DNS Firewall クエリログデータをインタラクティブに検索および分析できます。詳細については、「CloudWatch Logs Insights を使用したログデータの分析」を参照してください。

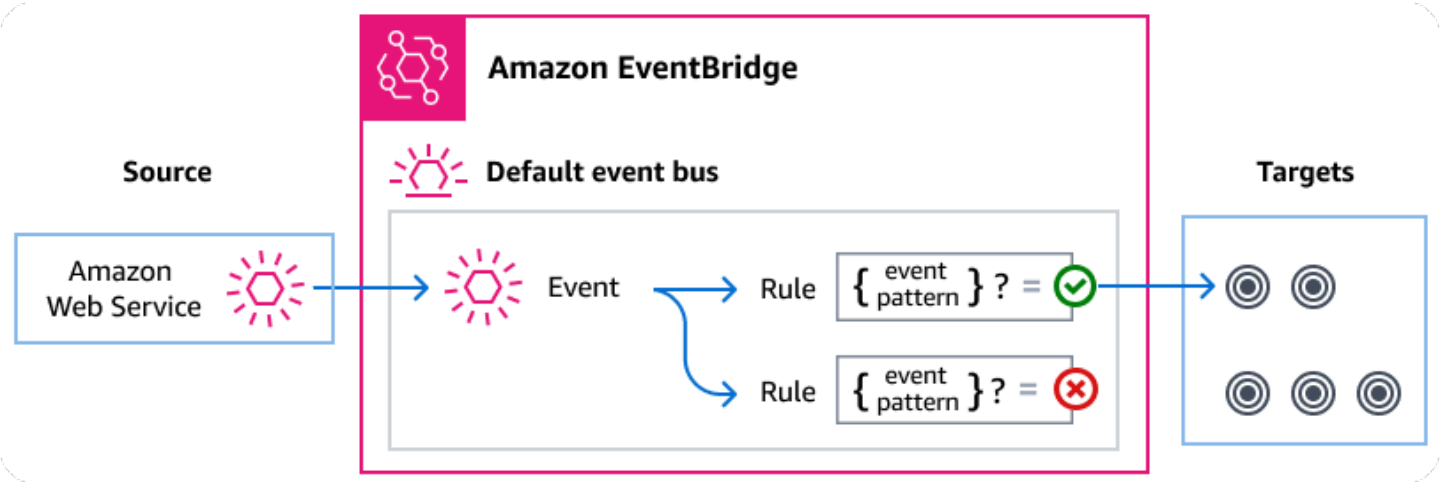
Amazon CloudWatch Logs Insights を使用して DNS Firewall ログを分析するには

1. Analytics タブから、Logs Insights を選択します。
2. 分析するロググループを 1 つ以上選択します。これらは、Route 53 VPC Resolver クエリのログ記録用に作成したロググループです。インデックスを作成するフィールドの選択の詳細については、「フィールドインデックスの作成」を参照してください。
3. 分析するディメンションを選択します。リソース、メトリクス、アクションの 3 つのディメンションから選択できます。
4. クエリを実行します。

を使用したリゾルバー DNS ファイアウォールイベントの管理 Amazon EventBridge

Amazon EventBridge は、イベントを使用してアプリケーションコンポーネントを接続するサーバーレスサービスであり、スケーラブルなイベント駆動型アプリケーションを簡単に構築できます。イベント駆動型アーキテクチャとは、イベントの発信と応答によって連携する、疎結合のソフトウェアシステムを構築するスタイルです。イベントとは、リソースまたは環境で発生した変更を指します。

多くの AWS サービスと同様に、DNS Firewall はイベントを生成してデフォルトのイベントバスに送信します EventBridge 。(デフォルトのイベントバスは、すべての AWS アカウントで自動的にプロビジョニングされます)。イベントバスは、イベントを受信して、ゼロ個以上の送信先 (ターゲット) に配信するルーターです。イベントが受信されると、ユーザーがイベントバスに対して指定したルールによって評価されます。各ルールは、イベントがルールのイベントパターンに一致するかどうかをチェックします。一致する場合、イベントバスはそのイベントを指定されたターゲットに送信します。



トピック

- リゾルバー DNS ファイアウォールイベント
- EventBridge ルールを使用したリゾルバー DNS ファイアウォールイベントの送信
- Amazon EventBridge アクセス許可
- その他の EventBridge リソース
- Resolver DNS Firewall イベントの詳細リファレンス

リゾルバー DNS ファイアウォールイベント

VPC Resolver は、DNS Firewall イベントをデフォルトの EventBridge イベントバスに自動的に送信します。イベントバスにルールを作成できます。各ルールには、イベントパターンと 1 つ以上のターゲットが含まれます。ルールのイベントパターンに一致するイベントは、ベストエフォートベースで指定されたターゲットに配信されます。イベントは順序どおりに配信される可能性があります。

次のイベントは DNS ファイアウォールによって生成されます。詳細については、Amazon EventBridge ユーザーガイドの EventBridgeを参照してください。

DNS ファイアウォールイベント

イベントの詳細のタイプ	説明
DNS ファイアウォールブロック	ドメインに対して実行されるブロックアクション。
DNS ファイアウォールアラート	ドメインに対して実行されるアラートアクション。

EventBridge ルールを使用したリゾルバー DNS ファイアウォールイベントの送信

EventBridge デフォルトのイベントバスが DNS Firewall イベントをターゲットに送信するには、目的の DNS Firewall イベントのデータに一致するイベントパターンを含むルールを作成する必要があります。

ルールの作成ステップは以下のとおりです。

1. 以下を指定するルールのイベントパターンを作成します。
   - VPC Resolver は、ルールによって評価されるイベントのソースです。
   - (オプション): 照合対象となるその他のイベントデータ。

   詳細については、???を参照してください。
2. (オプション): がルールのターゲットに情報を EventBridge 渡す前に、イベントからのデータをカスタマイズする入力トランスフォーマーを作成します。

   詳細については、「EventBridge ユーザーガイド」の「入力変換」を参照してください。
3. イベントパターンに一致するイベント EventBridge を配信するターゲット (複数可) を指定します。

   ターゲットは、他の AWS サービス、software-as-a-service (SaaS) アプリケーション、API 送信先、またはその他のカスタムエンドポイントです。詳細については、EventBridge ユーザーガイドのターゲットを参照してください。

イベントバスルールの詳細な作成方法については、「EventBridge ユーザーガイド」の「イベントに反応するルールの作成」を参照してください。

Resolver DNS Firewall イベントのイベントパターンの作成

DNS Firewall がデフォルトのイベントバスにイベントを配信すると、 は各ルールに定義されたイベントパターン EventBridge を使用して、イベントをルールのターゲット (複数可) に配信するかどうかを決定します。イベントパターンは、目的の DNS ファイアウォールイベントのデータに一致します。各イベントパターンは JSON 形式のオブジェクトで、以下が含まれています。

- イベントを送信するサービスを識別する `source` 属性。DNS ファイアウォールイベントの場合、ソースは `aws.route53resolver` です。
- (オプション): 照合するイベントタイプの配列を含む `detail-type` 属性。
- (オプション): 照合対象となるその他のイベントデータを含む `detail` 属性。

例えば、次のイベントパターンは、DNS ファイアウォールからのアラートイベントとブロックイベントの両方に一致します。

```
{
  "source": ["aws.route53resolver"],
  "detail-type": ["DNS Firewall Block", "DNS Firewall Alert"]
}
```

次のイベントパターンが BLOCK アクションと一致している間:

```
{
  "source": ["aws.route53resolver"],
  "detail-type": ["DNS Firewall Block"]
}
```

DNS ファイアウォールは、6 時間以内に同じドメインに対して同じイベントを 1 回だけ送信します。例えば、次のようになります。

1. インスタンス i-123 は、T1 に DNS クエリ exampledomain.com を送信しました。DNS ファイアウォールは、これが最初の発生であるため、アラートイベントまたはブロックイベントを送信します。
2. インスタンス i-123 は、T1+30 分に DNS クエリ exampledomain.com を送信しました。DNS ファイアウォールは、6 時間の時間枠内に繰り返し発生するため、アラートまたはブロックイベントを送信しません。

3. インスタンス i-123 は T1+7 時間に DNS クエリ exampledomain.com を送信しました。DNS ファイアウォールは、6 時間の時間枠外に発生したアラートイベントまたはブロックイベントを送信します。

詳細については、「EventBridge ユーザーガイド」の「イベントパターン」を参照してください。

での DNS Firewall イベントのイベントパターンのテスト EventBridge

EventBridge サンドボックスを使用すると、ルールを作成または編集する大規模なプロセスを完了することなく、イベントパターンをすばやく定義してテストできます。サンドボックスを使用すると、イベントパターンを定義し、サンプルイベントを使用して、パターンが目的のイベントと一致することを確認できます。サンドボックスから直接、そのイベントパターンを使用して新しいルールを作成するオプション EventBridge を提供します。

詳細については、 EventBridge ユーザーガイドの EventBridge 「サンドボックスを使用したイベントパターンのテスト」を参照してください。

DNS ファイアウォールの EventBridge ルールとターゲットの作成

次の手順では、EventBridge がすべての DNS Firewall アラートアクションとブロックアクションのイベントを送信し、ルールのターゲットとして AWS Lambda 関数を追加できるようにするルールを作成する方法を示します。

1. AWS CLI を使用して EventBridge ルールを作成します。

```
aws events put-rule \
--event-pattern "{\"source\":
[\"aws.route53resolver\"],\"detail-type\":
[\"DNS Firewall Block\", \"DNS Firewall Alert\"]}" \
--name dns-firewall-rule
```

2. ルールのターゲットとして Lambda 関数をアタッチします。

```
AWS events put-targets --rule dns-firewall-rule --targets
Id=1,Arn=arn:aws:lambda:us-east-1:111122223333:function:<your_function>
```

3. ターゲットを呼び出すために必要なアクセス許可を追加するには、次の Lambda AWS CLI コマンドを実行します。

```
AWS lambda add-permission --function-name <your_function> --statement-
id 1 --action 'lambda:InvokeFunction' --principal events.amazonaws.com
```

Amazon EventBridge アクセス許可

DNS ファイアウォールでは、 Amazon EventBridgeにイベントを配信するために追加のアクセス許可は必要ありません。

指定するターゲットには、特定のアクセス許可または設定が必要になる場合があります。ターゲットに特定のサービスを使用する方法の詳細については、「Amazon EventBridge ユーザーガイド」の「Amazon EventBridge ターゲット」を参照してください。

その他の EventBridge リソース

EventBridge を使用してイベントを処理および管理する方法の詳細については、 Amazon EventBridge ユーザーガイドの以下のトピックを参照してください。

- イベントバスの仕組みに関する詳細は、「Amazon EventBridge イベントバス」を参照してください。
- イベント構造については、「Amazon EventBridge イベント」を参照してください。
- ルールとイベントを照合するときに EventBridge が使用するイベントパターンの構築については、「イベントパターン」を参照してください。
- EventBridge が処理するイベントを指定するルールの作成方法については、「Amazon EventBridge ルール」を参照してください。
- 一致するイベント EventBridge を送信するサービスまたは他の送信先を指定する方法については、「ターゲット」を参照してください。

Resolver DNS Firewall イベントの詳細リファレンス

AWS サービスからのすべてのイベントには、イベントに関するメタデータを含む共通のフィールドセットがあります。これらのフィールドには、ソースサービス、イベントが生成された時刻、イベントが発生したアカウントとリージョンが含まれます。これらの一般的なフィールドの定義については、「Amazon EventBridge ユーザーガイド」の「イベント構造リファレンス」を参照してください。

さらに、各イベントには、その特定のイベントに固有のデータを含む `detail` フィールドがあります。以下のリファレンスでは、さまざまな DNS ファイアウォールイベントの詳細フィールドを定義しています。

EventBridge を使用して DNS Firewall イベントを選択および管理する場合、次の点に注意してください。

- DNS ファイアウォールのすべてのイベントの source フィールドは、aws.route53resolver に設定されています。
- detail-type フィールドはイベントタイプを指定します。

  例えば、DNS Firewall Block、DNS Firewall Alert です。
- detail フィールドには、その特定のイベントに固有のデータが含まれます。

DNS ファイアウォールイベントに一致するようにルールを有効化するイベントパターンの作成方法については、「Amazon EventBridge ユーザーガイド」の「イベントパターン」を参照してください。

イベントとその EventBridge 処理方法の詳細については、Amazon EventBridge 「 ユーザーガイド」のAmazon EventBridge 「 イベント」を参照してください。

トピック

- DNS ファイアウォールアラートイベントの詳細
- DNS ファイアウォールブロックイベントの詳細

DNS ファイアウォールアラートイベントの詳細

以下は、アラートステータスイベントの詳細の詳細フィールドです。

source と detail-type のフィールドがあるのは、Route 53 イベントに、これらに固有の値が含まれているためです。

```
{...,
 "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",
```

```
      "firewall-protection": "string",
      "resources": [{
         "resource-type": "string",
         "instance-details": {
             "id": "string",
       }
     },
     {
         "resource-type": "string",
         "resolver-endpoint-details": {
         "id": "string"
       }
     }
 ]
```

`detail-type`

イベントのタイプを示します。

このイベントの場合、この値は `DNS Firewall Alert` です。

`source`

イベントを発生させたサービスを識別します。DNS ファイアウォールイベントの場合、この値は `aws.route53resolver` です。

`detail`

イベントに関する情報を含む JSON オブジェクト。このフィールドの内容は、イベントを生成するサービスによって決まります。

このイベントの場合、このデータには以下が含まれます。

`account-id`

VPC AWS アカウント を作成した の ID。

`last-observed-at`

VPC でアラート/ブロッククエリが行われた時刻のタイムスタンプです。

`query-name`

クエリで指定されたドメイン名 (example.com) またはサブドメイン名 (www.example.com)。

`query-type`

リクエストで指定された DNS レコードタイプ、またはいずれか。Route 53 でサポートされるタイプについては、「サポートされる DNS レコードタイプ」を参照してください。

`query-class`

クエリのクラス。

`transport`

DNS クエリを送信するために使用されたプロトコル。

`firewall-rule-action`

クエリ内のドメイン名に一致したルールが指定しているアクション。ALERT または BLOCK です。

`firewall-rule-group-id`

クエリ内のドメイン名と一致した DNS Firewall ルールグループの ID。ファイアウォールルールグループの詳細については、「DNS Firewall DNS Firewall のルールグループとルール」を参照してください。

`firewall-domain-list-id`

クエリ内のドメイン名に一致したルールによって使用されるドメインリスト。

`firewall-protection`

DNS Firewall Advanced 保護: DGA、DICTIONARY_DGA、または DNS_TUNNELING。詳細については、「DNS Firewall DNS ファイアウォールの詳細ルール」を参照してください。

`resourcese`

リソースタイプとそれらの追加の詳細が含まれます。

`resource-type`

リゾルバーエンドポイントまたは VPC インスタンスなどのリソースタイプを指定します。

`resource-type``-detail`

リソースに関するその他の詳細。

Example DNS ファイアウォールアラートイベント

以下に示しているのは、アラートイベントの例です。

```
{
 "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",
 "firewall-protection": "DGA",
 "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 ファイアウォールブロックイベントの詳細

以下は、#####の詳細フィールドです。

source と detail-type のフィールドがあるのは、Route 53 イベントに、これらに固有の値が含まれているためです。

```
{...,
 "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",
      "firewall-protection": "string",
      "resources": [{
         "resource-type": "string",
         "instance-details": {
             "id": "string",
       }
     },
     {
         "resource-type": "string",
         "resolver-endpoint-details": {
         "id": "string"
       }
     }
 ]
```

detail-type

イベントのタイプを示します。

このイベントの場合、この値は DNS Firewall Alert です。

source

イベントを発生させたサービスを識別します。DNS ファイアウォールイベントの場合、この値は aws.route53resolver です。

`detail`

イベントに関する情報を含む JSON オブジェクト。このフィールドの内容は、イベントを生成するサービスによって決まります。

このイベントの場合、このデータには以下が含まれます。

`account-id`

VPC AWS アカウント を作成した の ID。

`last-observed-at`

VPC でアラート/ブロッククエリが行われた時刻のタイムスタンプです。

`query-name`

クエリで指定されたドメイン名 (example.com) またはサブドメイン名 (www.example.com)。

`query-type`

リクエストで指定された DNS レコードタイプ、またはいずれか。Route 53 でサポートされるタイプについては、「サポートされる DNS レコードタイプ」を参照してください。

`query-class`

クエリのクラス。

`transport`

DNS クエリを送信するために使用されたプロトコル。

`firewall-rule-action`

クエリ内のドメイン名に一致したルールが指定しているアクション。`ALERT` または `BLOCK` です。

`firewall-rule-group-id`

クエリ内のドメイン名と一致した DNS Firewall ルールグループの ID。ファイアウォールルールグループの詳細については、「DNS Firewall DNS Firewall のルールグループとルール」を参照してください。

`firewall-domain-list-id`

クエリ内のドメイン名に一致したルールによって使用されるドメインリスト。

`firewall-protection`

DNS Firewall Advanced 保護: DGA、DICTIONARY_DGA、または DNS_TUNNELING。詳細については、「DNS Firewall DNS ファイアウォールの詳細ルール」を参照してください。

`resourcese`

リソースタイプとそれらの追加の詳細が含まれます。

`resource-type`

リゾルバーエンドポイントまたは VPC インスタンスなどのリソースタイプを指定します。

`resource-type``-detail`

リソースに関するその他の詳細。

Exampleイベントの例

以下に示しているのは、ブロックイベントの例です。

```
{
 "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",
 "firewall-protection": "DNS_TUNNELING",
 "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"
 }
}
```

を使用した Amazon Route 53 API コールのログ記録 AWS CloudTrail

Route 53 は AWS CloudTrail、Route 53 のユーザー、ロール、または のサービスによって実行されたアクションを記録する AWS サービスである と統合されています。CloudTrail は、 Route 53 コンソールからのコールや、 Route 53 API へのコードのコールを含む Route 53 のすべての API コールを、イベントとしてキャプチャします。証跡を作成する場合は、Route 53 のイベントなど、Amazon S3 バケットへの CloudTrail イベントの継続的な配信を有効にすることができます。証跡を設定しない場合でも、CloudTrail コンソールの [Event history (イベント履歴)] で最新のイベントを表示できます。CloudTrail で収集された情報を使用して、Route 53 に対するリクエスト、そのリクエストが発信された IP アドレス、リクエストの作成者、リクエスト作成日時、その他の詳細情報などを確認できます。

トピック

- CloudTrail での Route 53 の情報
- イベント履歴での Route 53 イベントの表示
- Route 53 のログファイルエントリを理解する

CloudTrail での Route 53 の情報

CloudTrail は、 AWS アカウントの作成時にアカウントで有効になります。Route 53 でアクティビティが発生すると、そのアクティビティはイベント履歴の他の AWS サービスイベントとともに

CloudTrail イベントに記録されます。 AWS アカウントで最近のイベントを表示、検索、ダウンロードできます。詳細については、「CloudTrail Event 履歴でのイベントの表示」を参照してください。

Route 53 のイベントなど、 AWS アカウントのイベントの継続的な記録については、証跡を作成します。証跡により、ログファイルを CloudTrail で Amazon S3 バケットに配信できます。デフォルトでは、コンソールで追跡を作成するときに、追跡がすべてのリージョンに適用されます。証跡は、AWS パーティション内のすべてのリージョンからのイベントをログに記録し、指定した Amazon S3 バケットにログファイルを配信します。さらに、CloudTrail ログで収集されたイベントデータをさらに分析して処理するように他の AWS サービスを設定できます。詳細については、以下を参照してください。

- 証跡を作成するための概要
- CloudTrail がサポートされているサービスと統合
- 「CloudTrail の Amazon SNS 通知の設定」
- 「CloudTrail ログファイルを複数のリージョンから受け取る」、「複数のアカウントから CloudTrail ログファイルを受け取る」

すべての Route 53 アクションが CloudTrail により記録されます。また、これらのアクションは Amazon Route 53 API リファレンスで説明されています。例えば、`CreateHostedZone`、`CreateHealthCheck`、`RegisterDomain` の各アクションを呼び出すと、CloudTrail ログファイルにエントリが生成されます。

各イベントまたはログエントリには、リクエストの生成者に関する情報が含まれます。同一性情報は次の判断に役立ちます。

- リクエストが、ルートと IAM ユーザー認証情報のどちらを使用して送信されたか。
- リクエストがロールまたはフェデレーションユーザーの一時的なセキュリティ認証情報を使用して行われたかどうか。
- リクエストが別の AWS サービスによって行われたかどうか。

詳細については、「CloudTrail userIdentity エレメント」を参照してください。

イベント履歴での Route 53 イベントの表示

CloudTrail では、[イベント履歴] に最近のイベントが表示されます。Route 53 API リクエストのイベントを表示するには、コンソールの上部にあるリージョンセレクターで米国東部 (バージニア北部)

を選択する必要があります。詳細については、AWS CloudTrail ユーザーガイドの「CloudTrail イベント履歴でのイベントの表示」を参照してください。

Route 53 のログファイルエントリを理解する

証跡は、指定した Amazon S3 バケットにイベントをログファイルとして配信するように設定できます。CloudTrail のログファイルは、単一か複数のログエントリを含みます。イベントはあらゆるソースからの単一のリクエストを表し、リクエストされたアクション、アクションの日時、リクエストのパラメータなどの情報が含まれます。CloudTrail ログファイルは、パブリック API コールの順序付けられたスタックトレースではないため、特定の順序では表示されません。

`eventName` 要素は、発生したアクションを示します。(CloudTrail Logs では、アクション名の最初の文字が大文字ですが、ドメイン登録アクションでは小文字です。例えば、`UpdateDomainContact` は口グ内で `updateDomainContact` としてあらわされます。CloudTrail は、すべての Route 53 API アクションをサポートしています。次の例では、次に示したアクションを表す CloudTrail ログエントリを確認できます。

- AWS アカウントに関連付けられているホストゾーンを一覧表示する
- ヘルスチェックの作成
- 2 つのレコードの作成
- ホストゾーンの削除
- 登録済みドメインの情報の更新
- Route 53 VPC Resolver アウトバウンドエンドポイントを作成する


```
{
    "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"
        }
    ]
}
```

Amazon Route 53 のトラブルシューティング

このページでは、Amazon Route 53 の以下のトラブルシューティングトピックについて説明します。

1. ドメインの非可用性:
   - 登録者の E メールの未確認、DNS サービス転送の問題、ネームサーバー設定の誤り、ホストゾーンの削除など、ドメインがインターネットで使用できない一般的な理由を理解します。
2. ドメインの停止:
   - ドメインの停止 (ClientHold ステータス) の原因と、期限切れのドメイン、登録者の E メール変更の未検証、支払い処理の問題など、ドメインの停止を解除する方法について説明します。
3. 失敗したドメインオペレーション:
   - 無効な連絡先情報に起因する登録、移管、更新、連絡先更新の問題など、ドメインオペレーションの失敗を解決します。
4. 失敗したドメイン転送:
   - Route 53 へのドメイン転送が失敗した一般的な理由について説明します。例えば、転送の未承認、無効な認可コード、国際化ドメイン名の問題などです。
5. DNS 設定が有効になっていない:
   - DNS リゾルバーのキャッシュ、ネームサーバーの更新の誤り、同じ名前の複数のホストゾーンなど、DNS 設定の変更がまだ反映されていない状況をトラブルシューティングします。
6. エラー「Server Not Found」:
   - レコードの欠落、レコード値の誤り、リソースを利用できないなど、ブラウザで「Server Not Found」エラーの解決策を見つけます。
7. S3 バケットへのトラフィックのルーティング:
   - ウェブサイトホスティングのために設定された Amazon S3 バケットにトラフィックをルーティングしようとした際の問題を解決します。
8. 請求に関する問題:
   - 同じホストゾーンに対して 2 回請求される、ドメインの複数の請求書、 AWS アカウント が閉鎖または完全に閉鎖されたときのドメイン登録の懸念など、一般的な請求シナリオを理解します。

トピック

- マイドメインはインターネットで使用できません
- マイドメインは停止しています (ステータスは ClientHold です)
- マイドメインオペレーションの失敗
- マイドメインを Amazon Route 53 に移管できませんでした
- DNS 設定を変更したが、変更が適用されていない
- ブラウザに「Server not found」エラーが表示されます
- ウェブサイトホスティングのために設定された Amazon S3 バケットにトラフィックをルーティングすることができません
- 同じホストゾーンで 2 回請求がありました
- ドメインに対して複数の請求書を受け取った
- AWS アカウントが閉鎖または完全に閉鎖され、ドメインが Route 53 に登録されている

マイドメインはインターネットで使用できません

ドメインをインターネットで使用できない最も一般的な理由をいくつか示します。

トピック

- 新しいドメインを登録しましたが、確認メールのリンクが選択されていません
- Amazon Route 53 にドメイン登録を移管したが、DNS サービスを移管しなかった
- ドメイン登録を移管し、ドメイン設定で誤ったネームサーバーを指定した
- DNS サービスをまず移管したが、ドメイン登録を移管する前に十分に時間を置かなかった
- Route 53 がドメインのインターネットトラフィックをルーティングするために使用しているホストゾーンを削除した
- ドメインは停止しています

新しいドメインを登録しましたが、確認メールのリンクが選択されていません

お客様が新しいドメインを登録するとき、ICANN の要件に従って、当社は登録者の連絡先の E メールアドレスが有効であることを確認する必要があります。確認を得るために、当社はリンクを含む E メールを送信します。最上位ドメインに応じて、リンクの選択には 3 ~ 15 日かかります。この期間の経過後、リンクは機能しなくなります。

割り当てられた時間内に E メール内のリンクを選択しない場合、ICANN ではドメインを停止する必要があるため、インターネットでは使用できません。登録者の連絡先に確認 E メールを再送信する方法については、「承認および確認メールの再送信」を参照してください。

Amazon Route 53 にドメイン登録を移管したが、DNS サービスを移管しなかった

前のレジストラが、ドメイン登録と一緒に無料 DNS サービスを提供していた場合、ドメイン登録を Route 53 に移管したときにレジストラが DNS サービスの提供を止めることがあります。次の手順を実行し、これが問題であることを特定します。また、そうである場合、解決します。

Route 53 にドメイン登録を移管した後、前のレジストラが DNS サービスを取り消した場合、サービスを復元するには

1. 前のレジストラに連絡し、ドメインの DNS サービスが取り消されたことを確認します。そうである場合、ドメインの DNS サービスを復元するには、推奨順に以下の 3 つの最も簡単な方法があります。

   - 前のレジストラが有料 DNS サービスを提供しているなら、ドメインの古い DNS レコードとネームサーバーを使用して DNS サービスを復元するように伝えます。
   - 前のレジストラが、ドメイン登録なしの有料 DNS サービスを提供していない場合は、ドメイン登録を元に戻し、ドメインの 古い DNS レコードとネームサーバーを使用して DNS サービスを復元することができるかどうかを確認します。
   - 前のレジストラにドメイン登録を戻すことができても、DNS レコードが保存されていない場合は、ドメイン登録を元に戻してドメインに以前割り当てられたのと同じネームサーバーのセットを取得できるかどうかを確認します。それが可能な場合は、古い DNS レコードを自分で再度作成する必要があります。ただし、これを行うとすぐにドメインを再度使用できるようになります。

   前のレジストラがこれらのオプションのいずれをも行うことができない場合は、ステップ 2 に進んでください。

   > **Important**
   >
   > Route 53 にドメインを移管したときに指定したネームサーバーを使用して DNS サービスを復元できない場合は、この手順の残りのステップを完了後、ドメインがインターネットで再び利用可能になるまでに最長で 2 日間かかります。DNS リゾルバーは一般的

にドメインのネームサーバーの名前を 24 ~ 48 時間キャッシュするので、すべての DNS リゾルバーが新しいネームサーバーの名前を取得するのにも同じ時間が必要です。

2. 新しい DNS サービス、例えば、Route 53 を選択してください。
3. 新しい DNS サービスから提供される方法を使用して、ホストゾーンとレコードを作成します。

   a. ドメインと同じ名前があるホストゾーンを作成します (例: example.com)。
   b. レコードを作成するために前のレジストラから取得したゾーンファイルを使用します。

   新しい DNS サービスとして Route 53 を選択すると、ゾーンファイルをインポートすることでレコードを作成できます。詳細については、「ゾーンファイルをインポートしてレコードを作成する」を参照してください。
4. 新しいホストゾーンのネームサーバーを取得します。DNS サービスとして Route 53 を選択する場合、「パブリックホストゾーンに対するネームサーバーの取得」を参照してください。
5. ドメインのネームサーバーをステップ 4 で取得したネームサーバーに変更します。詳細については、「ドメインのネームサーバーおよびグルーレコードの追加あるいは変更」を参照してください。

ドメイン登録を移管し、ドメイン設定で誤ったネームサーバーを指定した

Amazon Route 53 にドメイン登録を移管するとき、ドメインに指定する設定の 1 つは、ドメインの DNS クエリに応答するネームサーバーのセットです。これらのネームサーバーは、ドメインと同じ名前のホストゾーンにあります。ホストゾーンには、www.example.com のウェブサーバーの IP アドレスなど、ドメインのトラフィックをどのようにルーティングするかについての情報があります。

ドメインと同じ名前を持つ複数のホストゾーンがある場合は特に起こりやすいことですが、ネームサーバーを間違ったホストゾーンに誤って指定することがあります。ドメインが正しいホストゾーンのネームサーバーを使用していることを確認するには、また必要に応じてドメインのネームサーバーを更新するには、以下の手順を実行します。

Important

Route 53 にドメインを移管したとき、間違ったネームサーバーを指定した場合、ドメインのネームサーバーを修正した後、DNS サービスが完全に復元されるまで最長 2 日間かかります。これは、インターネットの DNS リゾルバーは通常 2 日ごとにしかネームサーバーをリクエストせず、応答をキャッシュするからです。

ホストゾーンのネームサーバーを取得するには

1. ドメインに別の DNS サービスを使用している場合、ホストゾーンのネームサーバーを取得するために DNS サービスが提供する方法を使用します。次の手順に進みます。

   ドメインの DNS サービスとして Route 53 を使用している場合は、 にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [Hosted Zones] を選択します。
3. [Hosted Zones (ホストゾーン)] ページで、ホストゾーンのラジオボタン (名前ではない) を選択します。

   > **Important**
   >
   > 同じ名前のホストゾーンが複数ある場合は、正しいホストゾーンのネームサーバーを取得していることを確認します。
4. 右ペインの [Name Servers (ネームサーバー)]に表示されている 4 つのサーバー名を書き留めます。

ドメインが正しいネームサーバーを使用していることを確認するには

1. ドメインに別の DNS サービスを使用している場合は、 にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。

   Route 53 を使用している場合、次のステップに進みます。
2. ナビゲーションペインで [Registered Domains] を選択します。
3. 設定を編集するドメインの名前を選択します。
4. [Add or Edit Name Servers] を選択します。
5. 前の手順で取得したネームサーバーのリストと、[Edit Name Servers for] ドメイン名ダイアログボックスにリスト表示されているネームサーバーとを比較します。
6. ここにリスト表示されているネームサーバーが、前の手順で取得したネームサーバーと一致しない場合は、ここのネームサーバーを変更し、[Update] を選択します。

DNS サービスをまず移管したが、ドメイン登録を移管する前に十分に時間を置かなかった

Amazon Route 53 または別の DNS サービスに DNS サービスを移管したとき、新しい DNS サービスでネームサーバーを使用するためにドメインレジストラでドメインの構成を更新しました。

ドメインへのリクエストに応答する DNS リゾルバーは、一般的に 24 ~ 48 時間ネームサーバーの名前をキャッシュします。ドメインの DNS サービスを変更して 1 つの DNS サービスのネームサーバーから別の DNS サービスのネームサーバーに置き換える場合、DNS リゾルバーが新しいネームサーバー、つまり新しい DNS サービスを使用し始めるまでに最長で 48 時間かかることがあります。

このため、DNS サービスを移管した直後にドメイン移管すると、ドメインがインターネットで使用できなくなる場合があります。

1. ドメインの DNS サービスを移管しました。
2. DNS リゾルバーが新しい DNS サービスのネームサーバーを使い始める前に Route 53 にドメインを移管しました。
3. ドメインが Route 53 に移管されるとすぐに、前のレジストラがドメインの DNS サービスを取り消しました。
4. DNS リゾルバーは今も古い DNS サービスにクエリをルーティングしていますが、トラフィックをルーティングする方法を示すレコードはもうありません。

古い DNS サービスのネームサーバーのキャッシュの有効期限が切れると、DNS は新しい DNS サービスの使用を開始します。残念ながら、そのプロセスを加速させる方法はありません。

Route 53 がドメインのインターネットトラフィックをルーティングするために使用しているホストゾーンを削除した

Route 53 がドメインの DNS サービスである場合に、ドメインのインターネットトラフィックをルーティングするために使用されているホストゾーンを削除すると、そのドメインはインターネットで利用できなくなります。これは、ドメインが Route 53 に登録されているかどうかに関係ありません。

> **Important**
>
> ドメインのインターネットサービスを復元するには、最大で 48 時間かかります。

Route 53 がドメインのインターネットトラフィックをルーティングするために使用しているホストゾーンを削除した場合に、インターネットサービスを復元するには

1. ドメインと同じ名前の別のホストゾーンを作成します。詳細については、「パブリックホストゾーンの作成」を参照してください。
2. 削除したホストゾーンにあったレコードを再作成します。詳細については、「レコードを使用する」を参照してください。
3. Route 53 が新しいホストゾーンに割り当てたネームサーバーの名前を取得します。詳細については、「パブリックホストゾーンに対するネームサーバーの取得」を参照してください。
4. ステップ 3 で取得したネームサーバーを使用するようにドメイン登録を更新します。

   - Route 53 に登録されているドメインに関しては、「ドメインのネームサーバーおよびグルーレコードの追加あるいは変更」を参照してください。
   - ドメインが他のドメインレジストラに登録されている場合、そのレジストラが提供する方法を使用して、新しいネームサーバーを使用するようにドメイン登録を更新します。
5. ネームサーバーの TTL が、削除されたホストゾーンのネームサーバーの名前をキャッシュした再帰的なリゾルバーに対して経過するのを待ちます。TTL が経過した後、ブラウザまたはアプリケーションがドメインまたはそのいずれかのサブドメインの DNS クエリを送信すると、再帰的なリゾルバーは、新しいホストゾーンの Route 53 ネームサーバーにクエリを転送します。詳細については、「Amazon Route 53 によりドメインのトラフィックをルーティングする方法」を参照してください。

   ネームサーバーの TTL は、ドメインの TLD に応じて最長 48 時間とすることができます。

ドメインは停止しています

ドメインは停止措置によってインターネット上で使用できなくなる場合があります。詳細については、「マイドメインは停止しています (ステータスは ClientHold です)」を参照してください。

マイドメインは停止しています (ステータスは ClientHold です)

Amazon Route 53 がドメインを停止すると、ドメインはインターネットで使用できなくなります。次のいずれかの方法を使用して、ドメインが停止されたかどうかを判断できます。

- Route 53 コンソールの [Registered Domains (登録済みドメイン)] ページで、ページの下部にある [Alerts] テーブルでドメイン名を見つけます。[Status] 列の値が [clientHold] であれば、ドメインは停止中です。

- ドメインの WHOIS クエリを送信します。[Domain Status] の値が [clientHold] であれば、ドメインは停止中です。WHOIS コマンドは多くのオペレーティングシステムで利用でき、多くのウェブサイトでウェブアプリケーションとしても利用できます。

また、ドメインの停止中は、ドメインの登録者の連絡先である E メールアドレスに E メールが送信されるのが一般的です。ただし、ドメインの停止が裁判所の命令に基づくものである場合、裁判所によって登録者の連絡先への通知が禁じられる場合があります。

インターネットのドメインを再度使用可能にするには、停止を解除する必要があります。以下にドメインが停止される理由と停止を解除する方法を示します。

> **Note**
>
> ドメインの停止を解除するためにサポートが必要な場合は、 AWS サポートに無料でお問い合わせください。詳細については、「ドメイン登録の問題に関する AWS サポートへのお問い合わせ」を参照してください。

トピック

- 新しいドメインを登録しましたが、確認メールのリンクが選択されていません
- ドメインの自動更新を無効にしていてドメインの有効期限が切れた
- 登録者の連絡先の E メールアドレスを変更しましたが、新しい E メールアドレスが有効であることを確認しませんでした
- AWS 適正使用ポリシーの違反によりドメインが停止されました
- 裁判所命令によってドメインを停止しました

新しいドメインを登録しましたが、確認メールのリンクが選択されていません

ドメインを AWS に初めて登録する場合、ICANN では、登録者の連絡先の E メールアドレスが有効であることを確認する必要があります。確認を得るために、当社はリンクを含む E メールを送信します。最上位ドメインに応じて、リンクの選択には 3 ~ 15 日かかります。この期間の経過後、リンクは機能しなくなります。

> **Note**
>
> 既に Amazon Route 53 でドメインを 1 つ以上登録していて、登録者の連絡先に同じ E メールアドレスを使用している場合、確認用 E メールは送信されません。

割り当てられた時間内に E メール内のリンクを選択しない場合、ICANN ではドメインを停止する必要があるため、インターネットでは使用できません。登録者の連絡先に確認 E メールを再送信する方法については、「承認および確認メールの再送信」を参照してください。メールアドレスが有効であることが確認されると、ドメインの停止は自動的に解除されます。

ドメインの自動更新を無効にしていてドメインの有効期限が切れた

ドメインの自動更新が有効な場合 (新しいドメインまたは転送されたドメインのデフォルト値)、ドメインの登録は有効期限が切れる直前に自動的に更新されます。自動更新を無効にすると、ドメイン登録の有効期限が近づいていることを、登録者の連絡先の E メールアドレスにリマインダー E メールを送信します。これらのメールの送信は、ドメインの有効期限が切れる 45 日前に開始されます。

ドメインの自動更新を無効にし、ドメインの登録期間を手動で延長しない場合、ドメインは有効期限終了日に停止されるのが一般的です。一部のドメインのレジストリーは、有効期限の終了前であってもドメインを削除するので注意してください。

有効期限の切れたドメインについては、「ドメインの登録の更新」を参照してください。

登録者の連絡先の E メールアドレスを変更しましたが、新しい E メールアドレスが有効であることを確認しませんでした

登録者の連絡先の E メールアドレスを、以前に確認していないアドレスに変更する場合、ICANN の規則では、登録者の連絡先の E メールアドレスが有効であることを確認する必要があります。確認を得るために、当社はリンクを含む E メールを送信します。最上位ドメインに応じて、リンクの選択には 3 ~ 15 日かかります。この期間の経過後、リンクは機能しなくなります。

TLD レジストリで許可されている時間内に E メール内のリンクを選択しない場合、ICANN ではドメインを停止する必要があるため、インターネットでは使用できません。登録者の連絡先に確認 E メールを再送信する方法については、「承認および確認メールの再送信」を参照してください。メールアドレスが有効であることが確認されると、ドメインの停止は自動的に解除されます。

AWS 適正使用ポリシーの違反によりドメインが停止されました

AWS の適正利用規約の違反を理由にドメインが停止された場合、ドメインの登録者の連絡先にメールで通知が送信されます (AWS アカウントが不正使用のために既に停止されている場合、通知 E メールは送信されません) 。

停止に異議がある場合は、trustandsafety@support.aws.com に E メールを送信します。

裁判所命令によってドメインを停止しました

裁判所命令によってドメインが停止された場合、裁判所命令が解除されるまでドメインの停止は解除されません。裁判所命令の有効性に異議を唱えるには、trustandsafety@support.aws.com に E メールを送信し、該当するドキュメントをアタッチします。

マイドメインオペレーションの失敗

ドメインオペレーションが失敗した場合のトラブルシューティングのヒントをいくつか示します。オペレーションには、登録、移管、更新、連絡先更新があります。

連絡先情報が無効であるため、ドメインオペレーションが失敗しました

ドメインオペレーションが無効な連絡先情報に関するエラーで失敗した場合、指定した連絡先情報はレジストリの検証要件を満たしていません。

この問題を解決するには、すべての連絡先情報が正しくフォーマットされていることを確認します。

- 名前 – 名前に有効な文字のみが含まれ、正しくフォーマットされていることを確認します。
- アドレス – アドレス形式が国の郵便番号標準と一致していることを確認します。
- 電話番号 – 国に適した国際形式を使用します。
- 識別フィールド – 識別番号を必要とするドメインの場合は、指定された国に対して形式が正しいことを確認してください。

連絡先情報を修正したら、ドメインオペレーションを再試行してください。さまざまな最上位ドメインの具体的な要件については、「Amazon Route 53 に登録できる最上位ドメイン」を参照してください。

マイドメインを Amazon Route 53 に移管できませんでした

ドメイン移管がすでに失敗しているか、拒否されている場合は、このセクションを使用して失敗を診断し、解決します。

> **Note**
>
> アクティブな移管中の問題の防止については、「Route 53 の一般的な移管問題の防止」を参照してください。

トピック

- 認可 E メールのリンクが選択されていません
- 現在のレジストラから取得した認可コードが無効である
- .es ドメインを Amazon Route 53 に移管する際に「Parameters in request are not valid」エラーを受信する
- Amazon Route 53 に移管する国際化ドメイン名の、Punycode で記述されたリストはありますか?
- 一般的な移管エラーメッセージ

認可 E メールのリンクが選択されていません

一部の最上位ドメインでは、レジストリは登録者の連絡先に移管を承認する必要があります。このような場合は、リンクを含む E メールを送信します。最上位ドメインに応じて、リンクの選択には 5 ~ 15 日かかります。この期間の経過後、リンクは機能しなくなります。

割り当てられた時間内に E メール内のリンクを選択しない場合、転送はキャンセルされます。登録者の連絡先に承認 E メールを再送信する方法については、「承認および確認メールの再送信」を参照してください。

現在のレジストラから取得した認可コードが無効である

ドメインを Amazon Route 53 に移管するようリクエストした一方で、承認の E メールが送られて来ない場合は、Route 53 コンソールのステータスページを参照してください。レジストラから取得した移管認可コードが無効であることがステータスページに示される場合、次のステップに従ってください。

1. ドメインの現在のレジストラに連絡して、新しい認可コードを申請します。次の点を確認します。

   - 新しい認可コードが有効である期間はどれぐらいか。コードの有効期限が切れる前にドメインの移管をリクエストする必要があります。
   - 新しい認可コードは無効なコードとは異なります。同じコードの場合には、現在のレジストラに認可コードを更新するよう申請してください。

2. ドメインを移管する別のリクエストを送信します。詳細については、「ドメイン登録の Amazon Route 53 への移管」トピックの「ステップ 5: 移管をリクエストする」を参照してください。

.es ドメインを Amazon Route 53 に移管する際に「Parameters in request are not valid」エラーを受信する

.es ドメインを Route 53 に転送しようとしたときに Amazon Route 53 が「リクエスト中のパラメータが無効です 」エラーを返した場合は、登録者の連絡先に必要なすべての ID フィールドが正しくフォーマットされていることを確認します。.es ドメインの場合、レジストリには、登録者が個人か会社かに応じて特定の識別情報が必要です。また、管理連絡先、技術連絡先、請求連絡先の連絡先タイプが Person であることを確認します。登録者の連絡先のみが会社になることができます。必須フィールドの詳細については、「」を参照してくださいAmazon Route 53 に登録できる最上位ドメイン。

Amazon Route 53 に移管する国際化ドメイン名の、Punycode で記述されたリストはありますか?

新しいドメイン名の登録時、あるいは、ホストゾーンとレコードの作成時には、a ~ z 以外の文字 (フランス語の ç など)、他のアルファベット文字 (キリル文字やアラビア文字など)、および中国語、日本語、韓国語の文字を指定できます。Amazon Route 53 では、これらの国際化ドメイン名 (IDN) を、Unicode 文字を ASCII 文字列として表現する Punycode で格納します。

IDN の Route 53 への移管中にエラーが発生した場合は、記述に Punycode を使用して、もう一度試してください。詳細については、「国際化ドメイン名の形式」を参照してください。

一般的な移管エラーメッセージ

ドメイン転送が失敗すると、通常、Route 53 コンソールまたは E メールでエラーメッセージが表示されます。最も一般的なエラーメッセージとその解決方法は次のとおりです。

「レジストリによって移管が拒否されました」

このエラーは、ドメインレジストリがいくつかの理由で移管をブロックした場合に発生します。最も一般的な原因は次のとおりです。

- ドメインが 60 日間の ICANN ルールを満たしていません。ICANN では、初回登録または登録者の連絡先変更から 60 日以内に移管をブロックする必要があります。
- ドメインでは、現在のレジストラで移管ロックが有効になっています。
- このドメイン
  は、clientTransferProhibited、serverTransferProhibited、pendingDelete、pendingTr
  などの移管を禁止するステータスです。

この問題を解決するには、現在のレジストラで以下を確認してください。

- ドメインが登録日から 60 日以上経過していることを確認します。登録者の連絡先情報を最近変更した場合は、その変更から 60 日間待機する必要がある場合があります。一部のレジストラではこの制限をオプトアウトできるため、このオプションが利用可能な場合は現在のレジストラにお問い合わせください。
- 移管ロックまたはドメインロックを無効にして、ドメインをロック解除します。
- ドメインのステータスで移管が許可されていることを確認します。ドメインのステータスを確認するには、WHOIS ルックアップを使用するか、現在のレジストラにお問い合わせください。

「無効な認可コード」または「認証コードが正しくありません」

このエラーは、入力した認可コード (EPP コードまたは移管コードとも呼ばれます) が無効であることを意味します。これは、コードの有効期限が切れた場合、誤って入力された場合、または現在のレジストラから取得されなかった場合に発生する可能性があります。

この問題を解決するには:

- 現在のレジストラに連絡して、新しい認可コードを申請します。コードの有効期限が切れる前に移管を完了できるように、コードのアクティブ期間を必ず確認してください。
- 新しいコードを受け取ったら、以前のコードと異なることを確認します。同じ場合は、レジストラに認可コードの更新または再生成を依頼してください。
- 大文字または小文字、数字、特殊文字など、指定されたとおりにコードを入力していることをダブルチェックします。

「移管承認 E メールが受信されませんでした」または「承認タイムアウト」

このエラーは、転送確認 E メールの承認リンクを必要な期間 (通常は 5 日) 内に選択しない場合に発生します。一部の最上位ドメインでは、レジストリにこの認可ステップが必要です。

承認 E メールが届かなかった場合、または期限に間に合わなかった場合は、以下を確認してください。

- 迷惑 E メールフォルダを確認します。移管承認 E メールは、E メールプロバイダーによってフィルタリングされることがあります。
- メールボックスが満杯ではなく、E メールの配信を妨げかねないストレージ制限がないことを確認します。
- E メールプロバイダーに、不明な送信者からの受信メールをフィルタリングするポリシーがあるかどうかを確認します。
- 登録者の E メールアカウントにアクセスできることおよび、E メールアドレスがまだアクティブであることを確認します。

必要に応じて、別の移管をリクエストする前に、現在のレジストラで連絡先情報を更新します。認可 E メールの再送信については、「承認および確認メールの再送信」を参照してください。

「ドメインがロックされている」または「移管禁止」

このエラーは、ドメインでロックが有効になっていて移管できないことを示します。ほとんどのレジストラは、不正な移管を防ぐためのセキュリティ対策として、デフォルトでドメインロックを有効にしています。

この問題を解決するには、現在のレジストラでアカウントにログインし、ドメインロックまたは移管ロック設定を無効にします。正確な手順はレジストラによって異なりますが、通常、これらの設定はドメイン管理またはセキュリティ設定にあります。これらの設定の検索にヘルプが必要な場合は、現在のレジストラにお問い合わせください。

「連絡先情報の検証が必要」

このエラーは、ドメインの連絡先情報を最近変更した場合に発生します。ICANN ルールでは、不正な移管を防ぐため、連絡先変更後 60 日間経過してからドメインを移管します。

この問題を解決するには 2 つのオプションがあります。

- 連絡先の変更日から 60 日間待機し、移管を再試行します。

- 現在のレジストラに連絡して、現在の連絡先情報を確認してください。レジストラによっては、アイデンティティを検証できる場合、60 日間の制限をオプトアウトできる場合があります。

> **Note**
>
> ここに記載されていないエラーメッセージが表示された場合は、 AWS サポートに連絡して、正確なエラーテキストを含めてください。サポートチームは、お客様個々の状況に合わせて移管問題の診断と解決を支援します。

DNS 設定を変更したが、変更が適用されていない

DNS 設定を変更したのに変更がまだ適用されていない場合の一般的な理由を次に示します。

トピック

- 過去 48 時間以内に DNS サービスを Amazon Route 53 に移管したため、DNS はまだ前の DNS サービスを使用している
- DNS サービスを Amazon Route 53 に移管したが、ドメインレジストラでネームサーバーを更新しなかった
- DNS リゾルバーがまだレコードの古い設定を使用している
- 同じ名前のホストゾーンが複数あり、ドメインに関連付けられていないホストゾーンを更新しました

過去 48 時間以内に DNS サービスを Amazon Route 53 に移管したため、DNS はまだ前の DNS サービスを使用している

DNS サービスを Amazon Route 53 に移管したとき、ドメインのレジストラが提供する方法を使用して、前の DNS サービスのネームサーバーを、Route 53 の 4 つのネームサーバーに置き換えました。

> **Note**
>
> この部分を実行したかどうか不明な場合は、DNS サービスを Amazon Route 53 に移管したが、ドメインレジストラでネームサーバーを更新しなかった を参照してください。

ドメインレジストラは通常ネームサーバーに 24 ~ 48 時間の TTL (有効期限) を使用します。つまり、DNS リゾルバーがドメインのネームサーバーを取得すると、ドメインの現在のネームサーバーに別のリクエストを送信するより最長 48 時間前まで、その情報を使用します。過去 48 時間以内に DNS サービスを Route 53 に移管して DNS 設定を変更した場合、ドメインのトラフィックをルーティングするのに古い DNS サービスをまだ使用する DNS リゾルバーもあります。

DNS サービスを Amazon Route 53 に移管したが、ドメインレジストラでネームサーバーを更新しなかった

ドメインのレジストラには、ドメインの DNS サービスのネームサーバーなど、ドメインについてのさまざまな情報があります。通常、ドメインレジストラは DNS サービスでもあるため、ドメインに関連付けられるネームサーバーはレジストラに属します。これらのネームサーバーは、例えばドメインのウェブサーバーの IP アドレスなど、ドメインのトラフィックをルーティングする方法に関する情報をどこで得るかを DNS に伝えます。

DNS サービスを Amazon Route 53 に移管する場合、ドメインに関連付けられているネームサーバーを変更するためにドメインレジストラによって提供されている方法を使用する必要があります。通常、レジストラによって提供されたネームサーバーを、ドメインのために作成したホストゾーンに関連付けられる 4 つの Route 53 ネームサーバーに置き換えます。

ドメインに新しいホストゾーンとレコードを作成し、前の DNS サービスに使用していたのとは異なる設定を指定しており、さらに、DNS がまだ古いリソースへルーティングしている場合、ドメインレジストラでネームサーバーを更新していなかった可能性があります。レジストラが Route 53 ホストゾーンのネームサーバーを使用しているかどうかを判断するには、また必要に応じてドメインのネームサーバーを更新するには、次の手順を実行します。

ホストゾーンのネームサーバーを取得し、ドメインレジストラでネームサーバーの設定を更新するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. ナビゲーションペインで [Hosted Zones] を選択します。
3. [Hosted Zones (ホストゾーン)] ページで、ホストゾーンのホストゾーン名 (ラジオボタンではない) を選択します。

> **Important**
>
> 同じ名前のホストゾーンが複数ある場合は、正しいホストゾーンのネームサーバーを取得していることを確認します。

4. [Record name (レコード名)] リストに、[Name Servers (ネームサーバー)] に記載されている 4 つのサーバー名を書き留めます。
5. ドメインのレジストラによって提供された方法を使用して、ドメインのネームサーバーのリストを表示します。
6. ドメインのネームサーバーが、ステップ 4 で取得したネームサーバーと一致する場合、ドメイン設定は正しくなされています。

   ドメインのネームサーバーが、ステップ 4 で取得したネームサーバーと一致しない場合、Route 53 ネームサーバーを使用するようにドメインを更新します。
7.

> **Important**
>
> ドメインのネームサーバーを Route 53 ホストゾーンからのネームサーバーに変更するとき、変更が反映されて Route 53 が DNS サービスになるまでに最長 2 日間かかります。これは、インターネットの DNS リゾルバーは通常 2 日ごとにしかネームサーバーをリクエストせず、応答をキャッシュするからです。

DNS リゾルバーがまだレコードの古い設定を使用している

レコードの設定を変更したのに、トラフィックがウェブサイトのウェブサーバーなどの古いリソースにルーティングされている場合、考えられる原因の 1 つは、DNS がキャッシュした以前の設定を保持していることです。それぞれのレコードには、DNS リゾルバーがレコードにウェブサーバーの IP アドレスなどの情報をキャッシュしておく長さ (秒単位) を指定した TTL (有効期限) の値があります。TTL で指定された時間が経過するまで、DNS リゾルバーは DNS クエリに応じて古い値を返し続けます。レコードでの TTL について知りたい場合は、以下の手順を実行します。

> **Note**
>
> エイリアスレコードの場合、TTL はレコードがトラフィックをルーティングする AWS リソースによって決まります。詳細については、「エイリアスレコードと非エイリアスレコードの選択」を参照してください。

レコードの TTL を表示するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。
2. [Hosted Zones] ページで、レコードを含むホストゾーンの名前を選択します。
3. レコードのリストで、TTL の値を知りたいレコードを探し、[TTL] の列の値を確認します。

> **Note**
>
> 今 TTL を変更しても、変更がより早く反映されることにはなりません。DNS リゾルバーには既にキャッシュされた値があり、古い設定で指定されている時間が経過するまでは、新しい設定は反映されません。

同じ名前のホストゾーンが複数あり、ドメインに関連付けられていないホストゾーンを更新しました

同じアカウントを使用するか、複数のアカウントを使用して、同じ名前のホストゾーンを複数作成できます。Route 53 がドメインのインターネットトラフィックをルーティングするために使用するホストゾーンを指定するには、そのホストゾーンの 4 つの Route 53 ネームサーバーを取得し、それらのネームサーバーを使用するようにドメイン登録を更新します。

あるホストゾーンのレコードを追加、変更、または削除しても、ドメイン登録で別のホストゾーンのネームサーバーが使用されている場合、DNS クエリへの Route 53 レスポンスには変更が反映されません。ドメイン登録で、レコードを更新したホストゾーンのネームサーバーが使用されているかどうかを判断するには、次のタスクを実行します。

1. ドメイン登録に関連付けられているネームサーバーを特定します。「ネームサーバーまたはグルーレコードの追加または変更」を参照してください。

2. ステップ 1 で取得したネームサーバーと、レコードを更新したホストゾーン Route 53 に割り当てられたネームサーバーを比較します。「パブリックホストゾーンに対するネームサーバーの取得」を参照してください。

ドメイン登録のネームサーバーが、レコードを更新したホストゾーンのネームサーバーと一致しない場合は、次の 2 つのオプションがあります。

ドメイン登録に現在関連付けられているホストゾーンのレコードを変更する (推奨)

ドメイン登録に現在関連付けられていないホストゾーンで行った変更を書き留めます。次に、ドメイン登録に関連付けられているホストゾーンに移動し、同じ変更を加えます。変更がほぼ即座に有効になるため、この方法が推奨されます。詳細については、「レコードの編集」を参照してください。

異なるネームサーバーを使用するようにドメイン登録を更新する

更新したホストゾーンのネームサーバーを使用するようにドメイン登録を変更します。

> **Important**
>
> ドメイン登録に関連付けられているネームサーバーを変更した場合、ドメインはインターネット上で最長 2 日間利用できなくなります。これは、DNS リゾルバーは通常、ネームサーバーの名前を 2 日間キャッシュするためです。リゾルバーキャッシュに関する情報など、DNS の動作の概要については、「Amazon Route 53 によりドメインのトラフィックをルーティングする方法」を参照してください。

ドメイン登録に関連付けられているネームサーバーを変更すると、基本的にはドメインの DNS サービスが変更されます。ドメインが現在使用中かどうかに応じて、次の 2 つのオプションがあります。

- ドメインが使用中の場合は、「Route 53 を使用中のドメインの DNS サービスにする」を参照してください。
- ドメインが現在アクティブでない場合は、次のタスクを実行します。
  1. ドメインへのトラフィックのルーティングに使用するホストゾーンのネームサーバーを取得します。「パブリックホストゾーンに対するネームサーバーの取得」を参照してください。
  2. ステップ 1 でネームサーバーを取得したホストゾーンで、NS レコードが同じ 4 つのネームサーバーを使用していることを確認します。そうでない場合は、NS レコードを更新します。「レコードの編集」を参照してください。

3. ステップ 1 で取得したネームサーバーを使用するようにドメイン登録を更新します。「ネームサーバーまたはグルーレコードの追加または変更」を参照してください。

ブラウザに「Server not found」エラーが表示されます

ドメイン (example.com) またはサブドメイン (www.example.com) を参照しようとすると、ブラウザに「Server not found」エラーが表示される場合、よくある理由は以下の通りです。

トピック

- ドメインまたはサブドメインの名前にレコードを作成しなかった
- レコードを作成したが、誤った値を指定した
- トラフィックをルーティングしているリソースが使用できない

ドメインまたはサブドメインの名前にレコードを作成しなかった

ドメインまたはサブドメインにレコードを作成しない場合、ブラウザにだれかがその名前を入力しても、DNS はどこでトラフィックをルーティングすればいいのか判断できません。詳細については、「レコードを使用する」を参照してください。

レコードを作成したが、誤った値を指定した

レコードを作成するとき、ウェブサーバーの IP アドレスや CloudFront がウェブディストリビューションに割り当てたドメインの名前など、誤った値を指定してしまうことがよくあります。レコードが存在するのに「Server not found」エラーが引き続き表示される場合は、値が正しいことを確認するようお勧めします。

トラフィックをルーティングしているリソースが使用できない

レコードが、ウェブサーバーなど使用できないリソースを指定している場合、ブラウザは「Server not found」エラーを返します。トラフィックをルーティングしているリソースのステータスを確認することをお勧めします。

ウェブサイトホスティングのために設定された Amazon S3 バケットにトラフィックをルーティングすることができません

ウェブサイトのホスティングのために Amazon S3 バケットを設定した場合、バケットの名前は、バケットにトラフィックをルーティングするのに使用するレコードと同じ名前にする必要があります。例えば、example.com のトラフィックを、ウェブサイトホスティングのため設定されている S3 バケットにルーティングするには、バケットの名前を example.com にする必要があります。

ウェブサイトホスティング用に設定された S3 バケットにトラフィックをルーティングするが、バケットの名前が Amazon Route 53 コンソールのエイリアスターゲットリストに表示されない場合、またはエイリアスレコードをプログラムで作成しようとして、 AWS SDKs の 1 つである Route 53 API から InvalidInput エラーが発生した場合は AWS CLI、以下 AWS Tools for Windows PowerShell を確認してください。

- バケットの名前は example.com、www.example.com などのレコードの名前と完全に一致しています。
- S3 バケットはウェブサイトホスティングのため正しく設定されています。詳細については、Amazon Simple Storage Service ユーザーガイドの Amazon S3 を使用して静的ウェブサイトをホスティングするを参照してください。

同じホストゾーンで 2 回請求がありました

作成後 12 時間以内に削除されたホストゾーンの料金は請求されません。12 時間後、当社は直ちにホストゾーンについて標準月額料金を請求します。ホストゾーンの月額料金は、日割り計算されません (ドメイン登録時に自動的に作成されたホストゾーンについては同じ料金が適用されます)。

月末最終日、例えば 1 月 31 日にホストゾーンを作成すると、1 月の料金が 2 月の料金とともに 2 月の請求書に記載される場合があります。Amazon Route 53 はタイムゾーンに協定世界時 (UTC) を使用してホストゾーンの作成時を識別するので注意してください。

ドメインに対して複数の請求書を受け取った

サブスクリプションにサインアップし、前払い料金で登録料、転送料金、または更新料を支払うと、一意の請求書が生成されます。この請求書は、支払いトランザクションが失敗した場合でも請求コンソールに残ります。関連する請求明細項目は、請求コンソールの [サービスごとの料金明細] タブの [レジストラグローバル] サブセクションの下に [[x] 数量] として表示されます。

免除される請求書を表示するには、次の手順を実行します。

請求コンソールで免除される請求書を表示するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/costmanagement/ で AWS Billing and Cost Management コンソールを開きます。
2. ナビゲーションペインで [請求] を選択します。
3. [請求書] を選択すると、免除される請求書の詳細が表示されます。

[請求コンソール] で正常な支払いと返金を表示するには、次のステップを実行します。

正常に処理された支払いまたは返金を確認するには

1. ナビゲーションペインで [支払い] を選択します。
2. トランザクションタブを選択すると、完了したすべてのトランザクションのトランザクションテーブルが表示されます AWS。

AWS アカウントが閉鎖または完全に閉鎖され、ドメインが Route 53 に登録されている

AWS アカウントを閉鎖した場合、またはアカウントが閉鎖または完全に閉鎖された場合、ドメインは削除プロセスを実行します。

1. アカウントが閉鎖され、ドメインは今後 5 日間、毎日停止されることをお知らせします。
2. ドメインが停止されると、以下が実行されます。
   - レジストラが Amazon Registrar の場合、ドメインは 30 日後に削除されることをお知らせします。詳細については、「レジストラとドメインに関するその他の情報の検索」を参照してください。
   - レジストラが Gandi の場合、アカウントが完全に閉鎖された後、ドメインを Gandi にリリースすることをお知らせします。
3. 30 日間の待機後、アカウントで Amazon Registrar に登録されているすべてのドメインを削除して、更新を送信します。
4. アカウントが完全に閉鎖されるときに、アカウントの Gandi で登録されているすべてのドメインを Gandi にリリースします。

ドメインを復元できる期間中にアカウントを再開する場合は、ドメインの停止を解除するか、ドメインが削除されたが復元できる可能性があることを通知します。詳細については、「Amazon Route 53 に登録できる最上位ドメイン」を参照してください。

> **Note**
>
> アカウントを閉鎖してから 90 日が経過すると、再開できなくなります。詳細については、「AWS アカウント管理ガイド」の「アカウントの解約」を参照してください。

詳細については、「ドメイン登録の問題に関する AWS サポートへのお問い合わせ」を参照してください。

Amazon Route 53 サーバーの IP アドレス範囲

Amazon Web Services (AWS) は、その現在の IP アドレス範囲を JSON 形式で公開します。ファイアウォールまたはセキュリティグループで送信元 IP アドレスに基づいて着信トラフィックを制限する場合は、設定で該当する IP アドレス範囲のトラフィックが許可されていることを確認してください。

Route 53 の現在の IP アドレス範囲を表示するには、ip-ranges.json をダウンロードし、ファイルで次の値を検索します。

- `"service": "ROUTE53"`
- `"service": "ROUTE53_HEALTHCHECKS"`
- `"service": "ROUTE53_HEALTHCHECKS_PUBLISHING"`

AWS リソースの IP アドレスの詳細については、のAWS 「IP アドレス範囲」を参照してくださいAmazon Web Services 全般のリファレンス。

Route 53 ネームサーバーの IP アドレス範囲

`"service": "ROUTE53"` – これらの IP アドレス範囲は、Route 53 ネームサーバーによって使用されます。1 つ以上のドメインの DNS サービスとして Route 53 を使用中で、`dig` または `nslookup` コマンドを使用して Route 53 ネームサーバーにクエリを実行できるようにする場合は、許可された IP アドレス範囲のリストに、これらの範囲を追加します。

> **Note**
>
> Route 53 ネームサーバーの IP アドレスは静的です。

Route 53 ヘルスチェックの IP アドレス範囲

`"service": "ROUTE53_HEALTHCHECKS"` – これらの IP アドレス範囲は、Route 53 ヘルスチェッカーによって使用されます。Route 53 ヘルスチェックを使用してネットワーク上のリソースの正常性をチェックする場合は、許可された IP アドレス範囲のリストにこれらの範囲を追加します。

> **Note**
>
> ヘルスチェッカーの IP アドレス範囲を変更することはめったにありません。これらの範囲の更新がないか、ip-ranges.json ファイルをモニタリングします。

ヘルスチェックの IP アドレスの詳細については、「Amazon Route 53 のヘルスチェックができるようにルーターとファイアウォールのルールを設定する」を参照してください。

プレフィックスリストの参照

「プレフィックスリスト」は、セキュリティグループを設定するために使用できる 1 つまたは複数の CIDR ブロックエントリを含むセットです。Amazon EC2 インスタンスのルールのルーターとファイアウォールは、Route 53 ヘルスチェックが使用する IP アドレスからのインバウンドトラフィックを許可する必要があります。プレフィックスリストへの参照を使用すると、ルール内の CIDR ブロックの管理を簡素化できます。複数のルールにわたって同じ CIDR を頻繁に指定する場合、各ルールで同じ CIDR を繰り返し参照する代わりに、これらの CIDR を 1 つのプレフィックスリストで管理できます。CIDR ブロックを削除する必要がある場合は、影響を受ける個々のルールから CIDR を削除する代わりに、プレフィクスリストから CIDR フロックのエントリを削除することができます。プレフィックスリストの全般的な情報については、「Amazon VPC ユーザーガイド」の「マネージドプレフィックスリストを使用して CIDR ブロックをグループ化する」を参照してください。

AWSマネージドプレフィックスリストは、 AWS サービスの IP アドレス範囲のセットです。 AWS マネージドプレフィックスリストは によって作成および管理 AWS され、 AWS アカウントを持つすべてのユーザーが使用できます。 AWSマネージドプレフィックスリストを作成、変更、共有、または削除することはできません。

AWSマネージドプレフィックスリストの詳細については、「Amazon VPC ユーザーガイド AWS」の「マネージドプレフィックスリストの使用」を参照してください。

Route 53 ヘルスチェックの内部 IP アドレス範囲

`"service": "ROUTE53_HEALTHCHECKS_PUBLISHING"` – Route 53 は、これらの IP アドレス範囲を内部的にのみ使用します。許可された範囲のリストにこれらの範囲を追加する必要はありません。

Amazon Route 53 リソースのタグ付け

タグは、 AWS リソースに割り当てるラベルです。タグはそれぞれ、1 つのキーと 1 つの値で構成されており、どちらもユーザーが定義します。例えば、キーが "domain" で値が "example.com" というタグを付けることができます。タグには多くの目的があります。一般的な用途の 1 つは、Amazon Route 53 のコストを分類して追跡することです。Route 53 ホストゾーン、ドメイン、ヘルスチェックにタグを適用すると、 はコスト配分レポートを CSV ファイルとして AWS 生成します。このレポートには、タグ別にグループ化された使用状況とコストが表示されます。自社のカテゴリ、たとえばコストセンター、アプリケーション名、所有者を表すタグを適用すると、複数のサービスにわたってコストを分類することができます。タグを使ったコスト配分の詳細については、AWS Billing ユーザーガイドのコスト配分タグの使用を参照してください。

最良の結果を得るには、 でタグエディタを使用します AWS マネジメントコンソール。タグエディタは、タグを作成および管理するための一元的な方法を提供します。詳細については、AWS マネジメントコンソールの開始方法のタグエディタの使用を参照してください。Route 53 コンソールを使用して、いくつかのリソースにタグを適用することもできます。

- ヘルスチェック 詳細については、ヘルスチェックの名前付けとタグ付けを参照してください。
- Route 53 VPC Resolver インバウンドエンドポイント – 詳細については、「」を参照してくださいインバウンドエンドポイントを作成または編集するときに指定する値。
- Resolver アウトバウンドエンドポイント – 詳細については、「アウトバウンドエンドポイントを作成または編集するときに指定する値」を参照してください。
- Resolver ルール— 詳細については、「ルールを作成または編集するときに指定する値」を参照してください。
- ホストゾーン – 詳細については、「ホストゾーンの使用」を参照してください。

> **Note**
>
> Resolver エンドポイントの料金は、VPC Resolver ネットワークインターフェイスごとに割り当てられます。VPC Resolver ネットワークインターフェイスにタグを付けることはできないため、Resolver エンドポイントではタグベースのコスト配分はサポートされていません。VPC Resolver の料金については、「Amazon Route 53 の料金」を参照してください。

Route 53 API を使用してリソースにタグを適用することもできます。詳細については、Amazon Route 53 API リファレンスのトピック「Amazon Route 53 API actions by function (関数別の Route 53 API アクション)」の中のタグに関連するアクションを参照してください。

チュートリアル

このセクションでは、次のチュートリアルについて説明します。

Route 53 をサブドメインの DNS サービスとして使用する

Amazon Route 53 を新しいサブドメインや既存のサブドメインの DNS サービスとして使用し、親ドメインでは引き続き別の DNS サービスを使用する方法を説明します。

レイテンシーベースルーティングへ移行する

Route 53 で標準ルーティングからレイテンシーベースのルーティングに徐々に移行し、利用可能な最小レイテンシーの AWS エンドポイントにユーザーを誘導する方法について説明します。

加重レコードとレイテンシーレコードを組み合わせると、フルコントロールとロールバック機能を備えたスムーズでリスクの低い移行が可能になります。

レイテンシーベースルーティングに別のリージョンを追加する

新しい AWS リージョンを追加し、トラフィックを新しいリージョンに徐々に移行することで、レイテンシーベースのルーティング設定を拡張します。

リージョン内の複数の Amazon EC2 インスタンスにトラフィックをルーティングする

レイテンシーレコードと加重レコードの組み合わせを使用して、特定の AWS リージョン内の複数の Amazon EC2 インスタンスにトラフィックをルーティングします。

100 を超える加重レコードを管理する

加重エイリアスレコードと加重レコードのツリーを作成して、100 を超えるエンドポイントにトラフィックを誘導する方法について説明します。

重み付けを利用した、耐障害性のある複数のレコードでの応答

複数のレコードを含む DNS レスポンスに重み付けを行う方法を理解し、複数のエンドポイント間で耐障害性と負荷分散を提供します。

これらのチュートリアルでは、Route 53 のルーティングポリシー、加重レコード、レイテンシーベースのルーティングを効果的に活用して、DNS 管理とトラフィックルーティングを最適化するのに役立つ、さまざまなユースケースとシナリオについて説明します。

トピック

- 親ドメインを移行しないで Amazon Route 53 をサブドメインの DNS サービスとして使用する
- Amazon Route 53 でレイテンシーベースルーティングへ移行する
- Amazon Route 53 のレイテンシーベースルーティングに別のリージョンを追加する
- Amazon Route 53 でレイテンシーおよび加重レコードを使用して、リージョン内の複数の Amazon EC2 インスタンスにトラフィックをルーティングする
- Amazon Route 53 で 100 を超える加重レコードを管理する
- Amazon Route 53 での重み付けを利用した、耐障害性のある複数のレコードでの応答

親ドメインを移行しないで Amazon Route 53 をサブドメインの DNS サービスとして使用する

Amazon Route 53 によって、サブドメインの DNS を柔軟に管理できるため、親ドメイン全体を移行することなく、その機能を活用できます。

別の DNS サービスプロバイダーでホストされている親ドメインを維持しながら、新しいサブドメインを作成するか既存のサブドメインを Route 53 に移行することができます。

Route 53 を使用した新しいサブドメインの作成:

1. 新しいサブドメインのホストゾーンを作成します。
2. サブドメインに必要な DNS レコード (例えば、A、CNAME、MX) をホストゾーンに追加します。
3. ホストゾーンに割り当てられた Route 53 ネームサーバーを取得します。
4. Route 53 ネームサーバーを指す、サブドメインの NS (ネームサーバー) レコードを追加して、親ドメインの DNS 設定を更新します。

既存のサブドメインを Route 53 に移行する:

1. サブドメインのホストゾーンを作成します。
2. サブドメインの現在の DNS 設定を既存の DNS サービスプロバイダーから取得します。
3. ホストゾーンに対応する DNS レコードを追加します。
4. ホストゾーンに割り当てられた Route 53 ネームサーバーを取得します。
5. Route 53 ネームサーバーを指す、サブドメインの NS レコードを追加して、親ドメインの DNS 設定を更新します。

これらのステップに従って、既存のプロバイダーで親ドメインの DNS 設定を維持しながら、サブドメインのヘルスチェック、ルーティングポリシー、トラフィックフロー管理などの Route 53 の高度な機能を活用できます。

トピック

- 親ドメインを移行しないで Amazon Route 53 を DNS サービスとして使用するサブドメインを作成する
- 親ドメインを移行しないでサブドメインの DNS サービスを Amazon Route 53 に移行

親ドメインを移行しないで Amazon Route 53 を DNS サービスとして使用するサブドメインを作成する

別の DNS サービスから親ドメインの移行を行わずに、DNS サービスとして Amazon Route 53 を使用するサブドメインを作成できます。

このプロセスには、以下の基本的なステップがあります。

1. この手順がユースケースに適用されるかどうかを判断します。
2. サブドメインの Route 53 ホストゾーンを作成します。
3. Route 53 ホストゾーンに、新しいサブドメインのレコードを追加します。
4. API のみ: すべての Route 53 DNS サーバーに変更が反映されたことを確認します。

> **Note**
>
> 現在、変更が反映されたことを確認するには、GetChange API アクションを使用する方法しかありません。通常、変更は 60 秒以内にすべての Route 53 ネームサーバーに反映されます。

5. サブドメインのネームサーバーレコードを追加して、親ドメインの DNS サービスを更新します。

サブドメインの作成に使用する手順の決定

これらのステップでは、まれなタスクについて説明します。ドメインの DNS サービスとして Route 53 を既に使用していて、サブドメインのトラフィックをルーティングする場合は、「」を参照してくださいサブドメインのトラフィックのルーティング。

この手順は、example.com などのドメインに別の DNS サービスを使用していて、www.example.com などのドメインの新しいサブドメインの DNS サービスとして Route 53 の使用を開始する場合にのみ使用します。

新しいサブドメインのホストゾーンを作成する

親ドメインを移行せずに Amazon Route 53 を新しいサブドメインの DNS サービスとして使用するには、まずサブドメインのホストゾーンを作成します。Route 53 は、サブドメインデータをこのゾーンに保存します。

Route 53 コンソールを使用したホストゾーンの作成方法については、「パブリックホストゾーンの作成」を参照してください。

レコードの作成

Amazon Route 53 コンソールまたは Route 53 API を使用してレコードを作成できます。作成するレコードは、「」で説明されているように、サブドメインを Route 53 に委任した後に DNS が使用するレコードになりますサブドメインのネームサーバーレコードで DNS サービスを更新する。

> **Important**
>
> Route 53 ホストゾーンに追加のネームサーバー (NS) レコードまたは認可開始 (SOA) レコードを作成しないでください。既存の NS レコードと SOA レコードを削除しないでください。

Route 53 コンソールを使用してレコードを作成するには、「レコードを使用する」を参照してください。Route 53 API を使用してレコードを作成するには、「ChangeResourceRecordSets」を参照してください。詳細については、Amazon Route 53 API リファレンスの「ChangeResourceRecordSets」を参照してください。

変更のステータスを確認する (API のみ)

新しいホストゾーンの作成や、レコードの変更は、Route 53 DNS サーバーに伝達されるまでに時間がかかります。レコードの作成に ChangeResourceRecordSets を使用した場合、GetChange アクションを使用して、変更が反映されたかどうかを判断できます (ChangeResourceRecordSets は ChangeId の値を返します。これは次の GetChange リクエストに含めることができます。コンソールを使用してレコードを作成した場合は、ChangeId を使用できません)。詳細については、Amazon Route 53 API リファレンスの「GET GetChange」を参照してください。

> **Note**
>
> 通常、変更は 60 秒以内にすべての Route 53 ネームサーバーに反映されます。

サブドメインのネームサーバーレコードで DNS サービスを更新する

Amazon Route 53 レコードへの変更が広まったら (「」を参照変更のステータスを確認する (API のみ))、サブドメインの NS レコードを追加して親ドメインの DNS サービスを更新します。これにより、サブドメインが Route 53 に委任されます。例えば、example.com が別の DNS サービスを使用していて、Route 53 で test.example.com を作成した場合は、example.com の DNS を test.example.com の NS レコードで更新します。

サブドメインのネームサーバーレコードで DNS サービスを更新するには

1. DNS サービスから提供される方法を使用して、親ドメインのゾーンファイルをバックアップします。
2. Route 53 コンソールで、Route 53 ホストゾーンのネームサーバーを取得します。

   a. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。

   b. ナビゲーションペインで [Hosted zones (ホストゾーン)] をクリックします。

   c. [Hosted Zones (ホストゾーン)] ページで、ホストゾーンのラジオボタン (名前ではない) を選択し、[View details (詳細を表示)] を選択します。

   d. ホストゾーンの詳細ページで、[Hosted zone details (ホストゾーンの詳細)] を選択します。

   e. [Name Servers] (ネームサーバー) で一覧表示されている 4 つのサーバー名を書き留めます。

   または、`GetHostedZone` アクションを使用できます。詳細については、Amazon Route 53 API リファレンスの「GetHostedZone」を参照してください。
3. DNS サービスの メソッドを使用して、親ドメインのゾーンファイルにサブドメインの NS レコードを追加します。これらの NS レコードで、ステップ 1 で作成したホストゾーンにリンクされた 4 つの Route 53 ネームサーバーを指定します。

> **Important**
>
> 親ドメインのゾーンファイルに Start of Authority (SOA) のレコードを追加しないでください。サブドメインは Route 53 を使用するため、親の DNS サービスはサブドメインを制御しません。
> DNS サービスがサブドメインの SOA レコードを追加した場合は、それを削除します。親ドメインの SOA レコードを削除しないでください。

親ドメインを移行しないでサブドメインの DNS サービスを Amazon Route 53 に移行

別の DNS サービスから親ドメインを移行せずに、Amazon Route 53 を DNS サービスとして使用するサブドメインを移行できます。

このプロセスには、以下の基本的なステップがあります。

1. この手順がユースケースに適用されるかどうかを判断します。
2. サブドメインの Route 53 ホストゾーンを作成します。
3. 親ドメインの現在の DNS サービスプロバイダから現在の DNS 設定を取得します。
4. Route 53 ホストゾーンに、サブドメインのレコードを追加します。
5. API のみ: すべての Route 53 DNS サーバーに変更が反映されたことを確認します。

> **Note**
>
> 現在、変更が反映されたことを確認するには、GetChange API アクションを使用する方法しかありません。通常、変更は 60 秒以内にすべての Route 53 ネームサーバーに反映されます。

6. サブドメインのネームサーバーレコードを追加して、親ドメインの DNS サービスプロバイダの DNS 設定を更新します。

サブドメインの作成に使用する手順の決定

このトピックの手順では、まれなタスクを実行する方法について説明します。ドメインの DNS サービスとして Route 53 を既に使用していて、www.example.com などのサブドメインのトラフィック

をリソースにルーティングする場合は、「」を参照してくださいサブドメインのトラフィックのルーティング。

この手順を使用するのは、ドメイン (example.com など) で別の DNS サービスを使用していて、そのドメインの既存のサブドメイン (www.example.com など) で Route 53 を DNS サービスとして使い始める場合に限ります。

サブドメイン用のホストゾーンの作成

親ドメインを移行せずにサブドメインを別の DNS サービスから Amazon Route 53 に移行するには、まずサブドメインのホストゾーンを作成します。Route 53 は、サブドメイン情報をこのホストゾーンに保存します。

Route 53 コンソールを使用したホストゾーンの作成方法については、「パブリックホストゾーンの作成」を参照してください。

DNS サービスプロバイダーから現在の DNS 設定を取得

現在の DNS サービスプロバイダーに連絡して、現在の DNS 設定をリクエストします。ゾーンファイルまたはレコードリストを取得する方法については、現在の DNS サービスプロバイダーにお問い合わせください。これは、Route 53 をサブドメインの DNS サービスとして設定するための基盤として使用できます。

リクエストの内容と形式は、現在の DNS サービスプロバイダーによって異なります。理想的には、現在の設定内のすべてのレコードを含むゾーンファイルを提供します。これらのレコードは、ドメインとサブドメインのトラフィックをルーティングする方法を DNS に伝えます。たとえば、レコードは、ドメイン名のトラフィックをデータセンターのウェブサーバー、Amazon EC2 インスタンス、または CloudFront ディストリビューションにルーティングできます。ゾーンファイルを取得できる場合は、編集して Amazon Route 53 に移行しないレコードを削除できます。次に、残りのレコードを Route 53 ホストゾーンにインポートします。これにより、プロセスが大幅に簡素化されます。

レコードの作成

現在の DNS サービスプロバイダーのレコードを出発点として使用し、サブドメイン用に作成した Amazon Route 53 ホストゾーンで一致するレコードを作成します。これらのレコードは、「」で説明されているように、サブドメインを Route 53 に委任した後に DNS が使用するレコードになりますサブドメインのネームサーバーレコードで DNS サービスを更新する。

> **Important**
>
> Route 53 ホストゾーンに追加のネームサーバー (NS) レコードまたは Start of Authority (SOA) レコードを作成しないでください。また、既存の NS レコードと SOA レコードを削除しないでください。

Route 53 コンソールを使用してレコードを作成するには、「レコードを使用する」を参照してください。Route 53 API を使用してレコードを作成するには、「ChangeResourceRecordSets」を参照してください。詳細については、Amazon Route 53 API リファレンスの「ChangeResourceRecordSets」を参照してください。

変更のステータスを確認する (API のみ)

新しいホストゾーンの作成や、レコードの変更は、Route 53 DNS サーバーに伝達されるまでに時間がかかります。レコードの作成に ChangeResourceRecordSets を使用した場合、GetChange アクションを使用して、変更が反映されたかどうかを判断できます (ChangeResourceRecordSets は ChangeId の値を返します。これは次の GetChange リクエストに含めることができます。コンソールを使用してレコードを作成した場合は、ChangeId を使用できません)。詳細については、Amazon Route 53 API リファレンスの「GET GetChange」を参照してください。

> **Note**
>
> 通常、変更は 60 秒以内にすべての Route 53 ネームサーバーに反映されます。

サブドメインのネームサーバーレコードで DNS サービスを更新する

Amazon Route 53 レコードへの変更が反映された後 (「変更のステータスを確認する (API のみ)」を参照)、サブドメインの NS レコードを追加して、親ドメインの DNS サービスを更新します。これにより、サブドメインが Route 53 に委任されます。たとえば、example.com が別の DNS サービスでホストされており、test.example.com を Route 53 に移行するとします。Route 53 が新しいホストゾーンに割り当てた NS レコードを使用して、example.com の DNS サービスを更新する必要があります。

サブドメインのネームサーバーレコードで DNS サービスを更新するには

1. DNS サービスから提供される方法を使用して、親ドメインのゾーンファイルをバックアップします。

2. 以前の DNS プロバイダーでネームサーバーの TTL 設定を変更できる場合は、設定を 900 秒に変更します。これにより、クライアントリクエストが古いネームサーバーを使用してドメイン名を解決しようとする時間が制限されます。現在の TTL が 172800 秒 (2 日) の場合、リゾルバーとクライアントが DNS レコードのキャッシュを停止するまで 2 日間待つ必要があります。TTL 設定の有効期限が切れたら、前のプロバイダーに保存されているレコードを安全に削除し、Route 53 にのみ変更を加えることができます。
3. Route 53 コンソールで、Route 53 ホストゾーンのネームサーバーを取得します。

   a. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/route53/ で Route 53 コンソールを開きます。

   b. ナビゲーションペインで [Hosted zones (ホストゾーン)] をクリックします。

   c. [Hosted Zones (ホストゾーン)] ページで、ホストゾーンのラジオボタン (名前ではない) を選択し、[View details (詳細を表示)] を選択します。

   d. ホストゾーンの詳細ページで、[Hosted zone details (ホストゾーンの詳細)] を選択します。

   e. [Name Servers] (ネームサーバー) で一覧表示されている 4 つのサーバー名を書き留めます。

   または、`GetHostedZone` アクションを使用できます。詳細については、Amazon Route 53 API リファレンスの「GetHostedZone」を参照してください。
4. 親ドメインの DNS サービスが提供する メソッドを使用して、サブドメインの NS レコードをゾーンファイルに追加します。NS レコードにサブドメイン名を付けます。値には、ステップ 2 で作成したホストゾーンにリンクされた 4 つの Route 53 ネームサーバーを指定します。DNS サービスによって用語は異なります。これを行う方法については、 サポートに問い合わせる必要がある場合があります。

   > **Important**
   >
   > 親ドメインのゾーンファイルに Start of Authority (SOA) のレコードを追加しないでください。サブドメインは Route 53 を使用するため、親ドメインの DNS サービスはサブドメインに関する権限を保持していません。
   > DNS サービスが自動的にサブドメインの SOA レコードを追加した場合、サブドメインのレコードを削除します。ただし、親ドメインの SOA レコードは削除しないでください。

DNS リゾルバーの変更が反映されるまでに 48 時間以上かかる場合があります。この間も、DNS リゾルバーは親ドメインの DNS サービスのネームサーバーで応答する可能性があります。また、クライアントコンピュータのキャッシュにサブドメインの以前のネームサーバーが残っている場合もあります。

5. レジストラのドメインの TTL 設定の有効期限が切れたら (ステップ 2 を参照) 、親ドメインのゾーンファイルからこれらのレコードを削除します。

   - Route 53 に追加したレコードについては、「レコードの作成」を参照してください。
   - DNS サービスの NS レコード。NS レコードの削除が完了すると、ゾーンファイル内の NS レコードのみがステップ 4 で作成したレコードになります。

Amazon Route 53 でレイテンシーベースルーティングへ移行する

レイテンシーベースのルーティングを使用すると、Amazon Route 53 は利用可能な最小レイテンシーの AWS エンドポイントにユーザーを誘導できます。例えば、`www.example.com` のような DNS 名を、米国東部 (オハイオ) リージョンや欧州 (アイルランド) リージョンでホストされている ELB Classic、Application、または Network Load Balancer、Amazon EC2 インスタンス、Elastic IP アドレスなどと関連付けることができます。Route 53 DNS サーバーは、過去数週間のネットワークの状態に基づいて、特定のユーザーをどのリージョンのどのインスタンスに割り当てるかを決定します。おそらくロンドンのユーザーは、欧州 (アイルランド) インスタンスに割り当てられ、シカゴのユーザーは、米国東部 (オハイオ) インスタンスに割り当てられるでしょう。Route 53 では、A や AAAA のレコードに対してエイリアスの作成がサポートされているのと同様に、A、AAAA、TXT、CNAME などのレコードに対してレイテンシーベースルーティングがサポートされます。

> **Note**
>
> ユーザーとリソース間のレイテンシーに関するデータは、ユーザーと AWS データセンター間のトラフィックに完全に基づいています。 AWS リージョンでリソースを使用していない場合、ユーザーとリソース間の実際のレイテンシーはレイテンシ AWS ーデータと大きく異なる場合があります。これは、リソースが AWS リージョンと同じ都市にある場合でも当てはまります。

スムーズで低リスクな移行を行うために、加重レコードとレイテンシーレコードを併用して、標準のルーティングから各ステージで完全な制御とロールバックを行う機能を備えたレイテンシーベースルーティングへと徐々に移行することができます。米国東部 (オハイオ) リージョンの Amazon EC2 インスタンスで現在ホストされている、www.example.com の例を考えてみましょう。インスタンスには Elastic IP アドレス W.W.W.W が関連付けられています。該当する場合に米国東部 (オハイオ) リージョンへのトラフィックのルーティングを継続しながら、米国西部 (北カリフォルニア) リージョン (Elastic IP X.X.X.X) や欧州 (アイルランド) リージョン (Elastic IP Y.Y.Y.Y) にある追加の Amazon EC2 インスタンスにユーザーのルーティングを開始するとします。example.com の Route 53 ホストゾーンは、A というタイプと、W.W.W.W という値 (IP アドレス) を持つ www.example.com のレコードを既に保持しています。

以下の例を完了すると、2 つの加重エイリアスレコードが作成されます。

- www.example.com の既存のレコードを、米国東部 (オハイオ) リージョンの既存の Amazon EC2 インスタンスに対してトラフィックの大部分を引き続きルーティングする、加重エイリアスレコードに変更します。
- 3 つのリージョンすべてにトラフィックをルーティングするレイテンシーレコードにトラフィックのごく一部のみを最初にルーティングする、別の加重エイリアスレコードを作成します。

これらの加重エイリアスレコードの重みを更新することにより、米国東部 (オハイオ) リージョンのみにトラフィックのルーティングを行う状態から、Amazon EC2 インスタンスがある 3 つのリージョンすべてにトラフィックをルーティングする状態へと徐々に移行することができます。

レイテンシーベースルーティングへ移行するには

1. www.example.com のレコードのコピーを作成しますが、新しいドメイン名 (copy-www.example.com など) を使います。新しいレコードに、 のレコードと同じように、タイプ (A) および値W.W.W.W (www.example.com) を指定します。
2. www.example.com の既存の A レコードを更新し、加重エイリアスレコードにします。
   - [Value/Route traffic to] (値/トラフィックのルーティング先) で、[Alias to another record in this hosted zone] (このホストゾーンにある別のレコードへのエイリアス) を選択し、copy-www.example.com を指定します。
   - [Weight] (ウェイト) で、100 を指定します。

   更新が完了すると、Route 53 では、W.W.W.W という IP アドレスを持つリソースにすべてのトラフィックをルーティングするために、このレコードを引き続き使用します。

3. 各 Amazon EC2 インスタンスにレイテンシーレコードを作成します。例えば、以下のようにします。

   - 米国東部 (オハイオ)、Elastic IP アドレス `W.W.W.W`
   - 米国西部 (北カリフォルニア)、Elastic IP アドレス `X.X.X.X`
   - 欧州 (アイルランド)、Elastic IP アドレス `Y.Y.Y.Y`

   すべてのレイテンシーレコードに同じドメイン名 (`www-lbr.example.com` など) と同じタイプ (A など) を設定します。

   レイテンシーレコードの作成が終了すると、Route 53 では、ステップ 2 で更新したレコードを使用して引き続きトラフィックをルーティングします。

   たとえば、検証テスト`www-lbr.example.com`に を使用して、各エンドポイントがリクエストを受け付けることができることを確認できます。

4. `www-lbr.example.com` というレイテンシーレコードを `www.example.com` という加重レコードに追加し、対応する Amazon EC2 インスタンスに対して限られた量のトラフィックのルーティングを開始しましょう。その後、米国東部 (オハイオ) リージョンの Amazon EC2 インスタンスは両方の加重レコードからトラフィックを受け取ります。

   `www.example.com` の加重エイリアスレコードを以下の方法でもう 1 つ作成します。

   - [Value/Route traffic to] (値/トラフィックのルーティング先) で、[Alias to another record in this hosted zone] (このホストゾーンにある別のレコードへのエイリアス) を選択し、`www-lbr.example.com.` を指定します。
   - [Weight] (ウェイト) で、1 を指定します。

   変更を完了し、その変更を Route 53 サーバーに同期させると、Route 53 では、ステップ 3 でレイテンシーレコードを作成した Amazon EC2 インスタンスにトラフィックのごく一部 (1/101) のルーティングを開始します。

5. エンドポイントが着信トラフィックに応じて適切にスケーリングされることを確認できたら、必要に応じて重みを調節します。例えば、レイテンシーベースルーティングに基づいてリクエストの 10% の受信を希望する場合、重みをそれぞれ 90 と 10 に変更します。

レイテンシーレコードの作成については、「Amazon Route 53 コンソールを使用したレコードの作成」を参照してください。

Amazon Route 53 のレイテンシーベースルーティングに別のリージョンを追加する

レイテンシーベースルーティングを使用中で、新しいリージョンのインスタンスを追加する必要がある場合、「Amazon Route 53 でレイテンシーベースルーティングへ移行する」でレイテンシーベースルーティングに徐々にトラフィックを移行したのと同様の方法で、新しいリージョンにトラフィックを徐々に移行することができます。

例えば、www.example.com に対するトラフィックのルーティングにレイテンシーベースルーティングを使用し、アジアパシフィック (東京) の Amazon EC2 インスタンスを米国東部 (オハイオ)、米国西部 (北カリフォルニア)、欧州 (アイルランド) のインスタンスに追加するとします。次の手順の例では、別のリージョンにインスタンスを追加する 1 つの方法について説明します。

この例では、example.com のAmazon Route 53 ホストゾーンは既に、www-lbr.example.com のレイテンシーベースレコードにトラフィックをルーティングする www.example.com の加重エイリアスレコードを保持しています。

- 米国東部 (オハイオ)、Elastic IP アドレス W.W.W.W
- 米国西部 (北カリフォルニア)、Elastic IP アドレス X.X.X.X
- 欧州 (アイルランド)、Elastic IP アドレス Y.Y.Y.Y

加重エイリアスレコードの重みは 100 です。レイテンシーベースルーティングに移行した後、移行に使用した他の加重レコードは削除するとします。

Route 53 のレイテンシーベースルーティングに別のリージョンを追加するには

1. トラフィックのルーティングを開始する新しいリージョンと、3 つの元からあるリージョンを含む、4 つの新しいレイテンシーベースレコードを作成します。

   - 米国東部 (オハイオ)、Elastic IP アドレス W.W.W.W
   - 米国西部 (北カリフォルニア)、Elastic IP アドレス X.X.X.X
   - 欧州 (アイルランド)、Elastic IP アドレス Y.Y.Y.Y
   - アジアパシフィック (東京)、Elastic IP アドレス Z.Z.Z.Z

   すべてのレイテンシーレコードに同じ新しいドメイン名 (www-lbr-2012-04-30.example.com など) と同じタイプ (A など) を設定します。

レイテンシーレコードの作成が完了すると、Route 53 では引き続き、元の加重エイリアスレコード (www.example.com) とレイテンシーレコード (www-lbr.example.com) を使用してトラフィックをルーティングします。

www-lbr-2012-04-30.example.com レコードは、検証テストに使用できます。たとえば、各エンドポイントがリクエストを受け入れることができるようにできます。

2. 新しいレイテンシーレコードの加重エイリアスレコードを作成します。

   - ドメイン名に、既存の加重エイリアスレコードの名前 (www.example.com) を指定します。
   - [Value/Route traffic to] (値/トラフィックのルーティング先) で、[Alias to another record in this hosted zone] (このホストゾーンにある別のレコードへのエイリアス) を選択し、www-lbr-2012-04-30.example.com を指定します。
   - [Weight] (ウェイト) で、1 を指定します。

   完了すると、Route 53 では、ステップ 1 で www-lbr-2012-04-30.example.com のレイテンシーレコードを作成した Amazon EC2 インスタンスに、トラフィックのごく一部 (1/101) のルーティングを開始します。残りのトラフィックは、アジアパシフィック (東京) リージョンの Amazon EC2 インスタンスを含まない、www-lbr.example.com のレイテンシーレコードに引き続きルーティングされます。

3. エンドポイントが着信トラフィックに応じて適切にスケーリングされることを確認できたら、必要に応じて重みを調節します。たとえば、東京リージョンを含むレイテンシーレコードにリクエストの 10% がルーティングされるようにする場合、www-lbr.example.com の重みを 100 から 90 に変更し、www-lbr-2012-04-30.example.com の重みを 1 から 10 に変更します。

レコード作成についての詳細は、「Amazon Route 53 コンソールを使用したレコードの作成」を参照してください。

Amazon Route 53 でレイテンシーおよび加重レコードを使用して、リージョン内の複数の Amazon EC2 インスタンスにトラフィックをルーティングする

アプリケーションが 2 つ以上の Amazon EC2 リージョンの Amazon EC2 インスタンスで実行されていて、1 つ以上のリージョンに複数の Amazon EC2 インスタンスがある場合は、レイテンシーベースのルーティングを使用してトラフィックを正しいリージョンにルーティングし、加重レコードを使

用して、指定した重みに基づいてリージョン内のインスタンスにトラフィックをルーティングできます。

例えば、米国東部 (オハイオ) リージョンに Elastic IP アドレスを持つ Amazon EC2 インスタンスが 3 つあり、米国東部 (オハイオ) リージョンに該当するユーザーについては、3 つすべての IP にリクエストを均等に分散させたいとします。多くのリージョンに同時に同じ方法を適用できますが、他のリージョンでは Amazon EC2 インスタンスは 1 つで十分です。

Amazon Route 53 でレイテンシーと加重レコードを使用して、リージョン内の複数の Amazon EC2 インスタンスにトラフィックをルーティングするには

1. リージョン内の Amazon EC2 インスタンスの加重レコードのグループを作成します。次の点に注意してください。

   - 各加重レコードで、[Record name] (レコード名) (`us-east.example.com` など) と [Record type] (レコードタイプ) に同じ値を指定します。
   - [Value/Route traffic to] (値/トラフィックのルーティング先) で、[IP address or another value depending on the record type] (IP アドレスまたはレコードタイプに応じた別の値) を選択し、Elastic IP アドレスのいずれかの値を指定します。
   - Amazon EC2 インスタンスに均等に重みを割り当てる場合は、[Weight] (ウェイト) に同じ値を指定します。
   - 各レコードの [セット ID] に一意の値を指定します。

   加重レコード値の詳細については、加重ルーティング を参照してください。
2. その他のリージョンに複数の Amazon EC2 インスタンスがある場合、他のリージョンに対してステップ 1 を繰り返します。リージョンごとに名前に異なる値を指定します。
3. 複数の Amazon EC2 インスタンス (米国東部 (オハイオ) など) があるリージョンごとに、レイテンシーエイリアスレコードを作成します。Value/Route トラフィックで、このホストゾーンの別のレコードへのエイリアスを選択し、そのリージョンの加重レコードに割り当てたレコード名フィールド (など`us-east.example.com`) の値を指定します。
4. 1 つの Amazon EC2 インスタンスがあるリージョンごとに、レイテンシーレコードを作成します。[Record name] (レコード名) には、ステップ 3 で作成したレイテンシーエイリアスレコードに指定したものと同じ値を指定します。[Value/Route traffic to] (値/トラフィックのルーティング先) で、[IP address or another value depending on the record type] (IP アドレスまたはレコードタイプに応じた別の値) を選択し、そのリージョンの Amazon EC2 インスタンスの Elastic IP アドレスを指定します。

Amazon EC2 インスタンスへのエイリアスレコードの追加の詳細については、Amazon EC2 インスタンスへのトラフィックのルーティング を参照してください。

レコード作成についての詳細は、「Amazon Route 53 コンソールを使用したレコードの作成」を参照してください。

Amazon Route 53 で 100 を超える加重レコードを管理する

Amazon Route 53 では、加重レコードを設定することができます。特定の名前やタイプ (たとえば、名前が www.example.comで、タイプが A) に対して、最大 100 の代替応答を設定することができ、それぞれに重みを設定できます。www.example.com のクエリへ応答する場合、Route 53 DNS サーバーは、重みが設定されたランダム応答を選択し、DNS リゾルバーに返します。重みが 2 の加重レコードの値は、重みが 1 の加重レコードの値よりも平均 2 倍の頻度で返されます。

100 を超すエンドポイントにトラフィックを振り分ける場合は、加重エイリアスレコードと加重レコードのツリーを使用する方法があります。たとえば、ツリーの最初の「レベル」は最大 100 個の加重エイリアスレコードであり、それぞれが最大 100 個の加重レコードを指すことができます。Route 53 では、再帰レベルは最大で 3 まで可能であり、最大 1,000,000 個の一意の加重エンドポイントを管理することができます。

シンプルな 2 階層のツリーは以下のようになります。

加重エイリアスレコード

- 重みが 1 の www-a.example.com に対応する、www.example.com エイリアス
- 重みが 1 の www-b.example.com に対応する、www.example.com エイリアス

加重レコード

- www-a.example.com、タイプ A、値 192.0.2.1、重み 1
- www-a.example.com、タイプ A、値 192.0.2.2、重み 1

- www-b.example.com、タイプ A、値 192.0.2.3、重み 1
- www-b.example.com、タイプ A、値 192.0.2.4、重み 1

レコード作成についての詳細は、「レコードを使用する」を参照してください。

Amazon Route 53 での重み付けを利用した、耐障害性のある複数のレコードでの応答

> **Note**
>
> 複数値回答ルーティングポリシーを使用するレコードは、このチュートリアルで説明されている設定と同じように動作します。主な違いは、チュートリアルの設定により、重みを指定できる点です。これは、エンドポイントごとにキャパシティーが異なる場合に便利です。詳細については、「複数値回答ルーティング」を参照してください。

Amazon Route 53 の加重レコードには、1 つのレコードのみを関連付けることができます。すなわち、1 つの名前 (`example.com` など) と 1 種類のレコードタイプ (A など) の組み合わせのみを関連付けることができます。ただし、複数のレコードを含む DNS 応答に重み付けすることが望ましい場合もあります。

例えば、あるサービスで 8 個の Amazon EC2 インスタンスまたは Elastic IP エンドポイントを使用しているとします。そのサービスが接続をサポートしているクライアントが (多くの一般的なブラウザと同じように) 再試行を行う場合、特定のエンドポイントで障害が発生したときには、DNS 応答で複数の IP アドレスを提供することにより、そのようなクライアントに代替エンドポイントを提供します。2 つ以上のアベイラビリティーゾーンにホストされる IP を複数含む応答を設定する場合、アベイラビリティーゾーンの障害から保護することもできます。

複数のレコードでの応答は、多数のクライアント (モバイルウェブアプリケーションなど) が小規模の DNS キャッシュのセットを共有する場合などにも役に立ちます。この場合、共有するキャッシュから共通の DNS 応答を受け取る場合でも、複数のレコードでの応答により、クライアントのリクエストを複数のエンドポイントにルーティングすることができます。

このようなタイプの重み付けした複数レコードでの応答は、レコードと加重エイリアスレコードの組み合わせを使用することにより実現できます。以下に示すように、8 個のエンドポイントを、それぞれ 4 個の IP アドレスを含む 2 個の異なるリソースレコードセットにグループ化できます。

タイプ A の `endpoint-a.example.com` には、以下の値が含まれます。

- 192.0.2.1
- 192.0.2.2
- 192.0.2.128

- 192.0.2.129

タイプ A の endpoint-b.example.com には、以下の値が含まれます。

- 192.0.2.3
- 192.0.2.4
- 192.0.2.130
- 192.0.2.131

これにより、次の各グループを指し示す加重エイリアスレコードを作成することができます。

- タイプ A、重み 1 の endpoint-a.example.com に対応する、www.example.com エイリアス
- タイプ A、重み 1 の endpoint-b.example.com に対応する、www.example.com エイリアス

レコード作成についての詳細は、「レコードを使用する」を参照してください。

Amazon Route 53 のベストプラクティス

このセクションでは、以下を含む Amazon Route 53 のさまざまなコンポーネントのベストプラクティスについて説明します。

1. DNS ベストプラクティス:
   - Time to Live (TTL) 値と、応答性と信頼性のトレードオフを理解します。
   - パフォーマンス向上とコスト削減のために、可能な限り CNAME レコードの代わりにエイリアスレコードを使用します。
   - デフォルトのルーティングポリシーを設定して、すべてのクライアントが応答を受け取るようにします。
   - レイテンシーベースのルーティングを活用し、アプリケーションのレイテンシーおよび位置情報/地理的近接性ルーティングを最小限に抑えて、安定性と予測可能性を高めます。
   - 自動ワークフロー用の `GetChange` API を使用して、変更の伝播を検証します。
   - 一貫したルーティングのために親ゾーンからサブドメインを委任します。
   - 複数値回答ルーティングを使用して、大規模な単一レスポンスを回避します。
2. リゾルバーのベストプラクティス:
   - Resolver ルールとそのインバウンドエンドポイントの両方に同じ VPC を関連付けないようにすることで、ルーティングループを防止します。
   - セキュリティグループルールを実装し、接続追跡のオーバーヘッドを減らして、クエリスループットを最大化します。
   - 冗長性を確保するために、複数のアベイラビリティーゾーンに IP アドレスを持つインバウンドエンドポイントを設定します。
   - 潜在的な DNS ゾーンウォーキング攻撃に注意し、エンドポイントでスロットリングが発生した場合は AWS サポートにお問い合わせください。
3. ヘルスチェックのベストプラクティス:
   - Route 53 ヘルスチェックを最適化するための推奨事項に従って、リソースを確実にモニタリングする
4. ドメイン登録のベストプラクティス:
   - ルートユーザーの E メールにドメイン AWS アカウント を使用するのと同じ で Route 53 にドメインを登録することは避けてください。これにより、ドメインを完全に削除できる循環的な依存関係を防ぐことができます。

これらのベストプラクティスに従うことで、DNS インフラストラクチャのパフォーマンス、信頼性、セキュリティを最適化し、アプリケーションやサービスへのトラフィックの効率的かつ効果的なルーティングを実現できます。

トピック

- Amazon Route 53 DNS のベストプラクティス
- VPC Resolver のベストプラクティス
- Amazon Route 53 ヘルスチェックのベストプラクティス
- Amazon Route 53 ドメイン登録のベストプラクティス

Amazon Route 53 DNS のベストプラクティス

Amazon Route 53 DNS サービスを使用するときに最良の結果が得られるようにするには、以下のベストプラクティスに従ってください。

DNS フェイルオーバーとアプリの回復にデータプレーン機能を使用してください

ヘルスチェックを含む Route 53 のデータプレーンと Amazon アプリケーション回復コントローラー (ARC) のルーティングコントロールは、グローバルに分散されており、重大なイベント中でも 100% の可用性と機能性を実現するように設計されています。これらは互いに統合され、コントロールプレーンの機能に依存しません。コンソールを含むこれらのサービスのコントロールプレーンは、一般的に非常に信頼性が高いですが、より一元化された方法で設計されており、高可用性よりも耐久性と一貫性が優先されます。ディザスタリカバリ時のフェイルオーバーなどのシナリオでは、DNS を更新するためにデータプレーン機能を利用する、Route 53 のヘルスチェックや ARC のルーティング制御などの機能の使用をお勧めします。詳細については、「コントロールプレーンとデータプレーンの概念」、および「Creating Disaster Recovery Mechanisms Using Amazon Route 53」(ブログ: Amazon Route 53 を使用した災害回復メカニズムの作成) を参照してください。

DNS レコードの TTL 値の選択

DNS TTL とは、Route 53 に対してさらなるクエリを行わずにレコードをキャッシュできる期間を決定するために DNS リゾルバーが使用する数値 (秒単位) です。すべての DNS レコードには TTL が指定されている必要があります。TTL 値の推奨範囲は 60 ~ 172,800 秒です。

TTL の選択は、レイテンシーと信頼性、および変化に対する応答性との間のトレードオフです。レコードの TTL が短くなると、DNS リゾルバーはより頻繁にクエリを実行する必要があるため、レコードの更新が速くなります。これにより、クエリのボリューム (およびコスト) が増大し

ます。TTL を長くすると、DNS リゾルバーはキャッシュからのクエリに頻繁に応答します。これは通常、高速で、安価で、場合によってはインターネットを介したクエリを回避するため信頼性が高くなります。絶対的に正しい値は存在せず、応答性と信頼性のどちらがより重要であるかを考える価値はあります。

TTL 値を設定する際に考慮すべき事項:

- 変更が有効になるのを待つ余裕があれば、DNS レコード TTL を設定します。これは、委任 (NS レコードセット) や、MX レコードなど、ほとんど変更されない他のレコードで特に当てはまります。これらのレコードでは、より長い TTL が推奨されます。一時間 (3600 秒) から 1 日 (86,400 秒) の間が一般的な数値です。
- 高速フェールオーバーメカニズム (特にヘルスチェックされるレコード) の一部として変更する必要があるレコードについては、TTL を下回るのが適切です。このシナリオでは、TTL を 60 秒または 120 秒に設定するのが一般的です。
- 重要な DNS エントリに変更を加える場合、TTL を一時的に短くすることをお勧めします。そうすれば、必要に応じてすばやく変更、監視、ロールバックを行うことができます。変更が確定し、期待どおりに機能した後、TTL を長くすることができます。

詳しくは、「TTL (秒) 」を参照してください。

CNAME レコード

DNS 内の CNAME レコードは、あるドメイン名を別のドメイン名でポイントする手段になります。DNS リゾルバーが domain-1.example.com を解決し、domain-2.example.com を指している CNAME が見つかった場合、DNS リゾルバーは応答する前に domain-2.example.com を解決する必要があります。これらのレコードは、例えば、ウェブサイトに複数のドメイン名がある場合に一貫性を保つためなど、多くの状況で役立ちます。

ただし、DNS リゾルバーは CNAME に応答するために、より多くのクエリを作成する必要があり、レイテンシーとコストが増加します。可能であれば、Route 53 エイリアス レコードを使用するのが高速かつ安価な代替手段です。エイリアスレコードを使用すると、Route 53 は AWS リソース (ロードバランサーなど) および同じホストゾーン内の他のドメインに対して直接応答できます。

詳細については、「AWS リソースへのインターネットトラフィックのルーティング」を参照してください。

高度な DNS ルーティング

- 位置情報、地理的近接性またはレイテンシーベースのルーティングを使用する場合は、一部のクライアントが回答なしのレスポンスを受信できるようにする場合を除き、常にデフォルトを設定します。
- アプリケーションのレイテンシーを最小限に抑えるには、レイテンシーベースのルーティングを使用します。このタイプのルーティングデータは頻繁に変更されることがあります。
- ルーティングの安定性と予測可能性を確保するには、位置情報ルーティングまたは地理的近接性ルーティングを使用します。

詳細については、位置情報ルーティング、地理的近接性ルーティング、および レイテンシーに基づくルーティング を参照してください。

DNS 変更の伝播

Route 53 コンソールまたは API を使用して、レコードやホストゾーンを作成または更新する場合、変更内容がインターネット上に反映されるまでにしばらく時間がかかります。これは変更の伝播と呼ばれます。通常、伝播はグローバルに 1 分未満で到達しますが、例えば、1 つのロケーションへの同期の問題や、まれに中央コントロールプレーン内の問題など、変更に時間がかかることがあります。自動プロビジョニングワークフローを構築している場合、またはD次のワークフローステップに進む前に、変更の伝播が完了するのを待つことが重要です。DNS の変更が反映されたこと (`Status =INSYNC`) を確認するために、GetChange API を使用します。

DNS の委任

DNS で複数のレベルのサブドメインを委任する場合、常に親ゾーンから委任することが重要です。たとえば、委任している場合www.dept.example.comとすると、example.comゾーンからではなくdept.example.comゾーンからそのようにすべきです。祖父母から子ゾーンへ委任すると、一切機能しないか、動作することもありますがそれは偶然に過ぎません。詳しくは、「サブドメインのトラフィックのルーティング 」を参照してください。

DNS レスポンスのサイズ

大きなシングルレスポンスの作成は避けてください。512 バイトを超えると、多くの DNS リゾルバーは UDP ではなく TCP で再試行する必要があります。これにより、レスポンスが遅くなり、信頼性が低下する可能性があります。レスポンスを 512 バイトの限度内に保つために、8 個の健全でランダムな IPアドレス を選択する複数値のアンサールーティングを使用するようお勧めします。

詳細については、「複数値回答ルーティング」および「DNS Reply Size Test Server」を参照してください。

VPC Resolver のベストプラクティス

このセクションでは、Route 53 VPC Resolver を最適化するためのベストプラクティスと、以下のトピックについて説明します。

1. Resolver エンドポイントとのループ構成を防ぐ:
   - 同じ VPC が Resolver ルールとそのインバウンドエンドポイントの両方に関連付けられないようにすることで、ルーティングループを防止します。
   - 適切なルーティング設定を維持しながら AWS RAM 、 を使用してアカウント間で VPCs を共有します。

   詳細については、Resolver エンドポイントとのループ構成を防ぐを参照してください。
2. Resolver エンドポイントのスケーリング:
   - 接続状態に基づいてトラフィックを許可するセキュリティグループルールを実装して、接続追跡のオーバーヘッドを削減する
   - インバウンドおよびアウトバウンドの Resolver エンドポイントの推奨されるセキュリティグループルールに従って、クエリスループットを最大化します。
   - 容量が制限されないように、DNS トラフィックを生成する一意の IP アドレスとポートの組み合わせを監視します。

   詳細については、Resolver エンドポイントのスケーリングを参照してください。
3. Resolver エンドポイントの高可用性:
   - 冗長性を確保するために、少なくとも 2 つのアベイラビリティーゾーンに IP アドレスを持つインバウンドエンドポイントを指定します。
   - メンテナンスやトラフィックの急増時に可用性を確保するための追加のネットワークインターフェイスをプロビジョニングする

   詳細については、Resolver エンドポイントの高可用性を参照してください。
4. DNS ゾーンウォーキング攻撃の防止:
   - 攻撃者が DNSSEC 署名付き DNS ゾーンからすべてのコンテンツを取得しようとする潜在的な DNS ゾーンウォーキング攻撃に注意してください。
   - ゾーンウォーキングが疑われるためにエンドポイントでスロットリングが発生した場合は、AWS サポートにお問い合わせください。

   詳細については、DNS ゾーンウォーキングを参照してください。
5. Resolver エンドポイントのサブネット互換性:

- Resolver エンドポイントには、Outposts 以外のサブネットを使用することをお勧めします。
- ローカルネットワークインターフェイス (LNI) が有効になっている Outposts サブネットは、VPC Resolver エンドポイントと互換性がありません。
- VPC Resolver エンドポイント ENIs、それらの ENIs機能しなくなります。

詳細については、Resolver エンドポイントのサブネット互換性を参照してください。

これらのベストプラクティスに従うことで、VPC Resolver デプロイのパフォーマンス、スケーラビリティ、セキュリティを最適化し、アプリケーションとリソースの DNS 解決の信頼性と効率性を確保できます。

Resolver エンドポイントとのループ構成を防ぐ

同じ VPC をリゾルバールールとそのインバウンドエンドポイント (エンドポイントの直接ターゲットであるか、オンプレミス DNS サーバー経由であるかにかかわらず) に関連付けないでください。アウトバウンドエンドポイントが、同じ Resolver ルールと VPC を共有するインバウンドエンドポイントを指している場合、インバウンドエンドポイントとアウトバウンドエンドポイント間でループが生成され、クエリの伝達が継続的に発生する場合があります。

転送ルールは、 AWS Resource Access Manager () を使用して他のアカウントと共有されている他の VPCs に関連付けることができますAWS RAM。転送リゾルバールールはこの解決を変更しないため、ハブまたは中央 VPC に関連付けられたプライベートホストゾーンは引き続きクエリからインバウンドエンドポイントに解決されます。

Resolver エンドポイントのスケーリング

Resolver エンドポイントセキュリティグループは、エンドポイントを出入りするトラフィックに関する情報を収集するために接続追跡を使用します。各エンドポイントインターフェイスが追跡可能な接続には最大数の制限があり、この接続数を超える大量の DNS クエリが送られた場合は、スロットリングやクエリの損失が発生する可能性があります。接続追跡は AWS、セキュリティグループ (SGs。SG における接続追跡を使用することでトラフィックのスループットが低下しますが、追跡されていない接続を実装してオーバーヘッドを減らし、パフォーマンスを改善することができます。詳細については、「追跡されていない接続」を参照してください。

制限付きセキュリティグループルールを使用して接続追跡が強制される場合、またはクエリが Network Load Balancer (自動追跡された接続を参照) を介してルーティングされる場合、エンドポイントの IP アドレスごとの 1 秒あたりの合計最大クエリ数は 1,500 に抑えられます。

次の表に、インバウンド Resolver エンドポイントに推奨されるセキュリティグループルールを示します。

インバウンドエンドポイントの進入ルール

プロトコルのタイプ	ポート番号	送信元 IP
TCP	53	0.0.0.0/0
UDP	53	0.0.0.0/0

インバウンドエンドポイント出力ルール

プロトコルのタイプ	ポート番号	送信先 IP
TCP	すべて	0.0.0.0/0
UDP	すべて	0.0.0.0/0

次の表に、アウトバウンド Resolver エンドポイントに推奨されるセキュリティグループルールを示します。

アウトバウンドエンドポイントの進入ルール

プロトコルのタイプ	ポート番号	送信元 IP
TCP	すべて	0.0.0.0/0
UDP	すべて	0.0.0.0/0

アウトバウンドエンドポイント出力ルール

プロトコルのタイプ	ポート番号	送信先 IP
TCP	53	0.0.0.0/0
UDP	53	0.0.0.0/0

> **Note**
>
> セキュリティグループポートの要件:
>
> - インバウンドエンドポイントには、ポート 53 の TCP と UDP がネットワークから DNS クエリを受信できるようにする進入ルールが必要です。エグレスルールでは、エンドポイントがさまざまなソースポートからのクエリに応答する必要がある可能性があるため、すべてのポートを許可できます。
> - アウトバウンドエンドポイントでは、エグレスルールにおいてネットワークの DNS クエリに使用するポートで TCP および UDP アクセスを許可する必要があります。ポート 53 は最も一般的な DNS ポートですが、ネットワークが異なるポートを使用する可能性があるため、上記の例に示しています。イングレスルールでは、すべてのポートが DNS サーバーからのレスポンスに対応できます。

インバウンド Resolver エンドポイント

インバウンドリゾルバーエンドポイントを使用するクライアントの場合、IP アドレスとポートの (DNS トラフィックを生成している) 固有の組み合わせが 40,000 個を超えると、Elastic Network Interface の容量に影響が生じます。

Resolver エンドポイントの高可用性

VPC リゾルバーのインバウンドエンドポイントを作成する場合、Route 53 では、ネットワーク上の DNS リゾルバーがクエリを転送する IP アドレスを少なくとも 2 つ作成する必要があります。冗長性を確保するために、少なくとも 2 つのアベイラビリティーゾーンで IP アドレスを指定する必要があります。

複数の Elastic Network Interface エンドポイントを常時使用できるようにする場合は、必要とするネットワークインターフェイス数の他に少なくとも 1 つ余分にインターフェイスを作成し、トラフィックが急増した場合にも処理できるよう追加の容量を確保しておくことをお勧めします。また、追加のネットワークインターフェイスでメンテナンスやアップグレードなどのサービス作業を行っている間の可用性も確保できます。

詳細については、この詳細なブログ記事「Resolver エンドポイントと で DNS の高可用性を実現する方法」を参照してくださいインバウンドエンドポイントを作成または編集するときに指定する値。

DNS ゾーンウォーキング

DNS ゾーンウォーキング攻撃とは、DNSSec 署名付き DNS ゾーンからすべてのコンテンツを取得しようとすることです。VPC Resolver チームがエンドポイントで DNS ゾーンがウォークされたときに生成されたトラフィックパターンと一致するトラフィックパターンを検出すると、サービスチームはエンドポイントのトラフィックを調整します。その結果、DNS クエリのタイムアウトの割合が高くなることがあります。

エンドポイントの容量が減少し、エンドポイントが誤って調整されたと思われる場合は、https://console.aws.amazon.com/support/home#/ にアクセスしてサポートケースを作成してください。

Resolver エンドポイントのサブネット互換性

Outposts ラックでエンドポイントを作成するには、 AWS Outposts で VPC Resolver AWS を使用することをお勧めします。

> **Important**
>
> ローカルネットワークインターフェイス (LNI) が有効になっている Outposts サブネットは、VPC Resolver エンドポイントと互換性がありません。VPC Resolver エンドポイントの Elastic Network Interface (ENIs) を含むサブネットで LNI を有効にすると、それらの ENIs機能しなくなります。

この問題を回避するには:

- Resolver エンドポイントを作成する前に、ターゲットサブネットで LNI が有効になっていないことを確認します。
- Resolver エンドポイント ENIs を有効にしないでください。
- LNI エンドポイントと Resolver エンドポイントの両方が必要な場合は、それぞれに個別のサブネットを使用します。

LNI の詳細については、AWS Outposts 「 ユーザーガイド」の「ローカルネットワークインターフェイス」を参照してください。

Amazon Route 53 ヘルスチェックのベストプラクティス

可用性と回復力の高いインフラストラクチャを維持するには、効果的なヘルスチェック設定が不可欠です。Amazon Route 53 ヘルスチェックをセットアップおよび管理する際に考慮すべきいくつかのベストプラクティスを以下に示します。

1. エンドポイントのヘルスチェックを行う際に Elastic IP アドレスを使用する:
   - ヘルスチェックエンドポイントに Elastic IP アドレスを活用して、一貫したモニタリングを確保します。
   - Amazon EC2 インスタンスを使用しなくなった場合は、潜在的なセキュリティリスクやデータ侵害を避けるため、関連するヘルスチェックを忘れずに削除してください。

   詳細については、「ヘルスチェックを作成または更新するときに指定する値」を参照してください。
2. 適切なヘルスチェック間隔を設定する:
   - アプリケーションの要件とモニタリング対象リソースの重要度に基づいてヘルスチェック間隔を設定します。
   - 間隔を短くすると、障害検出が速くなりますが、Route 53 のコストが増加し、リソースに負荷がかかる可能性があります。
   - 間隔を長くすると、コストとリソースの負荷は軽減されますが、障害検出が遅れる可能性があります。

   詳細については、「高度な設定 (「エンドポイントを監視」する場合のみ)」を参照してください。
3. アラーム通知を実装する:
   - ヘルスチェックが失敗または回復したときに通知を受信するように Amazon CloudWatchalarms を設定します。
   - アプリケーションの要件とリソースの予想される動作に基づいて、適切なアラームのしきい値を設定します。
   - 通知をモニタリングおよびインシデントレスポンスプロセスと統合します。

   詳細については、「CloudWatch を使用したヘルスチェックのモニタリング」を参照してください。
4. ヘルスチェックリージョンを戦略的に活用する:
   - ユーザーとリソースの地理的分布に基づいてヘルスチェックリージョンを選択します。

- 信頼性を向上させ、リージョンの停止の影響を軽減するために、重要なリソースに複数のヘルスチェックリージョンを使用することを検討してください。

5. ヘルスチェックのログとメトリクスをモニタリングする:
   - Route 53 ヘルスチェックのログと CloudWatch メトリクスを定期的に確認し、潜在的な問題やパフォーマンスのボトルネックを特定する
   - ヘルスチェックの失敗の理由を分析し、根本的な問題を解決するための適切なアクションを実行します。
6. フェイルオーバー戦略とフェイルバック戦略を実装する:
   - Route 53 のフェイルオーバールーティングポリシーを活用して、障害発生時に正常なリソースにトラフィックを自動的にルーティングします。
   - フェイルオーバーとフェイルバックのプロセスを計画してテストし、停止や復旧中にシームレスな移行を確実に行います。

   詳細については、「DNS フェイルオーバーの設定」を参照してください。
7. ヘルスチェックを定期的に確認および更新する:
   - 必要に応じてヘルスチェックのエンドポイント、間隔、アラームしきい値を更新して、最適なモニタリングとパフォーマンスを維持します。

これらのベストプラクティスに従うことで、Route 53 ヘルスチェックを効果的に活用して リソースのヘルスと可用性をモニタリングし、アプリケーションとサービスに対して信頼性が高く高性能なインフラストラクチャを確保できます。

Amazon Route 53 ドメイン登録のベストプラクティス

Amazon Route 53 にドメインを登録するときにアカウントとドメインの復旧の問題を回避するには、以下のベストプラクティスに従います。

同じアカウントのルートユーザー E メールに Route 53 ドメインを使用しない

> **Warning**
>
> Route 53 にドメインを登録し、そのドメインを同じアカウントの AWS アカウント ルートユーザーの E メールアドレスに使用する場合は、ドメインを完全に削除できる循環依存関係を作成します。

AWS アカウント が閉鎖または停止されると、Route 53 は 5 日以内にドメイン登録を一時停止します。ドメインの停止により、ドメインのネームサーバーが解決を停止し、ドメインの E メール配信が中断されます。ルートユーザーの E メールアドレスはドメインに依存するため、パスワードリセットやアカウント復旧の E メールを受信できなくなります。ルートユーザーの E メールにアクセスしないと、サインイン、アカウントの再開、ドメインの復元を行うことはできません。ドメインが中断されたままの場合、30 日後に修復パスなしで完全に削除されます。

このシーケンスは、回復不可能な循環依存関係を作成します。

1. アカウントの閉鎖または停止により、5 日以内にドメインの停止がトリガーされます。
2. ドメインの停止により DNS 解決が停止し、E メール配信が中断されます。
3. E メール配信がないと、ルートユーザーのパスワード復旧を完了できません。
4. ルートユーザーアクセスがないと、アカウントを再開したり、ドメインを復元したりすることはできません。
5. 30 日間の停止後、ドメインは完全に削除されます。

> **Important**
>
> このシナリオを回避するには、次のいずれかの推奨アーキテクチャを使用します。
>
> - 別の にドメインを登録する AWS アカウント – 専用 AWS アカウント (AWS Organizations 管理アカウントなど) を使用して、他のアカウントのルートユーザー E メールドメインとして機能するドメインを登録します。これにより、依存アカウントが閉鎖されてもドメイン登録がアクティブのままになります。
> - 外部でホストされている E メールアドレス AWSを使用する – 登録またはホストされていないドメインのルートユーザーの E メールアドレスを選択します AWS。これにより、アカウントのステータスと E メール配信の間の依存関係がなくなります。

API リクエストを行う

トピック

- ホストゾーン、リソースレコードセット、ヘルスチェックの API リクエストの実行
- ドメイン登録と Route 53 Resolver の API リクエストの作成
- Amazon Route 53 API リクエストの署名
- 関数別の Amazon Route 53 API アクション
- Amazon Route 53 API リクエストのスロットリング

このセクションでは、2 つの Route 53 APIs にリクエストを行う方法について説明します。

- ホストゾーン、リソースレコードセット、ヘルスチェック、コスト配分タグの REST API
- ドメイン登録用の RPC APIs と Route 53 Resolver 用の RPC API

API ごとに、リクエストのコンポーネントとレスポンスの内容について説明します。また、リクエストを認証する方法についても説明します。

ホストゾーン、リソースレコードセット、ヘルスチェックの API リクエストの実行

トピック

- REST リクエスト
- REST レスポンス

このセクションでは、ホストゾーン、リソースレコードセット、ヘルスチェック、コスト配分タグを作成および管理するために Amazon Route 53 API に REST リクエストを行う方法について説明します。リクエストのコンポーネント、レスポンスの内容、リクエストの認証方法について説明します。

> **Note**
>
> ドメインを登録および管理するには、Route 53 API を使用してドメインを登録します。詳細については、「ドメイン登録と Route 53 Resolver の API リクエストの作成」を参照してください。

REST リクエスト

Amazon Route 53 REST リクエストは、RFC 2616 で定義されている HTTPS リクエストです。このセクションでは、Route 53 REST リクエストの構造について説明します。

一般的な REST アクションは、単一の HTTPS リクエストを Route 53 に送信し、レスポンスを待つことで構成されます。HTTP リクエストと同様に、Route 53 への REST リクエストには、リクエストメソッド、URI、リクエストヘッダー、場合によってはクエリ文字列またはリクエスト本文が含まれます。レスポンスには HTTP ステータスコードとレスポンスヘッダーが含まれており、レスポンス本文が含まれている場合もあります。

リクエストの URI

リクエスト URI は常にスラッシュで始まり、使用する Route 53 API のバージョン (2013-04-01 など) が続きます。URI の残りは、実行の対象である特定のリソースを示します。たとえば、新しいホストゾーンを作成するときに使用する URI を次に示します。(詳細については、「CreateHostedZone」を参照してください。)

```
/2013-04-01/hostedzone
```

リクエストタイムスタンプについて

タイムスタンプは HTTP `Date`ヘッダーまたは AWS `x-amz-date` ヘッダーで指定する必要があります (一部の HTTP クライアントライブラリでは `Date`ヘッダーを設定できません) 。`x-amz-date` ヘッダーがある場合、リクエストの認証時に `Date` ヘッダーは無視されます。

タイムスタンプは、リクエストが受信された AWS システム時刻から 5 分以内にする必要があります。これ以外の場合、リクエストは失敗し、`RequestExpired` というエラーコードが出力されます。この目的は、相手がリクエストを繰り返すことを防止することです。

日付は、 などの ISO 8601 形式で指定する必要があります`2016-03-03T19:20:25.177Z`。ISO 8601 形式の詳細については、Wikipedia の記事「ISO 8601」を参照してください。

リクエスト本文

Route 53 API アクションの多くは、リクエストの本文に XML を含める必要があります。XML は Route 53 スキーマに準拠しています。

Exampleリクエストの例

次のリクエスト例では、シンプルな XML ステートメントを使用して、参照識別子 myUniqueIdentifier を使用して example.com という名前のホストゾーンを作成します。

リクエストの XML 要素は、リストされている順序で表示する必要があります。

```
POST /2013-04-01/hostedzone HTTP/1.1
host:route53.amazonaws.com
x-amz-date:date and time of the request
authorization:AWS4-HMAC-SHA256
              Credential=AKIAIOSFODNN7EXAMPLE/date of the request in yyyymmdd format/
us-east-1/route53domains/aws4_request,
              SignedHeaders=content-length;content-type;host;user-agent;x-amz-date;x-
amz-target,
              Signature=computed signature
[Other required headers]

<?xml version="1.0" encoding="UTF-8"?>
<CreateHostedZoneRequest xmlns="https://route53.amazonaws.com/
doc/2013-04-01/">
   <Name>example.com.</Name>
   <CallerReference>myUniqueIdentifier</CallerReference>
   <HostedZoneConfig>
      <Comment>This is my hosted zone.</Comment>
   </HostedZoneConfig>
</CreateHostedZoneRequest>
```

REST レスポンス

Amazon Route 53 レスポンスは、標準の HTTP レスポンスにすぎません。一部の Route 53 アクションは、レスポンス本文の HTTP ヘッダーまたは XML の形式で Route 53 に固有の特別な情報を返します。特定のアクションの詳細については、API リファレンスの該当のトピックを参照してください。

各レスポンスには、Route 53 でリクエストをトラブルシューティングする必要がある場合に使用できるリクエスト ID が含まれています。ID は、 という名前の HTTP ヘッダーに含まれていますx-amz-request-id。リクエスト ID の例は です647cd254-e0d1-44a9-af61-1d6d86ea6b77。

次の例は、ホストゾーンを作成するリクエストに対するレスポンスを示しています。CreatedHostedZoneResponse 要素には、Route 53 識別子、ホストゾーンが関連付けられているドメイン、リファレンスの説明とコメントなど、ホストゾーンに関する情報が含まれて

います。変更リクエスト自体は、 として表示される送信時間、識別子、ステータスに関連付けられますPENDING。最も重要なのは、 にはホストゾーンに割り当てられた Route 53 ネームサーバーCreatedHostedZoneResponseが含まれています。この情報は DelegationSet要素に含まれています。

Exampleレスポンスの例

```
HTTP/1.1 201 Created
x-amz-request-id: request_id
<?xml version="1.0" encoding="UTF-8"?>
<CreateHostedZoneResponse xmlns="https://route53.amazonaws.com/doc/
2013-04-01/">
   <HostedZone>
      <Id>/hostedzone/Z1PA6795UKMFR9</Id>
      <Name>example.com.</Name>
      <CallerReference>myUniqueIdentifier</CallerReference>
      <Config>
         <Comment>This is my first hosted zone.</Comment>
      </Config>
   </HostedZone>
   <ChangeInfo>
      <Id>/change/C1PA6795UKMFR9</Id>
      <Status>PENDING</Status>
      <SubmittedAt>2010-09-10T01:36:41.958Z</SubmittedAt>
   </ChangeInfo>
   <DelegationSet>
      <NameServers>
         <NameServer>ns-2048.awsdns-64.com</NameServer>
         <NameServer>ns-2049.awsdns-65.net</NameServer>
         <NameServer>ns-2050.awsdns-66.org</NameServer>
         <NameServer>ns-2051.awsdns-67.co.uk</NameServer>
      </NameServers>
   </DelegationSet>
</CreateHostedZoneResponse>
```

エラーレスポンス

REST リクエストでエラーが発生した場合、HTTP レスポンスは次のようになります。

- レスポンス本文としての XML エラードキュメント
- Content-Type ヘッダー: text/xml

- 該当する HTTP ステータスコード (3xx、4xx、または 5xx)

REST エラーレスポンスの XML エラードキュメントの例を次に示します。

```
<ErrorResponse xmlns="https://route53.amazonaws.com/doc/2013-04-01/">
   <Error>
      <Type>Sender</Type>
      <Code>InvalidInput</Code>
      <Message>The input is not valid.</Message>
   </Error>
   <RequestId>410c2a4b-e435-49c9-8382-3770d80d7d4c</RequestId>
</ErrorResponse>
```

ドメイン登録と Route 53 Resolver の API リクエストの作成

トピック

- RPC リクエスト
- RPC レスポンス

このセクションでは、2 つの Amazon Route 53 APIs に RPC リクエストを行う方法について説明します。1 つはドメインの登録と管理に使用し、もう 1 つは Route 53 Resolver の管理に使用します。リクエストのコンポーネント、レスポンスの内容、リクエストの認証方法について説明します。

> **Note**
>
> ホストゾーン、リソースレコードセット、ヘルスチェック、コスト配分タグを作成および管理するには、該当する Route 53 API を使用します。詳細については、「ホストゾーン、リソースレコードセット、ヘルスチェックの API リクエストの実行」を参照してください。

RPC リクエスト

Amazon Route 53 RPC リクエストは、RFC 2616 で定義されている HTTPS リクエストです。このセクションでは、Route 53 RPC リクエストの構造について説明します。

RPC アクションの場合、HTTPS リクエストを Route 53 に送信し、レスポンスを待ちます。Route 53 への RPC リクエストには、リクエストヘッダーと、場合によってはクエリ文字列また

はリクエスト本文が含まれます。レスポンスには HTTP ステータスコードとレスポンスヘッダーが含まれており、レスポンス本文が含まれている場合もあります。

リクエストタイムスタンプについて

タイムスタンプは HTTP Dateヘッダーまたは AWS x-amz-date ヘッダーで指定する必要があります (一部の HTTP クライアントライブラリでは Dateヘッダーを設定できません)。x-amz-date ヘッダーがある場合、リクエストの認証時に Date ヘッダーは無視されます。

タイムスタンプは、リクエストが受信された AWS システム時刻から 5 分以内にする必要があります。これ以外の場合、リクエストは失敗し、RequestExpired というエラーコードが出力されます。これにより、他のユーザーがリクエストを再送信するのを防ぐことができます。

日付は、 などの ISO 8601 形式で指定する必要があります2016-03-03T19:20:25.177Z。詳細については、Wikipedia の記事 ISO 8601 を参照してください。

リクエスト本文

多くの Route 53 API アクションでは、リクエストの本文に JSON を含める必要があります。JSON は、ドメイン登録または Route 53 Resolver の Route 53 スキーマに準拠しています。

Exampleリクエストの例

次のリクエスト例では、単純な JSON ステートメントを使用して、ドメイン名example.comが使用可能かどうかを判断します。

リクエストの JSON 要素は、リストされた順序で表示する必要があります。

```
POST / HTTP/1.1
host:route53domains.us-east-1.amazonaws.com
x-amz-date:date and time of the request
authorization:AWS4-HMAC-SHA256
              Credential=AKIAIOSFODNN7EXAMPLE/date of the request in yyyymmdd format/
us-east-1/route53domains/aws4_request,
              SignedHeaders=content-length;content-type;host;user-agent;x-amz-date;x-
amz-target,
              Signature=computed signature
x-amz-target:Route53Domains_v20140515.CheckDomainAvailability
user-agent:information about the source of the request
content-type:application/x-amz-json- 1.1
content-length:length
```

```
connections:Keep-Alive
{
   "DomainName":"example.com"
}
```

RPC レスポンス

Amazon Route 53 レスポンスは、標準の HTTP レスポンスにすぎません。一部の Route 53 アクションは、レスポンス本文の HTTP ヘッダーまたは JSON の形式で Route 53 に固有の特別な情報を返します。具体的な詳細は、 アクションのドキュメントに記載されています。

各レスポンスには、Route 53 でリクエストをトラブルシューティングする必要がある場合に使用できるリクエスト ID が含まれています。ID は、 という名前の HTTP ヘッダーに含まれていますx-amz-request-id。リクエスト ID の例は です647cd254-e0d1-44a9-af61-1d6d86ea6b77。

次の例は、指定されたドメイン名の可用性をチェックするリクエストに対するレスポンスを示しています。Availability 要素は、リクエストで指定したドメインが使用可能かどうかを示します。

Exampleレスポンスの例

```
HTTP/1.1 200
Content-Length:number of characters in the JSON string
{
   "Availability":"AVAILABLE"
}
```

エラーレスポンス

RPC リクエストでエラーが発生した場合、HTTP レスポンスは次のようになります。

- レスポンス本文としての JSON 形式のエラードキュメント
- Content-Type ヘッダー: text/xml
- 該当する HTTP ステータスコード (3xx、4xx、または 5xx)

RPC エラーレスポンスの JSON エラードキュメントの例を次に示します。

```
{
 "__type": "com.amazon.coral.service#UnrecognizedClientException",
```

```
  "message": "The security token included in the request is invalid."
}
```

Amazon Route 53 API リクエストの署名

リクエストには、アクセスキー ID およびシークレットアクセスキーによる署名が必要です。Route 53 での日常業務に AWS アカウント 認証情報を使用しないことを強くお勧めします。ユーザーの認証情報を使用するか、 AWS STS を使用して一時的なセキュリティ認証情報を生成できます。

API リクエストに署名するには、 AWS 署名バージョン 4 を使用することをお勧めします。詳細については、IAM ユーザーガイドの「アクセス管理」を参照してください。

さらに、以下のトピックにも関心があるかもしれません。

- AWS セキュリティ認証情報 – アクセスに使用される認証情報のタイプに関する一般的な情報を提供します AWS。
- IAM ベストプラクティス – IAM サービスを使用して AWS リソースを保護するための提案のリストを示します。
- 一時的なセキュリティ認証情報 – 一時的なセキュリティ認証情報を作成して使用する方法について説明します。

関数別の Amazon Route 53 API アクション

このトピックではRoute 53 および Route 53 Resolver のすべての API アクションを、実行する関数別にグループ別に一覧表示します。

トピック

- 関数のタイプ
- 関数別のアクション

関数のタイプ

DNS

- Public and private hosted zones

- Public hosted zones
- Private hosted zones
- Resource record sets
- Public DNS query logs
- Reusable delegation sets

DNS—Traffic flow

- Traffic policies
- Traffic policy instances

Domain registration

- Register, renew, and transfer domains
- Transfer domains between AWS accounts
- Get domain information
- Change domain settings

DNS—DNSSEC

- DNSSEC signing
- DNSSEC validation

DNS—IP-based routing

Health checking

- Health checks
- Health checker IP ranges

Limits (quotas) for accounts, hosted zones, and reusable delegation sets

Route 53 profiles

- Route 53 profiles
- Profile VPC associations
- Profile resource associations

Route 53 Resolver

- Route 53 Resolver endpoints
- Private DNS query logs

- Route 53 Resolver rules
- Route 53 Resolver DNS Firewall
- Amazon Route 53 Resolver on Outposts
- Resolver configuration

Tags

- Tags for hosted zones and health checks
- Tags for domains
- Tags for Route 53 Resolver

関数別のアクション

DNS | DNS—Traffic flow | Domain registration | DNS—DNSSEC | DNS—IP-based routing | Health checking | Limits (quotas) for accounts, hosted zones, and reusable delegation sets | Route 53 profiles | Route 53 Resolver | Tags

DNS

パブリックホストゾーンとプライベートホストゾーン

- CreateHostedZone
- DeleteHostedZone
- GetHostedZone
- GetHostedZoneCount
- ListHostedZones
- ListHostedZonesByName
- UpdateHostedZoneComment

パブリックホストゾーン

- TestDNSAnswer

プライベートホストゾーン

- AssociateVPCWithHostedZone
- DisassociateVPCFromHostedZone
- CreateVPCAssociationAuthorization

- DeleteVPCAssociationAuthorization
- ListHostedZonesByVPC
- ListVPCAssociationAuthorizations

リソースレコードセット

- ChangeResourceRecordSets
- GetChange
- ListResourceRecordSets
- GetGeoLocation
- ListGeoLocations

パブリック DNS クエリログ

- CreateQueryLoggingConfig
- DeleteQueryLoggingConfig
- GetQueryLoggingConfig
- ListQueryLoggingConfigs

再利用可能な委任セット

- CreateReusableDelegationSet
- DeleteReusableDelegationSet
- GetReusableDelegationSet
- ListReusableDelegationSets

DNS — トラフィックフロー

トラフィックポリシー

- CreateTrafficPolicy
- CreateTrafficPolicyVersion
- DeleteTrafficPolicy
- GetTrafficPolicy
- ListTrafficPolicies
- ListTrafficPolicyVersions
- UpdateTrafficPolicyComment

トラフィックポリシーインスタンス

- CreateTrafficPolicyInstance
- DeleteTrafficPolicyInstance
- GetTrafficPolicyInstance
- GetTrafficPolicyInstanceCount
- ListTrafficPolicyInstances
- ListTrafficPolicyInstancesByHostedZone
- ListTrafficPolicyInstancesByPolicy
- UpdateTrafficPolicyInstance

ドメイン登録

ドメインの登録、更新、転送

- RegisterDomain
- RenewDomain
- ResendContactReachabilityEmail
- RetrieveDomainAuthCode
- TransferDomain
- DeleteDomain
- PushDomain
- ResendOperationAuthorization

AWS アカウント間でドメインを転送する

- AcceptDomainTransferFromAnotherAwsAccount
- CancelDomainTransferToAnotherAwsAccount
- RejectDomainTransferFromAnotherAwsAccount
- TransferDomainToAnotherAwsAccount

ドメイン情報の取得

- CheckDomainAvailability
- CheckDomainTransferability
- GetContactReachabilityStatus

- GetDomainDetail
- GetDomainSuggestions
- GetOperationDetail
- ListDomains
- ListOperations
- ListPrices
- ViewBilling

ドメイン設定を変更する

- DisableDomainAutoRenew
- DisableDomainTransferLock
- EnableDomainAutoRenew
- EnableDomainTransferLock
- UpdateDomainContact
- UpdateDomainContactPrivacy
- UpdateDomainNameservers

DNS — DNSSEC

DNSSEC 署名

- ActivateKeySigningKey
- CreateKeySigningKey
- DeactivateKeySigningKey
- GetDNSSEC
- AssociateDelegationSignerToDomain
- DisassociateDelegationSignerFromDomain

DNSSEC 検証

- GetResolverDnssecConfig
- ListResolverDnssecConfigs
- UpdateResolverDnssecConfig

DNS - IP ベースのルーティング

- ChangeCidrCollection

- CreateCidrCollection
- DeleteCidrCollection
- ListCidrBlocks
- ListCidrCollections
- ListCidrLocations

ヘルスチェック

ヘルスチェック

- CreateHealthCheck
- DeleteHealthCheck
- GetHealthCheck
- GetHealthCheckCount
- GetHealthCheckLastFailureReason
- GetHealthCheckStatus
- ListHealthChecks
- UpdateHealthCheck

ヘルスチェッカーの IP 範囲

- GetCheckerIpRanges

アカウント、ホストゾーン、再利用可能な委任セットの制限 (クォータ)

- GetAccountLimit
- GetHostedZoneLimit
- GetReusableDelegationSetLimit

Route 53 プロファイル

Route 53 プロファイル

- CreateProfile
- DeleteProfile
- GetProfile
- ListProfiles

VPC の関連付けをプロファイルする

- AssociateProfile

- DisassociateProfile
- GetProfileAssociation
- ListProfileAssociations

リソースの関連付けをプロファイルする

- AssociateResourceToProfile
- DisassociateResourceFromProfile
- GetProfileResourceAssociation
- ListProfileResourceAssociations
- UpdateProfileResourceAssociation

Route 53 リゾルバー

Route 53 Resolver エンドポイント

- AssociateResolverEndpointIpAddress
- CreateResolverEndpoint
- DeleteResolverEndpoint
- DisassociateResolverEndpointIpAddress
- GetResolverEndpoint
- ListResolverEndpointIpAddresses
- ListResolverEndpoints
- UpdateResolverEndpoint

DNS クエリログ

- AssociateResolverQueryLogConfig
- CreateResolverQueryLogConfig
- DeleteResolverQueryLogConfig
- DisassociateResolverQueryLogConfig
- GetResolverQueryLogConfig
- GetResolverQueryLogConfigAssociation
- GetResolverQueryLogConfigPolicy
- ListResolverQueryLogConfigAssociations

- ListResolverQueryLogConfigs
- PutResolverQueryLogConfigPolicy

Route 53 Resolver ルール

- AssociateResolverRule
- CreateResolverRule
- DeleteResolverRule
- DisassociateResolverRule
- GetResolverRule
- GetResolverRuleAssociation
- GetResolverRulePolicy
- ListResolverRuleAssociations
- ListResolverRules
- PutResolverRulePolicy
- UpdateResolverRule

Route 53 リゾルバー DNS ファイアウォール

- AssociateFirewallRuleGroup
- CreateFirewallDomainList
- CreateFirewallRule
- CreateFirewallRuleGroup
- DeleteFirewallDomainList
- DeleteFirewallRule
- DeleteFirewallRuleGroup
- DisassociateFirewallRuleGroup
- GetFirewallConfig
- GetFirewallDomainList
- GetFirewallRuleGroup
- GetFirewallRuleGroupAssociation
- GetFirewallRuleGroupPolicy
- ImportFirewallDomains

- ListFirewallConfigs
- ListFirewallDomainLists
- ListFirewallDomains
- ListFirewallRuleGroupAssociations
- ListFirewallRuleGroups
- ListFirewallRules
- PutFirewallRuleGroupPolicy
- UpdateFirewallConfig
- UpdateFirewallDomains
- UpdateFirewallRule
- UpdateFirewallRuleGroupAssociation

Outposts の Route 53 Resolver

- CreateOutpostResolver
- DeleteOutpostResolver
- GetOutpostResolver
- ListOutpostResolvers
- UpdateOutpostResolver

VPC リゾルバーの設定

- GetResolverConfig
- ListResolverConfigs
- UpdateResolverConfig

タグ

ホストゾーンとヘルスチェックのタグ

- ChangeTagsForResource
- ListTagsForResource
- ListTagsForResources

ドメインのタグ

- DeleteTagsForDomain
- ListTagsForDomain

- UpdateTagsForDomain

Route 53 Resolver のタグ

- ListTagsForResource
- TagResource
- UntagResource

Amazon Route 53 API リクエストのスロットリング

> **Important**
>
> Amazon Route 53 は API スロットリング動作を更新しました。更新には、1 秒あたりのリクエスト数の制限の引き上げと、変更ベースのスロットリングの導入が含まれます。このページでは、更新された制限について詳しく説明します。

Amazon Route 53 は API リクエストをアカウント単位でスロットリングし、サービスの安定性を維持し、すべてのお客様に公平な使用を確保します。Route 53 は 2 つの独立した制限を適用します。

- リクエストレート: 1 秒あたりの API リクエストの数。
- 変更スループット: DNS データを変更する API アクション全体で集計された、1 秒あたりの個々の DNS レコード変更の数。

リクエストはどちらの制限でもスロットリングできます。リクエストがスロットリングされると、Amazon Route 53 は HTTP 400 エラー () を返しますBad `request`。レスポンスヘッダーには、`Throttling` の値を持つ `Code` 要素と、`Rate exceeded` の値を持つ `Message` 要素も含まれています。

スロットリングの適用方法

Amazon Route 53 はトークンバケットアルゴリズムを使用します。各制限には、トークンの最大数を保持するバケットがあります。各リクエスト (リクエストレート制限の場合) または各変更 (変更スループット制限の場合) は、該当するバケットからトークンを削除します。バケットは、最大容量まで毎秒固定レートで補充されます。バケットがすでに満杯になったときにリフィルトークンが到着した場合、Route 53 はトークンを破棄します。

バケットごとに 2 つの値が記述されます。

- バケットの最大容量はバーストです。バケットがいっぱいになると、Route 53 が一度に吸収できるリクエストまたは変更の数です。
- バケットリフィルレートは、1 秒あたりのリクエスト数または変更数を無期限に維持できる持続的なレートです。

追加時にリフィルトークンを使用できます。バケットが完全にリフィルするのを待つ必要はありません。

リクエストレートトークンバケットサイズとリフィルレート

Route 53 は、次の 2 つのレベルでリクエストレートスロットリングを適用します。

- アカウントレベル: アカウントからのすべての Amazon Route 53 API リクエストは、1 つのバケットから取得されます。
- アカウントレベルとオペレーションレベル: 各 API アクションには独自のバケットもあります。

リクエストは両方のバケットからトークンを消費し、いずれかのバケットが空の場合にスロットリングされます。以下のアクションには、デフォルトのリクエストレート制限が異なります。

API アクションあたりのリクエストレート制限

API アクション	バケットの最大容量	バケットリフィルレート
すべての Amazon Route 53 API アクションの組み合わせ (アカウントレベル)	50	10
以下にリストされていない単一の API アクション (アクションごとのデフォルト)	50	10
`AssociateVPCWithHostedZone`	20	5
`ChangeCidrCollection`	40	5
`CreateCidrCollection`	40	5
`CreateHealthCheck`	50	0.5
`CreateHostedZone`	40	2

API アクション	バケットの最大容量	バケットリフィルレート
CreateReusableDelegationSet	40	2
CreateTrafficPolicyInstance	1	1
DeleteCidrCollection	40	5
DeleteHealthCheck	15	3
DeleteHostedZone	40	5
DeleteReusableDelegationSet	40	5
DeleteTrafficPolicyInstance	1	1
DisassociateVPCFromHostedZone	10	5
GetHealthCheckLastFailureReason	4	1
GetHealthCheckStatus	4	1
UpdateHealthCheck	50	5
UpdateTrafficPolicyInstance	1	1

Amazon Route 53 API アクションの完全なリストについては、「Amazon Route 53 API リファレンス」の「アクション」を参照してください。 Amazon Route 53

CreateHealthCheck リクエストでオプションで指定するパラメータです。

CreateHealthCheck リクエストは、 AWS アカウント ごとに 2 秒に 1 回送信できます。これは、前の表に示す 1 秒あたり 0.5 リクエストの補充レートに対応します。

スループット制限の変更

リクエストレート制限に加えて、DNS データを変更する API アクションには、変更スループット制限が適用されます。この制限は、リクエストの数ではなく、リクエストによって行われた DNS レコードの変更の数に基づいて枯渇する別のトークンバケットを使用します。変更スループットは API

アクションごとではなく AWS アカウント、 ごとに制限されます。以下のすべてのアクションは、最大容量が 1,500 の変更 (バースト) で、1 秒あたり 100 の変更 (持続) で補充される 1 つのバケットから取得されます。

変更は次のようにカウントされます。

オペレーションごとに消費されるトークン

運用	消費されたトークン
ChangeResourceRecordSets	ごとに 1CREATE、 ごとに 1DELETE、 ごとに 2 UPSERT
AssociateVPCWithHostedZone	2
DisassociateVPCFromHostedZone	2
CreateHostedZone	2
DeleteHostedZone	2

他のすべての Amazon Route 53 API アクションは、変更スループットトークンを消費せず、リクエストレートによってのみ制限されます。

例: 1,000 個のトークンを消費する 1,000 個の変更 (バースト) を含む 1 つのリクエストを送信できます。バースト後、バケットは 1 秒あたり 100 トークンで補充されます。1 秒あたり 100 件の変更を送信し続けると、そのレートを無期限に維持できます。1 秒あたり 500 回の変更を維持しようとすると、バケットは枯渇し、それ以降のリクエストは補充されるまでスロットリングされます。

API スロットリングをモニタリングする

Amazon Route 53 API の使用状況をモニタリングするには、アプリケーションログの HTTP 400 レスポンスを監視するか、CloudWatch メトリクスを介して API の使用状況を追跡します。スロットリングエラーが発生すると、リクエストは前のセクションで説明した制限のいずれかを超えています。

再試行とエクスポネンシャルバックオフ

API リクエストをポーリングまたは再試行するときは、エクスポネンシャルバックオフアルゴリズムを使用してリクエスト間のスリープ間隔を計算することをお勧めします。エクスポネンシャルバックオフでは、連続するエラーレスポンスの再試行間隔が徐々に長くなります。最大遅延間隔と最大再

試行回数を実装し、連続する衝突を防ぐためにジッター (ランダム遅延) を追加することを検討してください。詳細については、「ビルダーライブラリ」の「タイムアウト、再試行、ジッターによるバックオフ」を参照してください。 AWS

各 AWS SDK は自動再試行ロジックを実装します。これには、スロットリングに応じてクライアント側のリクエストレートを調整するアダプティブ再試行モードが含まれます。これらの制限に定期的に近づくワークロードの場合は、アダプティブ再試行を有効にすることを検討してください。詳細については、「AWS SDK とツールのリファレンスガイド」の「再試行動作」を参照してください。

制限の引き上げのリクエスト

API リクエストレートまたは変更スループット制限の引き上げは、 AWS サポートを通じてリクエストできます。引き上げをリクエストするには:

- AWS サポートセンターを開きます。
- ケースを作成し、サービス制限の引き上げを選択します。
- 制限タイプで、Route 53 を選択します。
- 現在の使用量と必要な制限を指定します。

API スロットリングのベストプラクティス

- リクエストレートとバッチサイズのバランス: リクエストレート制限によって調整されている場合は、リクエストごとにより多くの変更を送信します。変更スループット制限によって調整されている場合は、合計変更率を減らします。非常に小さいバッチも非常に大きいバッチも、単独では最適ではありません。
- アトミック性にバッチ処理を使用する: 1 つのChangeResourceRecordSetsリクエストのすべての変更はアトミックに適用されるため、成功または失敗します。
- 時間の経過とともに変更を分散する: 大きなバッチを同時に送信するのではなく、数秒間にわたって変更を均等に分散します。
- 持続的なスループットではなく、時折の急増に頼る: バースト容量は正当なトラフィックの急増に対応します。持続的な運用上限ではありません。
- エクスポネンシャルバックオフで再試行: HTTP 400 レスポンスを受け取ったら、試行のたびに増加する遅延後に再試行します (「」を参照the section called “再試行とエクスポネンシャルバックオフ”)。
- リクエスト制限の事前引き上げ: ワークロードの増加が予想される場合は、制限に達する前に引き上げをリクエストします (「」を参照the section called “制限の引き上げのリクエスト”)。

より広範な Amazon Route 53 のガイダンスについては、「」を参照してくださいベストプラクティス。

クォータ

Amazon Route 53 API リクエストとエンティティには、次のクォータが適用されます (以前は「制限」と呼ばれていました)。

トピック

- Service Quotas を使用したクォータの表示と管理
- エンティティのクォータ
- API リクエストの最大数

Service Quotas を使用したクォータの表示と管理

Service Quotas サービスを使用して、多くの AWS サービスのクォータを表示し、クォータの引き上げをリクエストできます。詳細については、Service Quotas ユーザーガイドを参照してください。(Service Quotas を使用して、ドメイン、Route 53、Route 53 VPC Resolver のクォータを表示および管理できます)。

> **Note**
>
> クォータを表示し、Route 53 のクォータ引き上げをリクエストするには、リージョンを米国東部 (バージニア北部) に変更する必要があります。VPC Resolver のクォータを表示してクォータの引き上げをリクエストするには、該当するリージョンに変更します。

エンティティのクォータ

Amazon Route 53 のエンティティには、次のクォータが適用されます。

現在のクォータ (以前は「制限」と呼ばれていました) の取得については、次の Route 53 アクションを参照してください。

- GetAccountLimit: ヘルスチェック、ホストゾーン、再利用可能な委託セット、トラフィックフローポリシー、トラフィックフローポリシーレコードのクォータを取得
- GetHostedZoneLimit: ホストゾーン、およびプライベートホストゾーンに関連付けることができる Amazon VPC のレコードのクォータを取得

- GetReusableDelegationSetLimit: 再利用可能な委託セットに関連付けることができるホストゾーンの数のクォータを取得

トピック

- ドメインのクォータ
- ホストゾーンのクォータ
- レコードのクォータ
- Route 53 VPC リゾルバーのクォータ
- ヘルスチェックのクォータ
- クエリログの設定のクォータ
- トラフィックフローポリシーおよびポリシーレコードのクォータ
- 再利用可能な委任セットのクォータ
- Route 53 プロファイルのクォータ

ドメインのクォータ

ドメインクォータ

エンティティ	Quota
ドメイン	AWS アカウントあたり 20* クォータ引き上げのリクエスト

* 2021 年 3 月時点の、新規顧客向けの上限は 20 です。

すでにアカウントをお持ちで、デフォルトの制限が 50 の場合、50 のままになります。

ホストゾーンのクォータ

ホストゾーンのクォータ

エンティティ	Quota
ホストゾーン	

エンティティ	Quota
	初期クォータは AWS アカウントあたり 500 ですが、必要に応じてより高いクォータをリクエストできます。 クォータ引き上げのリクエスト
同じ再利用可能な委託セットを使用できるホストゾーン	100 クォータ引き上げのリクエスト
ホストゾーン ごとに、プライベートホストゾーン に関連付けることができる Amazon VPC	300 300 を超える関連付けが必要な場合は、Route 53 プロファイルを使用することをお勧めします。詳細については、「Amazon Route 53 プロファイルとは」を参照してください。
VPC を関連付けることができるプライベートホストゾーン	クォータなし *
あるアカウントで作成した VPC と、別のアカウントで作成したホストゾーンを関連付けられるように作成できる許可	1,000
ホストゾーンごとに作成できる鍵署名鍵 (KSK) の数	2

* AWS アカウントを通じて制御するプライベートホストゾーンの一部またはすべてに VPC を関連付けることができます。たとえば、3 つの AWS アカウントがあり、3 つすべてに 500 個のホストゾーンのデフォルトのクォータがあるとします。3 つのアカウントすべてに 500 個のプライベートホストゾーンを作成する場合、VPC を 1,500 個のプライベートホストゾーンすべてにリンクできます。

レコードのクォータ

レコードクォータ

エンティティ	Quota
レコード	10,000/ホストゾーン クォータ引き上げのリクエスト ホストゾーンのレコードのクォータが 10,000 を超える場合は、追加料金が適用されます。詳細については、「Amazon Route 53 料金表」を参照してください。
レコードセット内のレコード	レコードセットあたり 400
位置情報、レイテンシー、複数値回答、加重、および IP ベースの各レコード	同じ名前とタイプのレコードは 100 個まで
地理的近接性レコード	同じ名前とタイプのレコードは 30 個まで
CIDR コレクション	あたり 5 AWS アカウント。 クォータ引き上げのリクエスト。
CIDR ブロック	CIDR コレクションあたり1000 個。 クォータ引き上げのリクエスト。

Route 53 VPC リゾルバーのクォータ

このセクションでは、Route 53 VPC Resolver のすべてのクォータについて説明します。

Route 53 VPC リゾルバーのクォータ

Route 53 VPC Resolver のクォータを引き上げるには、次の手順に従います。

Resolver のクォータを増やすには

1. https://console.aws.amazon.com/servicequotas/home/services/route53resolver/quotasでService Quotas コンソールを開きます。
2. 制限を引き上げるリージョンに移動します。
3. 増やす Route 53 VPC Resolver クォータ名を選択します。
4. [クォータ引き上げリクエスト] を選択し、クォータ値を入力してから、[リクエスト] を選択します。

Route 53 VPC Resolver エンドポイントのクォータ

リゾルバーエンドポイントのクォータ

エンティティ	クォータ
AWS リージョンあたりのエンドポイント	AWS アカウントあたり 4 クォータ引き上げのリクエスト
エンドポイントあたりの IP アドレス数	6 クォータ引き上げのリクエスト。
ルールあたりの IP アドレス数	6
AWS リージョンあたりのルール	AWS アカウントあたり 1000 クォータ引き上げのリクエスト。
AWS リージョンあたりのルールとVPCsの関連付け	AWS アカウントあたり 2000 クォータ引き上げのリクエスト。
	10,000*

エンティティ	クォータ
エンドポイントの IP アドレスごとに 1 秒あたりの UDP クエリ数	

*エンドポイント内の各 IP アドレスでは、1 秒あたり最大 10,000 UDP DNS クエリ (QPS) を処理できます。実際の DNS QPS は、クエリのタイプ、レスポンスのサイズ、ターゲットネームサーバーの正常性、クエリ応答時間、ラウンドトリップレイテンシー、使用中のプロトコルによって異なります。たとえば、応答が遅いターゲットネームサーバーへのクエリは、ネットワークインターフェイスの容量を減らすことができます。また、高可用性を確保するために、Route 53 Resolver は受信した DNS リクエストごとに冗長なアウトバウンドクエリを送信します。その結果、各アウトバウンドネットワークインターフェイスの QPS は、Route 53 VPC Resolver に送信された QPS と一致しません。CloudWatch メトリクスを使用して、各ネットワークインターフェイスに送信されるクエリの数を測定します。詳細については、「Route 53 VPC Resolver の IP アドレスのメトリクス」を参照してください。最大クエリレートがエンドポイント内の任意のネットワークインターフェイスの容量の 50% を超える場合は、ネットワークインターフェイスを追加してエンドポイントの容量を増やすことができます。

Network Load Balancer や AWS Lambda (完全なリストについては、「自動追跡接続」を参照) などのサービスを介して行われた接続は、セキュリティグループのセットアップで追跡が必要ない場合でも、デフォルトで追跡されます。

制限付きセキュリティグループルールによって接続追跡が強制される場合、またはクエリが Network Load Balancer を介してルーティングされる場合、インバウンドエンドポイントの IP アドレスあたりの 1 秒あたりの最大クエリ数は 1500 に抑えられます。

Route 53 VPC Resolver クエリログのクォータ

Resolver クエリログのクォータ

エンティティ	クォータ
AWS リージョンあたりのクエリログ設定	20 クォータ引き上げのリクエスト。
AWS リージョンごとのクエリログ設定 VPC の関連付け	100 *

エンティティ	クォータ
	クォータ引き上げのリクエスト。
設定が共有されたアカウントの AWS リージョンごとのアカウントあたりのクエリログ設定 VPC 関連付け (RAM を使用して共有されたクエリロングコンフィギュレーションを含む)。	100 クォータ引き上げのリクエスト

* これは、1 つのリージョン内のすべての VPC Resolver クエリログ設定に適用されるリージョンの制限です。同じリージョンでより多くのクエリログ設定を作成しても、VPC 関連付け容量は増えません。

Resolver DNS ファイアウォールのクォータ

DNS ファイアウォールのクォータ

エンティティ	Quota
AWS リージョンあたり 1 つのアカウントの VPC に関連付けられたルールグループの数	5
AWS リージョンごとに 1 つのアカウントの 1 つの Amazon S3 ファイル内の DNS Firewall ドメインの数	250,000 クォータ引き上げのリクエスト。
AWS リージョンあたりの 1 つのアカウントの DNS Firewall ルールグループの数	1,000 クォータ引き上げのリクエスト。
AWS リージョンごとに 1 つのアカウントのルールグループ内のルールの数	100 クォータ引き上げのリクエスト

エンティティ	Quota
AWS リージョンあたりの 1 つのアカウントのドメインリストの数	1,000 クォータ引き上げのリクエスト。
AWS リージョンあたりの単一アカウントに対する、すべてのドメインリストで指定できるドメインの最大数	100,000 クォータ引き上げのリクエスト。

第 1 世代の Resolver のクォータ AWS Outposts

Outposts のリゾルバーのクォータ

エンティティ	クォータ
Resolver on Outpost インスタンス制限	6 (最低 4 つ必要)

Resolver on Outpost インスタンスタイプ、および各インスタンスタイプが 1 秒あたりに処理できる DNS クエリの数:

インスタンスタイプ別の 1 秒あたりのクエリ数

インスタンスタイプ	1 秒あたりのクエリ数
c5.large	最大 7,000
c5.xlarge	最大 12,000
c5.2xlarge	最大 24,000
c5.4xlarge	最大 56,000
c5d.large	最大 7,000

インスタンスタイプ	1 秒あたりのクエリ数
c5d.xlarge	最大 12,000
c5d.2xlarge	最大 24,000
c5d.4xlarge	最大 56,000
m5.large	最大 7,000
m5.xlarge	最大 12,000
m5.2xlarge	最大 24,000
m5.4xlarge	最大 56,000
m5d.large	最大 7,000
m5d.xlarge	最大 12,000
m5d.2xlarge	最大 24,000
m5d.4xlarge	最大 56,000
r5.large	最大 7,000
r5.xlarge	最大 12,000
r5.2xlarge	最大 24,000
r5.4xlarge	最大 56,000

インスタンスタイプ	1 秒あたりのクエリ数
r5d.large	最大 7,000
r5d.xlarge	最大 12,000
r5d.2xlarge	最大 24,000
r5d.4xlarge	最大 56,000

Resolver on Outpost エンドポイントインスタンスタイプ、および各インスタンスタイプが 1 秒あたりに処理できる DNS クエリの数:

エンドポイントインスタンスタイプ別の 1 秒あたりのクエリ数

インスタンスタイプ	1 秒あたりのクエリ数
c5.large	最大 5,000
c5.xlarge	最大 10,000
c5.2xlarge	最大 18,000
c5.4xlarge	最大 30,000
c5d.large	最大 5,000
c5d.xlarge	最大 10,000
c5d.2xlarge	最大 18,000
c5d.4xlarge	最大 30,000

インスタンスタイプ	1 秒あたりのクエリ数
m5.large	最大 5,000
m5.xlarge	最大 10,000
m5.2xlarge	最大 18,000
m5.4xlarge	最大 30,000
m5d.large	最大 5,000
m5d.xlarge	最大 10,000
m5d.2xlarge	最大 18,000
m5d.4xlarge	最大 30,000
r5.large	最大 5,000
r5.xlarge	最大 10,000
r5.2xlarge	最大 18,000
r5.4xlarge	最大 30,000
r5d.large	最大 5,000
r5d.xlarge	最大 10,000
r5d.2xlarge	最大 18,000

インスタンスタイプ	1 秒あたりのクエリ数
r5d.4xlarge	最大 30,000

第 2 世代のリゾルバーのクォータ AWS Outposts

次の表に、第 2 世代の Resolver のクォータを示します AWS Outposts。

第 2 世代 AWS Outposts のクォータのリゾルバー

クォータ名	クォータ値
1 秒あたりの DNS クエリ	最大 75,000

ヘルスチェックのクォータ

ヘルスチェックのクォータ

エンティティ	Quota
ヘルスチェック	AWS アカウントあたり 200 件のアクティブなヘルスチェック クォータ引き上げのリクエスト。
算出したヘルスチェックが監視できる子ヘルスチェック	255
ヘルスチェックリクエストへのレスポンスのヘッダーの最大合計長	16,384 バイト (16K)

クエリログの設定のクォータ

クエリログ設定クォータ

エンティティ	Quota
クエリログの設定	1/ホストゾーン

トラフィックフローポリシーおよびポリシーレコードのクォータ

トラフィックフローのクォータ

エンティティ	Quota
トラフィックポリシー Route 53 トラフィックフローの詳細については、「DNS トラフィックのルーティングにトラフィックフローを使用する」を参照してください。	AWS アカウントあたり 50 クォータ引き上げのリクエスト。
トラフィックポリシーバージョン	トラフィックポリシーあたり 1000
トラフィックポリシーレコード (Route 53 API、 AWS SDKs」と呼ばれます AWS Tools for Windows PowerShell) AWS Command Line Interface	AWS アカウントあたり 5 クォータ引き上げのリクエスト。

再利用可能な委任セットのクォータ

再利用可能な委任セットのクォータ

エンティティ	Quota

エンティティ	Quota
再利用可能な委託セット	AWS アカウントあたり 100 クォータ引き上げのリクエスト。

Route 53 プロファイルのクォータ

Route 53 プロファイルクォータ

エンティティ	クォータ
リージョン AWS アカウント 内の あたりの Route 53 プロファイルの数	5 クォータ引き上げのリクエスト。
プロファイルに関連付けることができる VPC の数	1,000 クォータ引き上げのリクエスト。
プロファイルあたりの DNS ファイアウォールルールグループの数	5
プロファイルあたりの Resolver ルールの数	1,000 クォータ引き上げのリクエスト。
プロファイルあたりのプライベートホストゾーンの数	5000 クォータ引き上げのリクエスト。
プロファイルあたりの VPC Resolver クエリログ記録設定の数	2

API リクエストの最大数

Amazon Route 53 API リクエストには、次の最大値が適用されます。

トピック

- ChangeResourceRecordSets リクエストの要素数と文字数
- Amazon Route 53 API リクエストの頻度
- Route 53 VPC Resolver API リクエストの頻度

`ChangeResourceRecordSets` リクエストの要素数と文字数

`ResourceRecord` 要素

リクエストには、1000 個を超える `ResourceRecord` 要素を含めることはできません (エイリアスレコードを含む)。`Action` 要素の値が `UPSERT` の場合、各 `ResourceRecord` 要素は 2 回カウントされます。

最大文字数

リクエストに含まれるすべての `Value` 要素内の文字 (スペースを含む) の合計数は、32,000 文字を超えることはできません。`Action` 要素の値が `UPSERT` の場合、`Value` 要素の各文字は 2 回カウントされます。

Amazon Route 53 API リクエストの頻度

すべての Amazon Route 53 API リクエスト

Amazon Route 53 は、アカウントごとに API リクエストをスロットリングしてサービスの安定性を維持し、すべてのお客様に公平な使用を確保します。Route 53 は 2 つの独立した制限を適用します。

- リクエストレート: 1 秒あたりの API リクエストの数。
- 変更スループット: DNS データを変更する API アクション全体で集計された、1 秒あたりの個々の DNS レコード変更の数。

リクエストはどちらの制限でもスロットリングできます。リクエストがスロットリングされると、Amazon Route 53 は HTTP 400 エラー () を返しますBad `request`。レスポンスヘッダーには、`Throttling` の値を持つ `Code` 要素と、`Rate exceeded` の値を持つ `Message` 要素も含まれています。

各 API アクション、バケットサイズ、リフィルレート、および引き上げのリクエストに適用される制限については、「」を参照してくださいthe section called “API スロットリング”。

> **Note**
>
> アプリケーションがこの制限を超える場合は、再試行のエクスポネンシャルバックオフを実装することをお勧めします。詳細については、「Amazon Web Services 全般のリファレンス」の「エラーの再試行と AWSでのエクスポネンシャルバックオフ」を参照してください。

`ChangeResourceRecordSets` リクエストでオプションで指定するパラメータです。

Route 53 で、次のリクエストが到着するまでにリクエストを処理できない場合、同じホストゾーンの後続のリクエストが却下され、HTTP 400 エラー (`Bad request`) が返されます。レスポンスヘッダーには、`PriorRequestNotComplete` の値を持つ `Code` 要素と、`The request was rejected because Route 53 was still processing a prior request.` の値を持つ `Message` 要素も含まれています。

Route 53 VPC Resolver API リクエストの頻度

すべてのリクエスト

リージョンごとに AWS 、アカウントごとに 1 秒あたり 5 つのリクエスト。リージョンで 1 秒あたり 5 件を超えるリクエストを送信すると、VPC Resolver は HTTP 400 エラー () を返しますBad request。レスポンスヘッダーには、Throttling の値を持つ Code 要素と、Rate exceeded の値を持つ Message 要素も含まれています。

> **Note**
>
> アプリケーションがこの制限を超える場合は、再試行のエクスポネンシャルバックオフを実装することをお勧めします。詳細については、「Amazon Web Services 全般のリファレンス」の「エラーの再試行と AWSでのエクスポネンシャルバックオフ」を参照してください。

関連情報

このサービスを利用する際に役立つ関連リソースは以下の通りです。

トピック

- AWS のリソース
- サードパーティ製ツールとライブラリ
- グラフィカルユーザーインターフェイス

AWS のリソース

いくつかの有益なガイド、フォーラム、およびその他のリソースを Amazon Web Services から利用できます。

- Amazon Route 53 API リファレンス – スキーマの場所、API のすべてのアクション、パラメータ、データ型についての詳しい説明、このサービスから返されるエラーのリストを含むリファレンスガイドです。
- 「AWS::Route53::RecordSetタイプ」(「AWS CloudFormation ユーザーガイド」) - Amazon Route 53 を CloudFormation と共に使用して、CloudFormation スタック用のカスタマイズした DNS 名を作成するためのプロパティです。
- フォーラム – デベロッパーのためのコミュニティベースのフォーラムです。Route 53 に関連する技術的な質問についてディスカッションできます。
- AWS サポートセンター - このサイトには、お客様の最近のサポートケース、AWS Trusted Advisor の助言とヘルスチェックの結果に関する情報がまとめられており、フォーラム、技術上のよくある質問、サービスヘルスダッシュボード、AWS サポートプランに関する情報へのリンクも掲載されています。
- AWS Premium Support Information (プレミアムサポート情報) - 1 対 1 での迅速な対応を行うサポートチャネルである AWS プレミアムサポートに関する情報のメインウェブページです。プレミアムサポートは、AWS インフラストラクチャサービスでのアプリケーションの構築および実行を支援します。
- お問い合わせ – 請求やアカウントに関するお問い合わせ用のリンクです。技術的な質問の場合は、上記のディスカッションフォーラムまたはサポート用のリンクをご利用ください。
- Route 53 製品情報 – 機能、料金、その他の情報を含む、Route 53 に関する情報を提供しているメインのウェブページです。

- クラスとワークショップ – AWS のスキルを磨き、実践的な経験を得るために役立つセルフペースラボに加えて、ロールベースのコースと特別コースへのリンクです。
- AWS デベロッパーセンター – チュートリアルの検索、ツールのダウンロード、AWS デベロッパーイベントの確認を行います。
- AWS デベロッパーツール - AWS アプリケーションを開発および管理するためのデベロッパーツール、SDK、IDE ツールキット、およびコマンドラインツールへのリンクです。
- ご利用開始のためのリソースセンター — AWS アカウント をセットアップする方法、AWS コミュニティに参加する方法、最初のアプリケーションを起動する方法を説明します。
- ハンズオンチュートリアル - ステップ バイ ステップのチュートリアルに従って、最初のアプリケーションを AWS で起動します。
- AWS ホワイトペーパー – アーキテクチャ、セキュリティ、エコノミクスなどのトピックについて、AWS のソリューションアーキテクトや他の技術エキスパートが記述した AWS の技術ホワイトペーパーの包括的なリストへのリンクです。
- AWS サポート センター – AWS サポート のケースを作成して管理するためのハブです。フォーラム、技術上のよくある質問、サービスヘルスステータス、AWS Trusted Advisor など、他の役立つリソースへのリンクも含まれています。
- サポート – サポート に関する情報のメインウェブページです。クラウド内でのアプリケーションの構築および実行を支援するために 1 対 1 での迅速な対応を行うサポートチャネルとして機能します。
- お問い合わせ - AWS の請求、アカウント、イベント、不正使用、その他の問題などに関するお問い合わせの受付窓口です。
- AWS サイトの利用規約 – 当社の著作権、商標、お客様のアカウント、ライセンス、サイトへのアクセス、およびその他のトピックに関する詳細情報です。

サードパーティ製ツールとライブラリ

AWS リソースに加えて、Amazon Route 53 に対応する各種サードパーティーツールやライブラリがあります。

- AmazonRoute53AppsScript (webos-goodies 経由)

  Amazon Route 53 の Google スプレッドシート管理。
- .NET 用 AWS コンポーネント (SprightlySoft 経由)

REST オペレーションおよび Route 53 のサポートを含む、Amazon Web Services 向けの SprightlySoft .NET コンポーネント。

- Boto API のダウンロード (github 経由)

  Amazon Web Services への Boto Python インターフェイス。

- cli53 (github 経由)

  Route 53 用のコマンドラインインターフェイス。

- Dasein Cloud API

  Java ベースの API。

- R53.py (github 経由)

  ソース管理の対象となっている DNS 設定の正規バージョンを維持し、設定の変更に必要な変更の最小セットを計算します。

- route53d

  Route 53 API への DNS フロントエンド (増分ゾーン転送 (IXFR) を有効にします)。

- Route53Manager (github 経由)

  ウェブベースのインターフェイス。

- Ruby Fog (github 経由)

  Ruby クラウドサービスライブラリ。

- WebService::Amazon::Route53 (CPAN 経由)

  Amazon Route 53 API への Perl インターフェイス。

グラフィカルユーザーインターフェイス

次のサードパーティツールは、Amazon Route 53 を使用して作業するためのグラフィカルユーザーインターフェイス (GUI) を提供します。

- R53 Fox
- Ylastic

ドキュメント履歴

以下の項目に、Route 53 ドキュメントの各リリースにおける重要な変更点を示します。このドキュメントの更新に関する通知を受け取るには、RSS フィードにサブスクライブできます。

トピック

- 2025 年のリリース
- 2024 年のリリース
- 2023 年のリリース
- 2022 年のリリース
- 2021 年のリリース
- 2020 年のリリース
- 2018 年のリリース
- 2017 年のリリース
- 2016 年のリリース
- 2015 年のリリース
- 2014 年のリリース
- 2013 年のリリース
- 2012 年のリリース
- 2011 年のリリース
- 2010 年のリリース

2025 年のリリース

2025 年 12 月 15 日

Route 53 Resolver エンドポイントの詳細な CloudWatch メトリクスを追加しました。新しいメトリクスは、DNS クエリの P90 応答レイテンシー、SERVFAIL、NXDOMAIN、REFUSED、および FORMERR 応答ステータスの追跡、アウトバウンドリゾルバーエンドポイントのターゲットネームサーバーの可用性モニタリングなど、リゾルバーネットワークインターフェイスおよびターゲットネームサーバーレベルで強化されたモニタリング機能を提供します。詳細については、「Route 53 VPC リゾルバーの CloudWatch 詳細メトリクス Route 53」を参照してください。

2025 年 6 月 26 日

`ResolverEndpointCapacityStatus` を `AWS/Route53Resolver` 名前空間に追加しました。詳細については、「Route 53 VPC Resolver エンドポイントのメトリクス」を参照してください。

2025 年 6 月 25 日

Amazon Route 53 は、VPC Lattice サービスのカスタムドメインエンドポイントのエイリアスレコードをサポートできるようになりました。詳細については、「Amazon VPC Lattice サービスドメインエンドポイントへのトラフィックのルーティング」を参照してください。

2025 年 6 月 24 日

VPC Resolver でインバウンド委任とアウトバウンド委任を使用できるようになりました。詳細については、「ネットワーク上の DNS リゾルバーが DNS クエリを Resolver エンドポイントに転送する方法」を参照してください。

2025 年 6 月 1 日

`cloudwatch:GetMetricData`、`tag:GetResources`、`es:ListDomainNames`、`es:DescribeDoma` のアクセス許可を追加しました。これらのアクセス許可により、最大 500 個の CloudWatch ヘルスチェックメトリクス、最大 100 個のヘルスチェック名の取得、指定された Amazon OpenSearch Service ドメインのドメイン設定の取得、アクティブなリージョンの現在のユーザーが所有するすべての Amazon OpenSearch Service ドメイン名の一覧表示、CloudFront マルチテナントディストリビューションの取得、Lightsail コンテナサービスの取得を行えます。詳細については、「AWS マネージドポリシー: AmazonRoute53FullAccess」を参照してください。

2025 年 4 月 28 日

インターフェイス VPC エンドポイントを Route 53 プロファイルに関連付けることができるようになりました。詳細については、「インターフェイス VPC エンドポイントを Route 53 プロファイルに関連付ける」を参照してください。

2025 年 4 月 28 日

CloudFront ディストリビューションテナントにエイリアスレコードを追加できるようになりました。詳細については、「ドメイン名を使用したトラフィックの Amazon CloudFront ディストリビューションへのルーティング」を参照してください。

2025 年 2 月 27 日

Route 53 ガイドを更新し、Traffic Flow の新しいコンソールエクスペリエンスを追加しました。詳細については、「トラフィックポリシーの作成と管理」および「ポリシーレコードの作成および管理」を参照してください。

2025 年 1 月 14 日

Amazon Route 53 は、OpenSearch Service のカスタムドメインエンドポイントのエイリアスレコードをサポートできるようになりました。詳細については、「Amazon OpenSearch Service ドメインエンドポイントへのトラフィックのルーティング」を参照してください。

2025 年 1 月 13 日

Resolver DNS Firewall の検出結果を Security Hub CSPM に追加しました。詳細については、「Resolver DNS Firewall から Security Hub CSPM に検出結果を送信する」を参照してください。

2024 年のリリース

2024 年 11 月 15 日

Resolver DNS Firewall Advanced を追加しました。これは、DNS トンネリング、ドメイン生成アルゴリズム (DGA)、ディクショナリ DGA ベースの脅威など、高度な DNS 脅威に関連する DNS トラフィックを識別してブロックできる Resolver DNS Firewall の新しい機能セットです。詳細については、「DNS ファイアウォールの詳細ルール」を参照してください。

2024 年 10 月 29 日

HTTPS、SSHFP、SVCB、TLSA DNS レコードタイプのサポートが追加されました。詳細については、「サポートされる DNS レコードタイプ」を参照してください。

2024 年 10 月 3 日

DoH アウトバウンド Resolver エンドポイントのサービス名表示 (SNI) のサポートを追加しました。詳細については、「ルールを作成または編集するときに指定する値」を参照してください。

2024 年 9 月 3 日

`route53:VPCs` ポリシー条件を使用して、VPC へのホストゾーンの関連付けを管理するためのきめ細かなアクセスを許可できるようになりました。詳細については、「詳細に設定されたアクセスコントロールのための IAM ポリシー条件の使用」を参照してください。

2024 年 8 月 27 日

`AmazonRoute53ProfilesFullAccess` は、`GetProfilePolicy` と `PutProfilePolicy` のアクセス許可を追加しました。これらはアクセス許可のみの IAM アクションです。IAM プリンシパルにこれらのアクセス許可が付与されていない場合、 AWS RAM サービスを使用してプロファ

イルを共有しようとするとエラーが発生します。詳細については、「AWS マネージドポリシー: AmazonRoute53ProfilesFullAccess」を参照してください。

2024 年 8 月 27 日

AmazonRoute53ProfilesReadOnlyAccess は GetProfilePolicy のアクセス許可を追加しました。これはアクセス許可のみの IAM アクションです。IAM プリンシパルにこのアクセス許可が付与されていない場合、 AWS RAM サービスを使用してプロファイルのポリシーにアクセスしようとするとエラーが発生します。詳細については、「AWS マネージドポリシー: AmazonRoute53ProfilesReadOnlyAccess」を参照してください。

2024 年 8 月 5 日

マネージドポリシー AmazonRoute53ResolverFullAccess を一意に識別するためのステートメント ID (Sid) を追加しました。詳細については、「AWS マネージドポリシー: AmazonRoute53ResolverFullAccess」を参照してください。

2024 年 8 月 5 日

マネージドポリシー AmazonRoute53ResolverReadOnlyAccess を一意に識別するためのステートメント ID (Sid) を追加しました。詳細については、「AWS マネージドポリシー: AmazonRoute53ResolverReadOnlyAccess」を参照してください。

2024 年 7 月 18 日

ヘルスチェックの新しいコンソールエクスペリエンスで Route 53 ガイド全体を更新しました。詳細については、「ヘルスチェックの作成、更新、削除」を参照してください。

2024 年 4 月 30 日

DNS ファイアウォールルールが DNS リダイレクトチェーンを検査 (デフォルト) する、または信頼するのいずれかを決定できるようになりました。詳細については、「Resolver DNS Firewall のコンポーネントと設定」および「DNS Firewall のルール設定」を参照してください。

2024 年 4 月 22 日

Route 53 Profiles を使用して、DNS 固有の設定を多数の VPCs および AWS アカウントと共有できるようになりました。詳細については、「Amazon Route 53 プロファイルとは」を参照してください。

2024 年 4 月 22 日

Amazon Route 53 プロファイルへの読み取り専用アクセスおよびフルアクセスを付与するマネージドポリシー AmazonRoute53ProfilesReadOnlyAccess と

`AmazonRoute53ProfilesFullAccess` を追加しました。詳細については、「AWS Amazon Route 53 の マネージドポリシー」を参照してください。

2024 年 2 月 5 日

Amazon EventBridge を使用して、DNS ファイアウォールでのリアルタイムアラートを行えるようになりました。詳細については、「を使用したリゾルバー DNS ファイアウォールイベントの管理 Amazon EventBridge」を参照してください。

2024 年 1 月 9 日

DNS クエリタイプを DNS ファイアウォールルールのオプション値として使用して、特定の DNS クエリタイプのルールのレスポンスを区別できるようになりました。詳細については、「Resolver DNS Firewall のコンポーネントと設定」および「DNS Firewall のルール設定」を参照してください。

2024 年 1 月 9 日

クイック作成レコードまたはレコードの作成ウィザードを使用して、地理的近接性ルーティングレコードを作成できるようになりました。詳細については地理的近接性ルーティング、地理的近接性レコードに固有の値、および地理的近接性エイリアスレコードに固有の値を参照してください。

2023 年のリリース

2023 年 12 月 20 日

Resolver エンドポイントで DNS over HTTPS を使用できるようになりました。詳細については、「エンドポイントのプロトコルの選択」を参照してください。

2023 年 7 月 20 日

Amazon Route 53 on Outposts が AWS Outposts ラックで利用可能になりました。これには、から送信されるすべての DNS クエリをキャッシュする VPC リゾルバーが含まれています AWS Outposts。インバウンドおよびアウトバウンドエンドポイントをデプロイするとき、Outpost とオンプレミス DNS リゾルバーの間でハイブリッド接続をセットアップすることもできます。詳細については、「Amazon Route 53 on Outposts とは」を参照してください。

2023 年 7 月 19 日

ローカルゾーンを有効にした後、ローカルゾーンと地理的近接性ルーティング (トラフィックフローのみ) を使用できるようになりました。詳細については、「地理的近接性ルーティング」と「トラフィックポリシーのドキュメント形式」を参照してください。

2023 年 3 月 22 日

Route 53 ガイド全体でドメインの新しいコンソール体験を更新しました。新しいコンソールエクスペリエンスを使用して、ドメイン AWS アカウント を 間で転送することもできます AWS アカウント。詳細については、「新しいドメインの登録」および「ドメインの移管」を参照してください。

2023 年 3 月 10 日

Route 53 VPC Resolver で IPv4、IPv6、またはデュアルスタックエンドポイントを使用してリソースに接続できるようになりました。詳細については、「インバウンドエンドポイントを作成または編集するときに指定する値」および「アウトバウンドエンドポイントを作成または編集するときに指定する値」を参照してください。

2022 年のリリース

2022 年 9 月 21 日

今後は、ポリシー条件を使用することで、Amazon Route 53 内で更新中のリソースレコードセットに対する、より詳細なアクセス権をユーザーに付与できます。詳細については、「詳細に設定されたアクセスコントロールのための IAM ポリシー条件の使用」を参照してください。

2022 年 8 月 30 日

Amazon Route 53 は、2022 年 8 月 1 日以降に作成された AWS App Runner サービスのエイリアスレコードをサポートするようになりました。詳細については、「AWS App Runner サービスへのトラフィックのルーティング」を参照してください。

2022 年 6 月 1 日

Amazon Route 53 で IP ベースのルーティングオプションが利用可能になりました。詳細については、「IP ベースルーティング」を参照してください。

2022 年 3 月 16 日

Amazon Route 53 のプライベートホストゾーンで、地理位置情報およびレイテンシーベースのルーティングオプションがサポートされるようになりました。詳細については、「プライベートホストゾーンを使用する場合の考慮事項」を参照してください。

2022 年 1 月 25 日

「.com.au」および「.net.au」TLD の所有権を変更するプロセスは、2 つの電子メールへの返信 (古い登録者と新しい登録者の両方による) を含む内容に簡素化されており、フォーム入力は含ま

れていません。詳細については、「.com.au (オーストラリア)」および「.net.au (オーストラリア)」を参照してください。

2021 年のリリース

2021 年 10 月 26 日

Amazon Route 53 でデフォルトの逆引き DNS ルールを無効にするためのサポートが追加されました。これらのルールの作成を無効にし、代わりに逆引き DNS 名前空間のクエリを必要な場合に外部サーバーに転送できるようになりました。詳細については、「VPC Resolver でのリバース DNS クエリの転送ルール」を参照してください。

2021 年 9 月 1 日

静的ウェブサイト用の Amazon CloudFront ディストリビューションの作成手順を説明する新しい入門トピックを追加。詳細については、「Amazon CloudFront ディストリビューションを使用して静的なウェブサイトを提供する」を参照してください。

2021 年 7 月 14 日

Amazon Route 53 AWS の管理ポリシーの追跡を開始しました。詳細については、「AWS Amazon Route 53 の マネージドポリシー」を参照してください。

2021 年 3 月 31 日

Resolver DNS Firewall を追加しました。DNS Firewall を使うと、VPC からのアウトバウンド DNS リクエストを保護できます。詳細については、「DNS ファイアウォールを使用してアウトバウンド DNS トラフィックをフィルタリングする」を参照してください。

2020 年のリリース

2020 年 12 月 17 日

Route 53 VPC Resolver の DNSSEC 署名のサポートが追加されました。詳細については、「Amazon Route 53 での DNSSEC 署名の設定」を参照してください。

Route 53 VPC Resolver の DNSSEC 検証のサポートが追加されました。詳細については、「Amazon Route 53 での DNSSEC 検証の有効化」を参照してください。

2020 年 9 月 23 日

新しいコンソールエクスペリエンスで Route 53 ガイド全体が更新されました。詳細については、「Amazon Route 53 とは？」を参照してください。

2020 年 9 月 1 日

Resolver のクエリログのサポートを追加 詳細については、「リゾルバーでのクエリのログ記録」を参照してください。

2018 年のリリース

2018 年 12 月 20 日

API Gateway API、または Amazon VPC インターフェイスエンドポイントにトラフィックをルーティングする、Route 53 エイリアスレコードを作成できます。詳細については、「への値/ルートトラフィック」を参照してください。

2018 年 11 月 28 日

Route 53 Auto Naming (Service Discovery とも呼ばれる) が別のサービスになりました AWS Cloud Map。詳細については、AWS Cloud Map デベロッパーガイドを参照してください。

2018 年 11 月 19 日

Route 53 Resolver を使用して、Direct Connect または VPN 接続を介して VPC とネットワーク間の DNS 解決を設定できます。(Resolver は、Amazon Virtual Private Cloud (Amazon VPC) ですべてのお客様にデフォルトで提供される再帰 DNS サービスの新しい名称です)。これにより、ネットワーク上のリゾルバーからの DNS クエリを、Route 53 Resolver に転送することが可能になります。Resolver を使用すると、選択したドメイン名 (example.com) およびサブドメイン名 (api.example.com) に対するクエリを VPC からネットワーク上のリゾルバーに転送することもできます。詳細については、「Route 53 VPC Resolver とは」を参照してください。

2018 年 11 月 7 日

Route 53 トラフィックフローと地理的近接性ルーティングを使用している場合は、インタラクティブマップを使用して、エンドユーザーが世界中のエンドポイントにどのようにルーティングされるかを可視化できます。詳細については、「地理的近接性の設定の効果を示す地図の表示」を参照してください。

2018 年 10 月 18 日

Route 53 コンソールと API を使用して、Route 53 ヘルスチェックを一時的に無効にすることができます。これにより、ウェブサーバーなどのエンドポイントのモニタリングを一時停止する簡単な方法を得られるため、アラームを起動したり、不要なログやステータスメッセージを生成したりすることなく、エンドポイントのメンテナンスを実行できます。詳細については、「ヘルスチェックを作成または更新するときに指定する値」の「無効化」を参照してください。この機能は、エンドポイントをモニタリングするヘルスチェック、他のヘルスチェックをモニタリングするヘルスチェック、CloudWatch アラームをモニタリングするヘルスチェックの 3 種類すべての Route 53 ヘルスチェックで使用可能です。

2018 年 3 月 13 日

自動命名を使用している場合は、サードパーティーのヘルスチェッカーを使用してリソースのヘルスを評価できるようになりました。これは、インスタンスが Amazon VPC に存在するなどの理由でインターネット上でリソースを利用できない場合に役立ちます。詳細については、Amazon Route 53 API リファレンスの「HealthCheckCustomConfig」を参照してください。。

2018 年 3 月 9 日

自動命名用の管理ポリシーが IAM に追加されました。詳細については、「AWS Amazon Route 53 の マネージドポリシー」を参照してください。

2018 年 2 月 6 日

ELB ロードバランサーにトラフィックをルーティングするエイリアスレコードを作成するか、CNAME レコードを作成するように自動命名を設定できるようになりました。詳細については、Amazon Route 53 API リファレンスの RegisterInstance API に関する項目で「属性」を参照してください。

2017 年のリリース

2017 年 5 月 12 日

Route 53 自動命名 API を使用して、マイクロサービス用のインスタンスをプロビジョニングできるようになりました。自動命名では、定義したテンプレートに基づいて、DNS レコードとオプションでヘルスチェックを自動的に作成できます。詳細については、AWS 「 クラウドマップとは」を参照してください。 「 AWS Cloud Map デベロッパーガイド」の「

2017 年 11 月 16 日

ホストゾーンやヘルスチェックなど、Route 53 リソースの現在のクォータと、現在使用している各リソースの数をプログラムで取得できるようになりました。詳細については、Amazon Route 53 API リファレンスの「GetAccountLimit」、「GetHostedZoneLimit」、および「GetReusableDelegationSetLimit」を参照してください。

2017 年 10 月 3 日

Route 53 が HIPAA 対象のサービスになりました。詳細については、「Amazon Route 53 のコンプライアンス検証」を参照してください。

2017 年 9 月 29 日

ドメインを Route 53 に移管できるかどうかを、プログラムで確認できるようになりました。詳細については、Amazon Route 53 API リファレンスの「CheckDomainTransferability」を参照してください。

2017 年 9 月 11 日

インターネットトラフィックを、Elastic Load Balancing のネットワークロードバランサーにルーティングする、Route 53 エイリアスレコードを作成できるようになりました。エイリアスレコードの詳細については、「エイリアスレコードと非エイリアスレコードの選択」を参照してください。

2017 年 9 月 7 日

パブリックで信頼できる DNS サービスとして Route 53 を使用している場合は、Route 53 により受信される DNS クエリのログ記録が可能になりました。詳細については、「パブリック DNS クエリのログ記録」を参照してください。

2017 年 9 月 1 日

Route 53 トラフィックフローを使用している場合は、地理的近接性ルーティングを使用できるようになりました。これにより、ユーザーとリソース間の物理的な距離に基づいてトラフィックをルーティングできます。また、正または負のバイアスを指定して、各リソースに多かれ少なかれトラフィックをルーティングすることもできます。詳細については、「地理的近接性ルーティング」を参照してください。

2017 年 8 月 21 日

Route 53 を使用して、ドメインおよびサブドメインの証明書を発行する認証機関を指定するための、認証機関の承認 (CAA) レコードを作成できるようになりました。詳細については、「CAA レコードタイプ」を参照してください。

2017 年 8 月 18 日

Route 53 コンソールを使用して、多数のドメインを Route 53 に転送できるようになりました。詳細については、「ドメイン登録の Amazon Route 53 への移管」を参照してください。

2017 年 8 月 4 日

ドメインを登録するときに、一部の最上位ドメイン (TLD) のレジストリで、登録者の連絡先に有効な電子メールアドレスを指定したことを確認する必要があります。確認メールを送信して、ドメイン登録プロセス中にメールアドレスを正常に検証したことを確認できます。詳細については、「新しいドメインの登録」を参照してください。

2017 年 6 月 21 日

複数のリソース (ウェブサーバーなど) に対し、トラフィックをほぼランダムにルーティングする場合、各リソースのために複数値回答のレコードを 1 つ作成できるようになりました。また必要に応じて、各レコードに Route 53 ヘルスチェックを関連付けることもできます。Route 53 は、DNS クエリへの応答に、各クエリに対応した最大 8 つの正常なレコードを使用します。また、それぞれのDNS リゾルバーには異なる回答を返します。詳細については、「複数値回答ルーティング」を参照してください。

2017 年 4 月 10 日

Route 53 コンソールを使用して Route 53 にドメイン登録を移管する場合に、ドメインの DNS サービスのネームサーバーを、移管されたドメイン登録に関連付けるための、次のいずれかのオプションが選択できるようになりました。

- 選択した Route 53 のホストゾーンのネームサーバーを使用する
- ドメインの現在の DNS サービスのネームサーバーを使用する
- 指定したネームサーバーを使用する

Route 53 は、これらのネームサーバーを、移管されたドメイン登録と自動的に関連付けます。

2016 年のリリース

2016 年 11 月 21 日

エンドポイントのヘルスチェックをするために、IPv6 アドレスを使用したヘルスチェックを作成できるようになりました。詳細については、「ヘルスチェックの作成と更新」を参照してください。

2016 年 11 月 15 日

Route 53 API アクションを使用して、別のアカウントで作成したプライベートホストゾーンを使用するアカウントで作成した Amazon VPC での、関連付けが行えるようになりました。詳細については、「Amazon VPC と、作成したプライベートホストゾーンを異なる AWS アカウントに関連付ける」を参照してください。

2016 年 8 月 30 日

このリリースの Route 53 には、次の新機能が追加されています。

- 名前付け権限ポインタ (NAPTR) レコード – ある値を別の値に変換したり、ある値を別の値で置き換えたりするための、動的委任発見システム (DDDS) アプリケーションが使用する NAPTR レコードを作成できるようになりました。例えば、1 つの一般的な用途は、電話番号を SIP URI に変換する場合です。詳細については、「NAPTR レコードタイプ」を参照してください。
- DNS クエリのテストツール – レコードの DNS クエリをシミュレートして、Route 53 が返す値を表示することができるようになりました。位置情報およびレイテンシーレコードの場合、特定の DNS リゾルバーおよび (または) クライアント IP アドレスからのリクエストをシミュレートして、そのリゾルバーまたは IP アドレスを使用して Route 53 がクライアントに返すレスポンスを調べることもできます。詳細については、「Route 53 からの DNS 応答の確認」を参照してください。

2016 年 8 月 11 日

このリリースでは、ELB アプリケーションロードバランサーにトラフィックをルーティングするアリアスレコードを作成できます。このプロセスは、Classic ロードバランサーと同様です。詳細については、「への値/ルートトラフィック」を参照してください。

2016 年 8 月 9 日

このリリースでは、DNSSEC のドメイン登録に関するサポートが、Route 53 に追加されました。DNSSEC は、DNS のなりすまし攻撃 (中間者攻撃とも呼ばれる) からドメインを保護するために役立ちます。詳細については、「ドメインの DNSSEC の設定」を参照してください。

2016 年 7 月 7 日

ドメインの登録を手動で延長して、レジストリから特定される最低登録期間よりも長い初期登録期間のドメインを登録できるようになりました。詳細については、「ドメインの登録期間の延長」を参照してください。

2016 年 7 月 6 日

インドに連絡先がある AISPL のお客様も、Route 53 を使用したドメインの登録ができるようになりました。詳細については、「Managing an Account in India」を参照してください。

2016 年 5 月 26 日

このリリースの Route 53 には、次の新機能が追加されています。

- ドメイン請求レポート – 指定した期間のドメイン登録に関わるすべての料金が、ドメインごとに一覧表示されるレポートをダウンロードできます。このレポートには、料金が発生するすべてのドメイン登録オペレーションが含まれます。ドメインの登録、ドメインの Route 53 への転送、ドメイン登録の更新、およびドメイン所有者の変更 (一部の TLD の場合)などが含まれます。詳細については、次のドキュメントを参照してください。
  - Route 53 コンソール –「ドメイン請求レポートのダウンロード」を参照してください。
  - Route 53 API – Amazon Route 53 API リファレンスの「ViewBilling」を参照してください。
- 新しい TLD – 次の TLD を含むドメインを登録できるようになりました。TLD: .college、.consulting、.host、.name、.online、.republican、.rocks、.sucks、.trade、.websit
詳細については、「Amazon Route 53 に登録できる最上位ドメイン」を参照してください。
- ドメイン登録用の新しい API – 新規ドメインの登録など、登録者の連絡用 E メールアドレスが有効であるかどうかの確認を必要とするオペレーションでは、登録者の連絡先で確認メールのリンクがクリックされたかどうか、クリックしていない場合はリンクが有効かどうかを、プログラムで検証できます。また、別の確認用 E メールの送信をプログラムでリクエストできます。詳細については、Amazon Route 53 API リファレンスで、次のドキュメントを参照してください。
  - GetContactReachabilityStatus
  - ResendContactReachabilityEmail

2016 年 4 月 5 日

このリリースの Route 53 には、次の新機能が追加されています。

- CloudWatch メトリクスに基づくヘルスチェック – CloudWatch メトリクスのアラーム状態に基づくヘルスチェックを作成できるようになりました。これは、プライベート IP アドレスしか割り当てられていない Amazon Virtual Private Cloud (VPC) 内のインスタンスなど、標準の Route 53 ヘルスチェックでは到達できないエンドポイントの正常性をチェックする場合に有用です。詳細については、次のドキュメントを参照してください。
  - Route 53 コンソール –「ヘルスチェックを作成または更新するときに指定する値」トピックの「CloudWatch アラームのモニタリング」を参照してください。

  - Route 53 API – Amazon Route 53 API リファレンスの「CreateHealthCheck」および「UpdateHealthCheck」を参照してください。
- 設定可能なヘルスチェックロケーション – リソースの正常性をチェックする場合に、Route 53 がヘルスチェックの対象とするリージョンを選択できるようになりました。これにより、ヘルスチェックによりエンドポイントで生じる負荷を抑えることができます。これは、顧客が 1 つまたは少数の地理的リージョンに集中している場合に便利です。詳細については、次のドキュメントを参照してください。
  - Route 53 コンソール –「ヘルスチェックを作成または更新するときに指定する値」トピックの「高度な設定 (「エンドポイントを監視」する場合のみ)」を参照してください。
  - Route 53 API – Amazon Route 53 API リファレンスで、「CreateHealthCheck」および「UpdateHealthCheck」の「`Regions` 要素」を参照してください。
- プライベートホストゾーンのフェイルオーバー – プライベートホストゾーンで、フェイルオーバーレコードおよびフェイルオーバーエイリアスレコードを作成できるようになりました。メトリクスベースのヘルスチェックにこの機能を組み合わせると、プライベート IP アドレスしかなく標準の Route 53 ヘルスチェックでは到達できないエンドポイントについても、DNS フェイルオーバーを設定することができます。詳細については、次のドキュメントを参照してください。
  - Route 53 コンソール –「プライベートホストゾーンのフェイルオーバーの設定」を参照してください。
  - Route 53 API – Amazon Route 53 API リファレンスの「ChangeResourceRecordSets」を参照してください。
- プライベートホストゾーンのエイリアスレコード – 以前は、同じホストゾーン内の他の Route 53 レコードにのみ、DNS クエリをルーティングするエイリアスレコードを作成することができました。このリリースでは、ローカル化されたサブドメインがある Elastic Beanstalk 環境、Elastic Load Balancing のロードバランサー、および Amazon S3 バケットにも、DNS クエリをルーティングするためのエイリアスレコードを作成することができます。(CloudFront ディストリビューションに DNS クエリをルーティングするエイリアスレコードを作成することはできません) 詳細については、次のドキュメントを参照してください。
  - Route 53 コンソール –「エイリアスレコードと非エイリアスレコードの選択」を参照してください。
  - Route 53 API – Amazon Route 53 API リファレンスの「ChangeResourceRecordSets」を参照してください。

2016 年 2 月 23 日

HTTPS ヘルスチェックを作成または更新する場合、TLS ネゴシエーション中にエンドポイントにホスト名を送信するよう、Route 53 を設定できるようになりました。これにより、エンドポイントは該当する SSL/TLS 証明書で HTTPS リクエストに応答することができます。詳細については、「ヘルスチェックを作成または更新するときに指定する値」トピックの 高度な設定 (「エンドポイントを監視」する場合のみ) フィールドの SNI の説明を参照してください。API を使用してヘルスチェックを作成または更新する際、SNI を有効にする方法については、Amazon Route 53 API リファレンスの「CreateHealthCheck」および「UpdateHealthCheck」を参照してください。

2016 年 1 月 27 日

これにより、.accountants、.band、.city など、100 以上の追加の最上位ドメイン (TLD) のドメインを登録することができます。サポートされる TLD の完全なリストについては、「Amazon Route 53 に登録できる最上位ドメイン」を参照してください。

2016 年 1 月 19 日

これにより、Elastic Beanstalk 環境にトラフィックをルーティングするエイリアスレコードを作成できます。Route 53 コンソールを使用したレコード作成の詳細については、「Amazon Route 53 コンソールを使用したレコードの作成」を参照してください。API を使用したレコード作成の詳細については、Amazon Route 53 API リファレンスの「ChangeResourceRecordSets」を参照してください。

2015 年のリリース

2015 年 12 月 3 日

Route 53 コンソールに含まれるようになったビジュアルエディターでは、Route 53 の加重、レイテンシー、フェイルオーバー、および地理的位置情報のルーティングポリシーを組み合わせて使用する、複雑なルーティング設定を迅速に作成することができます。その後、設定を、同じホストゾーンまたは複数のホストゾーンで 1 つ以上のドメイン名 (example.com など) またはサブドメイン名 (www.example.com など) に関連付けることができます。さらに、新しい設定が期待どおりに機能していない場合は、更新を元に戻すことができます。Route 53 API、AWS SDKs、、および を使用して AWS CLI、同じ機能を使用できます AWS Tools for Windows PowerShell。ビジュアルエディターの詳細については、「DNS トラフィックのルーティングにトラフィックフローを使用する」を参照してください。API を使用してトラフィックフロー設定を作成する方法の詳細については、Amazon Route 53 API リファレンスを参照してください。

2015 年 10 月 19 日

このリリースの Route 53 には、次の新機能が追加されています。

- Amazon Registrar, Inc. による .com および .net ドメインのドメイン登録 – Amazon は Amazon Registrar, Inc. を通じて .com および .net トップレベルドメイン (TLD) の ICANN 認定レジストラとなりました。Route 53 を使用して .com または .net ドメインを登録すると、Amazon Registrar がレコードのレジストラとなり、WHOIS クエリの結果に「Sponsoring Registrar」として一覧表示されます。Route 53 を使用したドメインの登録の詳細については、「Amazon Route 53 を使用したドメインの登録と管理」を参照してください。
- .com および .net ドメインでのプライバシー保護 – Route 53 で .com または .net ドメインを登録する場合、姓名を含むすべての個人情報は非表示になります。他のドメインを Route 53 で登録する場合には、姓名は非表示ではありません。プライバシー保護については、「ドメインの連絡先情報のプライバシー保護の有効化/無効化」を参照してください。

2015 年 9 月 15 日

このリリースの Route 53 には、次の新機能が追加されています。

- 計算されたヘルスチェック – 他のヘルスチェックの状態によってステータスが決定されるヘルスチェックを作成できるようになりました。詳細については、「ヘルスチェックの作成と更新」を参照してください。また、Amazon Route 53 API リファレンスの「CreateHealthCheck」もご確認ください。
- ヘルスチェックのレイテンシー測定 – ヘルスチェッカーとエンドポイント間のレイテンシーを測定するように、Route 53 を設定できるようになりました。レイテンシーデータは、Route 53 コンソール上で、Amazon CloudWatch のグラフに表示されます。新しいヘルスチェックのレイテンシー測定を有効にする場合は、トピック「ヘルスチェックを作成または更新するときに指定する値」の「高度な設定 (「エンドポイントを監視」する場合のみ)」で、[Latency measurements] (レイテンシー測定) 設定をご確認ください。(既存のヘルスチェックについてはレイテンシーの測定を有効にできません。) また、Amazon Route 53 API リファレンスの「CreateHealthCheck」トピックで「MeasureLatency」についてもお読みください。
- Route 53 コンソールでのヘルスチェックダッシュボードの更新 – ヘルスチェックをモニタリングするためのダッシュボードには、例えば、Route 53 ヘルスチェッカーとエンドポイント間でのレイテンシーを監視するための CloudWatch グラフなど、さまざまな形での改良が加えられています。詳細については、「ヘルスチェックのステータス監視と通知の受信」を参照してください。

2015 年 3 月 3 日

Amazon Route 53 デベロッパーガイドでは、Route 53 ホストゾーンのホワイトラベルネームサーバーの設定方法が新たに解説されています。詳細については、「ホワイトラベルネームサーバーの設定」を参照してください。

2015 年 2 月 26 日

Route 53 API を使用して、 AWS アカウントに関連付けられているホストゾーンを名前順に一覧表示できるようになりました。あるアカウントに関連付けられたホストゾーンの数も取得できます。詳細については、Amazon Route 53 API リファレンスの「ListHostedZonesByName」および「GetHostedZoneCount」を参照してください。

2015 年 2 月 11 日

このリリースの Route 53 には、次の新機能が追加されています。

- ヘルスチェックステータス – Route 53 コンソールのヘルスチェックページに、すべてのヘルスチェックのステータスを包括的に表示するための、[Status (ステータス)] 列が追加されました。詳細については、「ヘルスチェックのステータスと失敗理由を表示する」を参照してください。
- との統合 AWS CloudTrail – Route 53 は CloudTrail と連携して、 AWS アカウントが Route 53 API に送信するすべてのリクエストに関する情報をキャプチャするようになりました。Route 53 と CloudTrail を統合することで、Route 53 API に対して実行されたリクエストの種類、リクエストの実行元 IP アドレス、実行者、実行日時、その他を判断できます。詳細については、「を使用した Amazon Route 53 API コールのログ記録 AWS CloudTrail」を参照してください。
- ヘルスチェックのクイックアラーム – Route 53 コンソールを使用してヘルスチェックを作成する際に、ヘルスチェックの Amazon CloudWatch アラームも同時に作成すると、エンドポイントの異常が 1 分間継続したと Route 53 が判断した場合に通知が送られるユーザーを指定できます。詳細については、「ヘルスチェックの作成と更新」を参照してください。
- ホストゾーンとドメインのタグ付け – 一般にコスト配分のために使用されるタグを、Route 53 ホストゾーンとドメインに付けることができるようになりました。詳細については、「Amazon Route 53 リソースのタグ付け」を参照してください。

2015 年 2 月 5 日

Route 53 コンソールを使用して、ドメインの連絡先情報を更新できるようになりました。詳細については、「ドメインを登録または移管するときに指定する値」を参照してください。

2015 年 1 月 22 日

Route 53 に新しいドメイン名を登録する際に、国際化ドメイン名も指定できるようになりました。(Route 53 は既にホストゾーンおよびレコードで国際化ドメイン名をサポートしています) 詳細については、「DNS ドメイン名の形式」を参照してください。

2014 年のリリース

2014 年 11 月 25 日

このリリースでは、ホストゾーンの作成時に指定したコメントを編集できるようになりました。コンソールで、コメントフィールドの横にある鉛筆アイコンを選択し、新しい値を入力します。Route 53 API を使用してコメントを変更する方法の詳細については、Amazon Route 53 API リファレンスの「UpdateHostedZoneComment」を参照してください。

2014 年 11 月 5 日

このリリースの Route 53 には、次の新機能が追加されています。

- Amazon Virtual Private Cloud サービスを使用して作成された VPC 用のプライベート DNS – Route 53 を使用して、DNS データをパブリックインターネットに公開することなく、VPC の内部ドメイン名を管理できるようになりました。詳細については、「プライベートホストゾーンの使用」を参照してください。
- ヘルスチェックの失敗理由 – 選択したヘルスチェックの現在のステータスに加えて、Route 53 の各ヘルスチェッカーからレポートされたヘルスチェックでの最後の失敗理由を、詳細に表示できるようになりました。ステータスには HTTP ステータスコードが含まれ、失敗理由には、文字列の不一致やレスポンスのタイムアウトなど、さまざまな種類の失敗に関する情報が含まれます。詳細については、「ヘルスチェックのステータスと失敗理由を表示する」を参照してください。
- 再利用可能な委託セット – 委託セットと総称される 4 つの権威ネームサーバーのセットを、異なるドメイン名に対応する複数のホストゾーンにも適用できるようになりました。これにより、DNS サービスを Route 53 に移行し、多数のホストゾーンを管理するプロセスが大幅に簡素化されます。現在、再利用可能な委託セットを使用するには、Route 53 API または AWS SDK を活用する必要があります。詳細については、「Amazon Route 53 API リファレンス」を参照してください。
- 位置情報ルーティングの向上 – EDNS0 の edns-client-subnet 拡張機能に対するサポートが追加されたことで、位置情報ルーティングの精度がさらに向上しました。詳細については、「位置情報ルーティング」を参照してください。

- 署名 v4 のサポート – 署名バージョン 4 を使用して、すべての Route 53 API リクエストに署名できるようになりました。詳細については、Amazon Route 53 API リファレンスの「Signing Route 53 API Requests (Route 53 API リクエストへの署名)」を参照してください。

2014 年 7 月 31 日

このリリースでは、次のことを実行できます。

- Route 53 を使用してドメイン名を登録できます。詳細については、「Amazon Route 53 を使用したドメインの登録と管理」を参照してください。
- クエリの発進元の地理的場所に基づいて DNS クエリに応答するように Route 53 を設定します。詳細については、「位置情報ルーティング」を参照してください。

2014 年 7 月 2 日

このリリースでは、次のことを実行できます。

- ヘルスチェックでのほとんどの値を編集できます。詳細については、「ヘルスチェックの作成、更新、削除」を参照してください。
- Route 53 API を使用して、リソースの正常性を確認する際に Route 53 ヘルスチェッカーで使用される IP 範囲のリストを取得できます。これらの IP アドレスを使用して、ヘルスチェッカーでリソースの正常性を確認できるようにルーターとファイアウォールのルールを設定できます。詳細については、Amazon Route 53 API リファレンスの「GetCheckerIpRanges」を参照してください。
- ヘルスチェックにコスト配分タグを割り当てることができます。これにより、ヘルスチェックに名前を割り当てることが可能になります。詳細については、「ヘルスチェックの名前付けとタグ付け」を参照してください。
- Route 53 API を使用して、 AWS アカウントに関連付けられているヘルスチェックの数を取得します。詳細については、Amazon Route 53 API リファレンスの「GetHealthCheckCount」を参照してください。

2014 年 4 月 30 日

このリリースでは、ヘルスチェックを作成し、IP アドレスの代わりにドメイン名を使用してエンドポイントを指定できます。これは、エンドポイントの IP アドレスが固定されていない場合、または複数の IP (Amazon EC2 インスタンスや Amazon RDS インスタンスなど) がエンドポイントの IP アドレスとして提供される場合に役立ちます。詳細については、「ヘルスチェックの作成と更新」を参照してください。

また、以前は Amazon Route 53 デベロッパーガイドに記載されていた、Route 53 API の使用に関する情報の一部が移動しました。現在、API に関するすべてのドキュメントは、Amazon Route 53 API リファレンスに集約されています。

2014 年 4 月 18 日

今回のリリースの Route 53 では、ヘルスチェックの [Port (ポート)] 値が [443] で、[Protocol (プロトコル)] 値が [HTTPS] である場合、Host ヘッダーには異なる値が渡されます この場合のヘルスチェックを行う際、Route 53 は、Host ヘッダーに [Host Name (ホストネーム)] フィールドの値を格納してエンドポイントに渡します。CreateHealthCheck API アクションを使用してヘルスチェックを作成した場合、この値は、FullyQualifiedDomainName 要素の値になります。

詳細については、「ヘルスチェックの作成、更新、削除」を参照してください。

2014 年 4 月 9 日

このリリースでは、エンドポイントが現在正常であることを報告している Route 53 ヘルスチェッカーの割合を表示できます。

また、Amazon CloudWatch のヘルスチェックステータスメトリクスには、0 (指定した期間でエンドポイントが異常であった場合) または 1 (該当する期間でエンドポイントが正常であった場合) のみが示されます。このメトリクスでは、エンドポイントが正常であると報告している Route 53 ヘルスチェックの割合を反映した、0 から 1 の間の値は示されなくなりました。

詳細については、「CloudWatch を使用したヘルスチェックのモニタリング」を参照してください。

2014 年 2 月 18 日

このリリースの Route 53 には、次の機能が追加されています。

- ヘルスチェックフェイルオーバーのしきい値: Route 53 がエンドポイントを異常と見なすために、エンドポイントのヘルスチェックが連続で何回不合格となる必要があるかを指定できます。1 ~ 10 回の回数を指定します。異常なエンドポイントが正常と見なされるには、同じ回数のチェックに合格する必要があります。詳細については、「Amazon Route 53 でヘルスチェックの正常性を判断する方法」を参照してください。
- ヘルスチェックリクエストの間隔: エンドポイントが正常であるかどうかを判断するために、Route 53 がエンドポイントにリクエストを送信する頻度を指定できます。有効な設定値は、10 秒と 30 秒です。詳細については、「Amazon Route 53 でヘルスチェックの正常性を判断する方法」を参照してください。

2014 年 1 月 30 日

このリリースの Route 53 には、次の機能が追加されています。

- HTTP と HTTPS に関する文字列一致のヘルスチェック: Route 53 で、指定された文字列がレスポンス本文に示されているかどうかにより、エンドポイントの正常性を判断するヘルス

チェックがサポートされました。詳細については、「Amazon Route 53 でヘルスチェックの正常性を判断する方法」を参照してください。

- HTTPS ヘルスチェック: – この Route 53 では、SSL のみでのアクセスが可能な、保護されたウェブサイトに対するヘルスチェックが サポートされました。詳細については、「Amazon Route 53 でヘルスチェックの正常性を判断する方法」を参照してください。
- **`ChangeResourceRecordSets`** API アクションの **`UPSERT`**: `ChangeResourceRecordSets` API アクションを使用してレコードの作成や変更を行うとき、UPSERT アクションを使用して、特定の名前やタイプのレコードがない場合に新しいレコードを作成したり、既存のレコードを更新したりすることができます。詳細については、Amazon Route 53 API リファレンスの「ChangeResourceRecordSets」を参照してください。

2014 年 1 月 7 日

このリリースの Route 53 で、指定された文字列がレスポンス本文に示されているかどうかに基づいてエンドポイントの正常性を判断するヘルスチェックが、サポートされるようになりました。詳細については、「Amazon Route 53 でヘルスチェックの正常性を判断する方法」を参照してください。

2013 年のリリース

2013 年 8 月 14 日

このリリースの Route 53 で、BIND 形式のゾーンファイルをインポートしてレコードを作成できるようになりました。詳細については、「ゾーンファイルをインポートしてレコードを作成する」を参照してください。

また、Route 53 ヘルスチェックの CloudWatch メトリクスが、Route 53 コンソールに統合され、効率化されました。詳細については、「CloudWatch を使用したヘルスチェックのモニタリング」を参照してください。

2013 年 6 月 26 日

この Route 53 のリリースでは、ヘルスチェックと CloudWatch メトリクスを統合するための機能が追加され、次のことが可能になりました。

- ヘルスチェックが適切に設定されているかどうかを確認できます。
- 指定した期間におけるヘルスチェックのエンドポイントの正常性を確認できます。

- CloudWatch を設定することで、指定したエンドポイントに異常があるとすべての Route 53 ヘルスチェッカーが判断した場合、Amazon Simple Notification Service (Amazon SNS) アラートを送信できます。

詳細については、「CloudWatch を使用したヘルスチェックのモニタリング」を参照してください。

2013 年 6 月 11 日

このリリースでは、DNS クエリを Amazon CloudFront ディストリビューションの代替ドメイン名にルーティングするエイリアスレコードを作成するためのサポートが、Route 53 に追加されました。この機能は、Zone Apex での代替ドメイン名 (example.com) およびサブドメインの代替ドメイン名 (www.example.com) の両方に対して使用できます。詳細については、「ドメイン名を使用したトラフィックの Amazon CloudFront ディストリビューションへのルーティング」を参照してください。

2013 年 5 月 30 日

このリリースでは、ELB ロードバランサーおよび関連する Amazon EC2 インスタンスの正常性を評価するためのサポートが Route 53 に追加されました。詳細については、「Amazon Route 53 ヘルスチェックの作成」を参照してください。

2013 年 3 月 28 日

ヘルスチェックとフェイルオーバーに関するドキュメントが書き換えられ、使いやすさが向上しました。詳細については、「Amazon Route 53 ヘルスチェックの作成」を参照してください。

2013 年 2 月 11 日

このリリースの Route 53 では、フェイルオーバーとヘルスチェックがサポートされるようになりました。詳細については、「Amazon Route 53 ヘルスチェックの作成」を参照してください。

2012 年のリリース

2012 年 3 月 21 日

このリリースの Route 53 では、レイテンシーレコードを作成できます。詳細については、「レイテンシーに基づくルーティング」を参照してください。

2011 年のリリース

2011 年 12 月 21 日

このリリースでは、 の Route 53 コンソール AWS マネジメントコンソール で、ホストゾーン ID とロードバランサーの DNS 名を手動で入力する代わりに、リストから Elastic Load Balancer を選択してエイリアスレコードを作成できます。この機能に関しては、Amazon Route 53 デベロッパーガイドでご確認ください。

2011 年 11 月 16 日

このリリースでは、 の Route 53 コンソールを使用して AWS マネジメントコンソール 、ホストゾーンの作成と削除、およびレコードの作成、変更、削除を行うことができます。この機能は、Amazon Route 53 デベロッパーガイドで適宜説明されています。

2011 年 10 月 18 日

Amazon Route 53 入門ガイドがAmazon Route 53 デベロッパーガイドにマージされ、また、ユーザビリティを高めるためにデベロッパーガイドの再編が行われました。

2011 年 5 月 24 日

Amazon Route 53 のこのリリースでは、エイリアスレコードが導入されています。この導入により、Zone Apex エイリアスの作成に加え、加重レコード、新しい API (2011-05-05)、サービスレベルアグリーメントの使用が可能になりました。加えて、ベータ版として 6 か月が経過し、Route 53 が一般的に利用可能となっています。詳細については、Amazon Route 53 デベロッパーガイドの Amazon Route 53 製品ページおよび「エイリアスレコードと非エイリアスレコードの選択」を参照してください。

2010 年のリリース

2010 年 12 月 5 日

Amazon Route 53 デベロッパーガイドの初回リリース版です。

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。