Guide du développeur

Amazon Route 53

Version de l'API 2013-04-01

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon Route 53: Guide du développeur

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Les marques commerciales et la présentation commerciale d’Amazon ne peuvent pas être utilisées en relation avec un produit ou un service extérieur à Amazon, d’une manière susceptible d’entraîner une confusion chez les clients, ou d’une manière qui dénigre ou discrédite Amazon. Toutes les autres marques commerciales qui ne sont pas la propriété d’Amazon appartiennent à leurs propriétaires respectifs, qui peuvent ou non être affiliés ou connectés à Amazon, ou sponsorisés par Amazon.

Table of Contents

Qu'est-ce qu'Amazon Route 53 ? ... 1
Fonctionnement de l'enregistrement de domaine ... 3
Acheminement du trafic Internet vers votre site web ou votre application web ... 5
Comment configurer Amazon Route 53 pour acheminer le trafic Internet pour votre domaine ... 5
Comment Amazon Route 53 achemine le trafic de votre domaine ... 7
Comment Amazon Route 53 vérifie l'état de vos ressources ... 8
Concepts Amazon Route 53 ... 10
Concepts d'enregistrement de domaine ... 11
Concepts du système de noms de domaine (DNS) ... 12
Concepts de plan de données et contrôle ... 18
Concepts des surveillances de l'état ... 19
Comment démarrer avec Amazon Route 53 ... 20
Accès à Amazon Route 53 ... 21
AWS Identity and Access Management ... 21
Tarification et facturation Amazon Route 53 ... 22
Travailler avec AWS SDKs ... 22
Premiers pas ... 24
Configuration ... 24
Inscrivez-vous pour un Compte AWS ... 25
Création d’un utilisateur doté d’un accès administratif ... 25
Télécharger les outils ... 27
Utilisation de votre domaine pour un site web statique ... 28
Prérequis ... 29
Étape 1 : Enregistrer un domaine ... 29
Étape 2 : créer un compartiment S3 pour votre domaine racine ... 29
Étape 3 (facultatif) : créer un autre compartiment S3, pour votre sous-domaine ... 30
Étape 4 : configurer votre compartiment de domaine racine pour l'hébergement de site web ... 30
Étape 5 :(facultatif) : configurer votre compartiment de sous-domaine pour la redirection de site web ... 32
Étape 6 : télécharger l'index pour créer le contenu du site web ... 32
Étape 7 : Modifier les paramètres de blocage de l'accès public S3 ... 33
Étape 8 : Attacher une stratégie de compartiment ... 34

Étape 9 : Tester le point de terminaison de domaine 36
Étape 10 : acheminer le trafic DNS pour votre domaine vers le compartiment de votre site web 36
Étape 11 : tester votre site web 39
Étape 12 (facultatif) : utilisez Amazon CloudFront pour accélérer la diffusion de votre contenu 39
Utiliser une CloudFront distribution Amazon pour diffuser un site Web statique 40
Prérequis 41
Étape 1 : Enregistrer un domaine 41
Étape 2 : demander un certificat public 41
Étape 3 : créer un compartiment S3 pour héberger votre sous-domaine 42
Étape 4 : créer un autre compartiment S3, pour votre domaine racine 43
Étape 5 : télécharger des fichiers de site web dans votre compartiment de sous-domaine 44
Étape 6 : configurer votre compartiment de domaine racine pour la redirection de site web ... 45
Étape 7 : créer une CloudFront distribution Amazon pour votre sous-domaine 45
Étape 8 : créer une CloudFront distribution Amazon pour votre domaine racine 47
Étape 9 : Acheminer le trafic DNS de votre domaine vers votre distribution CloudFront 48
Étape 10 : tester votre site web 50
Intégration à d'autres services 52
Journalisation, surveillance et balisage 52
Acheminement du trafic vers d'autres AWS ressources 53
Format de nom de domaine DNS 56
Mise en forme des noms de domaine pour l'enregistrement de noms de domaine 56
Mise en forme des noms de domaine pour les zones hébergées et les enregistrements 56
Utilisation d'un astérisque (*) dans les noms des zones hébergées et des enregistrements 57
Mise en forme des noms de domaine internationalisés 59
Enregistrement et gestion de domaines 61
Enregistrement de nouveaux domaines 62
Enregistrement d'un nouveau domaine 63
Valeurs que vous spécifiez lorsque vous enregistrez ou transférez un domaine 70
Valeurs renvoyées par Amazon Route 53 lorsque vous enregistrez un domaine 77
Affichage du statut de l'enregistrement d'un domaine 79
Mise à jour des paramètres d'un domaine 80
Mise à jour des informations de contact et de la propriété pour un domaine 81
Activation ou désactivation de la protection de la confidentialité pour les informations de contact pour un domaine 89

Activation ou désactivation du renouvellement automatique pour un domaine 92
Verrouillage d'un domaine pour empêcher son transfert non autorisé vers un autre bureau d'enregistrement 93
Extension de la période d'enregistrement pour un domaine 94
Mise à jour des serveurs de noms pour utiliser un autre bureau d'enregistrement 96
Ajout ou modification de serveurs de noms et d'enregistrements de type glue pour un domaine 97
Renouvellement d'un enregistrement de domaine 101
Restauration d'un domaine arrivé à expiration ou supprimé 105
Remplacement de la zone hébergée d'un domaine 108
Transfert de domaines 109
Transfert d'un enregistrement de domaine vers Route 53 110
Affichage du statut du transfert d'un domaine 130
Incidence du transfert d'un domaine vers Route 53 sur la date d'expiration 133
Transférer un domaine vers un autre AWS compte 134
Transfert d'un domaine depuis Route 53 138
Transfert du bureau d'enregistrement vers le bureau d'enregistrement Amazon 145
Renvoi des e-mails de confirmation et d'autorisation 146
Mise à jour de votre adresse électronique 147
Renvoi d'e-mails 147
Configuration du protocole DNSSEC pour un domaine 152
Vue d'ensemble de la protection de votre domaine grâce au protocole DNSSEC 153
Prérequis et limites maximales de la configuration du protocole DNSSEC pour un domaine 155
Ajout de clés publiques pour un domaine 155
Suppression de clés publiques pour un domaine 156
Identification de votre bureau d'enregistrement 158
Affichage d'informations sur vos domaines 158
Suppression d'un enregistrement de nom de domaine 160
Contacter le AWS Support à propos de problèmes d'enregistrement de domaine 163
Contacter AWS le Support lorsque vous pouvez vous connecter à votre AWS compte 164
Contacter AWS le Support lorsque vous ne parvenez pas à vous connecter à votre AWS compte 165
Téléchargement d'un rapport de facturation de domaine 165
Domaines que vous pouvez enregistrer avec Amazon Route 53 167
Index vers les domaines de premier niveau pris en charge 168

Domaines de premier niveau génériques ... 171
Domaines géographiques de premier niveau ... 444
Configuration d'Amazon Route 53 en tant que service DNS ... 507
Faire de Route 53 le service DNS d'un domaine existant ... 507
Configuration de Route 53 en tant que service DNS pour un domaine en cours d'utilisation ... 508
Configuration de Route 53 en tant que service DNS d'un domaine inactif ... 518
Configuration du routage DNS pour un nouveau domaine ... 523
Acheminement du trafic vers vos ressources ... 524
Acheminement du trafic pour les sous-domaines ... 525
Utilisation de zones hébergées ... 532
Utilisation de zones hébergées publiques ... 532
Utilisation des zones hébergées privées ... 561
Migration d'une zone hébergée vers un autre compte AWS ... 576
Utilisation des enregistrements ... 587
Sélection d'une stratégie de routage ... 589
Choix entre des enregistrements avec ou sans alias ... 616
Types d'enregistrements DNS pris en charge ... 621
Création d'enregistrements à l'aide de la console Amazon Route 53 ... 643
Autorisations relatives aux ensembles d'enregistrements ... 645
Valeurs que vous spécifiez ... 647
Création d'enregistrements par importation d'un fichier de zone ... 748
Modification des enregistrements ... 751
Suppression d'enregistrements ... 752
Liste des enregistrements ... 753
Configuration de la signature DNSSEC ... 755
Activation de la signature DNSSEC et établissement d'une chaîne d'approbation ... 757
Désactivation de la signature DNSSEC ... 768
Utilisation des clés gérées par le client ... 773
Utilisation de clés de signature () KSKs ... 774
Gestion des clés KMS et ZSK dans Route 53 ... 777
Preuves DNSSEC d'inexistence dans Route 53 ... 779
Résolution des problèmes de signature DNSSEC ... 779
Utilisation AWS Cloud Map pour créer des dossiers et des bilans de santé ... 781
Contraintes et comportements DNS ... 781
Taille de réponse maximale ... 781

Traitement de la section relative à l'autorité ... 781
Traitement de la section supplémentaire ... 782
Flux de trafic ... 783
Avantages de Traffic Flow ... 783
Création et gestion des stratégies de trafic ... 785
Création d'une stratégie de trafic ... 785
Valeurs à spécifier lors de la création d'une stratégie de trafic ... 789
Affichage d'une carte montrant l'effet des paramètres de proximité géographique ... 799
Création de versions supplémentaires d'une stratégie de trafic ... 802
Création d'une politique de trafic à l'aide d'un document JSON ... 806
Affichage des versions de stratégie de trafic et des enregistrements de stratégie associés ... 809
Suppression de versions de stratégie de trafic et de stratégies de trafic ... 813
Création et gestion des enregistrements de stratégie ... 816
Création d'enregistrements de stratégie ... 817
Valeurs à spécifier lors de la création ou de la mise à jour d'un enregistrement de stratégie ... 820
Mise à jour d'enregistrements de stratégie ... 821
Suppression d'enregistrements de stratégie ... 823
Qu'est-ce que Route 53 Resolver ? ... 826
Résolution des requêtes DNS entre VPCs et votre réseau ... 829
Comment les requêtes DNS de votre réseau sont transmises à Resolver ... 832
Comment le point de terminaison Route 53 Resolver transfère les requêtes DNS de vous VPCs vers votre réseau ... 835
Considérations lors de la création de points de terminaison entrants et sortants ... 843
Disponibilité et évolutivité du résolveur Route 53 ... 847
Mise en route avec Route 53 Resolver ... 850
Transférer les requêtes DNS entrantes vers votre VPCs ... 852
Configuration du réacheminement entrant ... 853
Valeurs à spécifier lors de la création ou de la modification de points de terminaison entrants ... 853
Gestion des points de terminaison entrants ... 857
Réacheminement des requêtes DNS sortantes vers votre réseau ... 860
Configuration du réacheminement sortant ... 862
Valeurs à spécifier lors de la création ou de la modification de points de terminaison sortants ... 863
Valeurs à spécifier lors de la création ou de la modification de règles ... 866

Gestion des points de terminaison sortants ... 868
Gestion des règles de réacheminement ... 871
Tutoriel sur les règles de délégation Resolver ... 880
Étapes relatives à la délégation sortante ... 880
Types de délégation ... 881
Activer la validation DNSSEC ... 886
Acheminement du trafic Internet vers vos AWS ressources ... 888
API Amazon API Gateway ... 888
Prérequis ... 889
Configuration de Route 53 pour acheminer le trafic vers un point de terminaison API Gateway ... 890
CloudFront Distribution sur Amazon ... 894
Prérequis ... 895
Configuration d'Amazon Route 53 pour acheminer le trafic vers une CloudFront distribution ... 896
EC2 Instance Amazon ... 898
Prérequis ... 899
Configuration d'Amazon Route 53 pour acheminer le trafic vers une EC2 instance Amazon ... 900
Service App Runner ... 901
Prérequis ... 902
Configuration d'Amazon Route 53 pour acheminer le trafic vers un service App Runner ... 903
Global Accelerator ... 904
Prérequis ... 905
Configuration d'Amazon Route 53 pour acheminer le trafic vers un accélérateur ... 905
AWS Elastic Beanstalk environnement ... 906
Déploiement d'une application dans un environnement Elastic Beanstalk ... 907
Obtention du nom de domaine pour votre environnement Elastic Beanstalk ... 907
Création d'un enregistrement Route 53 ... 908
Équilibreur de charge ELB ... 912
Prérequis ... 912
Configuration d'Amazon Route 53 pour acheminer le trafic vers un équilibreur de charge ELB ... 913
Compartiment Amazon S3 ... 915
Prérequis ... 915
Configuration d'Amazon Route 53 pour acheminer le trafic vers un compartiment S3 ... 917

Point de terminaison d'interface Amazon Virtual Private Cloud 918
Prérequis 919
Point de terminaison de l'interface Amazon VPC 920
Amazon WorkMail 921
Amazon OpenSearch Service 925
Prérequis 925
Configuration d'Amazon Route 53 pour acheminer le trafic vers un point de terminaison OpenSearch de domaine Amazon Service 925
VPC Lattice 927
Prérequis 927
Configuration d'Amazon Route 53 pour acheminer le trafic vers un point de terminaison de domaine du service VPC Lattice 927
Autres AWS ressources 929
Création de bilans de santé 930
Types de surveillances de l'état 931
Comment Route 53 détermine si une surveillance de l'état est saine 933
Comment Route 53 détermine le statut des surveillances de l'état qui surveillent un point de terminaison 933
Comment Route 53 détermine le statut des surveillances de l'état qui surveillent d'autres surveillances de l'état 935
Comment Route 53 détermine l'état des bilans de santé qui surveillent les CloudWatch alarmes 936
Création, mise à jour et suppression de surveillances de l'état 936
Création et mise à jour de surveillances de l'état 938
Valeurs que vous spécifiez lors de la création ou de la mise à jour de surveillances de l'état 940
Valeurs que Route 53 affiche lors de la création d'une surveillance de l'état 968
Mise à jour des bilans de santé lorsque vous modifiez les paramètres CloudWatch d'alarme 968
Activation ou désactivation des bilans de santé 970
Contrôles de santé inversés 971
Suppression de surveillances de l'état 972
Mise à jour ou suppression de surveillances de l'état lorsque le basculement DNS est configuré 973
Configuration des règles de pare-feu et de routeur pour les surveillances de l'état 975
Configuration du basculement DNS 976

Liste des tâches pour configurer le basculement DNS ... 977
Fonctionnement des surveillances de l'état dans les configurations simples ... 979
Fonctionnement des surveillances de l'état dans les configurations complexes ... 983
Choix des enregistrements par Route 53 lorsque la surveillance de l'état est configurée ... 991
Basculement actif-actif et actif-passif ... 994
Configuration du basculement dans une zone hébergée privée ... 998
Prévention des problèmes de basculement par Route 53 ... 999
Attribution de noms et balisage des surveillances de l'état ... 1000
Restrictions liées aux étiquettes ... 1001
Ajout, modification et suppression de balises pour les surveillances de l'état ... 1002
Utilisation des versions d'API antérieures au 2012-12-12 ... 1004
Surveillance du statut de la vérification de l'état et obtention de notifications ... 1006
Affichage du statut des vérifications de l'état et motifs des échecs de vérifications de l'état ... 1006
Surveillance de la latence entre les outils de vérification de l'état et votre point de terminaison ... 1009
Surveillance des bilans de santé à l'aide CloudWatch ... 1013
Afficher l'état de votre bilan de santé ... 1014
Afficher les alarmes de contrôle de santé ... 1017
Afficher les statistiques de contrôle de santé sur la CloudWatch console ... 1020
Créez une alarme avec une notification SNS ... 1020
Route 53 Resolver DNS Firewall ... 1025
Fonctionnement de Route 53 Resolver DNS Firewall ... 1026
Composants et paramètres du pare-feu DNS ... 1026
Comment Route 53 Resolver DNS Firewall filtre les requêtes DNS ... 1030
Étapes de haut niveau pour utiliser DNS Firewall ... 1031
Utilisation de groupes de règles de pare-feu DNS dans plusieurs régions ... 1032
Disponibilité régionale pour le pare-feu DNS ... 1032
Mise en route avec Route 53 Resolver DNS Firewall ... 1034
Exemple de Route 53 Resolver DNS Firewall « walled garden » (jardin fermé) ... 1034
Exemple de liste rouge Route 53 Resolver DNS Firewall ... 1036
Règles et groupes de règles de pare-feu DNS ... 1039
Paramètres de groupe de règles dans le pare-feu DNS ... 1039
Paramètres de règles dans le pare-feu DNS ... 1040
Actions de règle dans le pare-feu DNS ... 1043
Gestion des règles et groupes de règles dans le pare-feu DNS ... 1044
Listes de domaines Route 53 Resolver DNS Firewall ... 1047

Listes de domaines gérées ... 1048
Gestion de vos propres listes de domaines ... 1053
Pare-feu DNS avancé ... 1056
Configuration de la journalisation des requêtes du pare-feu DNS ... 1057
Partage de groupes de règles entre comptes ... 1060
Activation des protections de pare-feu DNS pour votre VPC ... 1063
Gestion des associations entre votre VPC et le groupe de règles de pare-feu ... 1063
Configuration de VPC du pare-feu DNS ... 1064
Que sont les profils Amazon Route 53 ? ... 1066
Priorisation des profils ... 1067
Disponibilité du profil ... 1067
Utilisation de profils ... 1067
Création d'un profil ... 1068
Associer des groupes de règles de pare-feu DNS ... 1070
Associer des zones hébergées privées ... 1072
Règles d'Associate Resolver ... 1072
Associer des points de terminaison VPC ... 1073
Modifier les configurations de profil ... 1074
Associé VPCs ... 1076
Affichage et mise à jour des profils ... 1077
Suppression d'un profil ... 1079
Afficher et mettre à jour les ressources associées aux profils ... 1080
Dissociation d'une ressource ... 1082
Affichage VPCs associé à un profil ... 1083
Dissociation d'un VPC ... 1085
Utilisation de profils Route 53 partagés ... 1086
Octroi d'autorisations pour le partage de profils Route 53 ... 1087
Conditions préalables au partage de profils Route 53 ... 1087
Partage d'un profil Route 53 ... 1088
Annulation du partage d'un profil Route 53 partagé ... 1089
Identifier un profil Route 53 partagé ... 1090
Responsabilités et autorisations pour les profils Route 53 partagés ... 1090
Facturation et mesures ... 1091
Quotas d'instances ... 1091
Qu'est-ce que Amazon Route 53 sur Outposts ? ... 1092
Fonctionnalités de Route 53 sur Outposts ... 1092

Comportement du résolveur Route 53 lorsqu'il AWS Outposts est déconnecté du VPC 1093
Mise en route avec le résolveur de Route 53 sur AWS Outposts 1094
Création de points de terminaison entrants 1095
Valeurs à spécifier lors de la création ou de la modification de points de terminaison entrants sur un Outpost 1095
Création de points de terminaison sortants 1097
Valeurs à spécifier lors de la création ou de la modification de points de terminaison sortants dans un AWS Outposts 1098
Création de règles de réacheminement pour les points de terminaison sortants 1100
Gestion du résolveur sur Outpost 1100
Modification du résolveur sur Outpost 1101
Affichage de l'état du résolveur sur Outpost 1101
Suppression du résolveur sur Outpost 1102
Gestion des points de terminaison entrants sur le résolveur sur Outpost 1103
Affichage et modification des points de terminaison entrants 1103
Affichage du statut des points de terminaison entrants 1104
Suppression des points de terminaison entrants 1105
Gestion des points de terminaison sortants sur le résolveur sur Outpost 1106
Affichage et modification des points de terminaison sortants 1106
Affichage du statut des points de terminaison sortants 1107
Suppression des points de terminaison sortants 1108
Création de AWS CloudFormation ressources 1110
Route 53, Route 53 Resolver et modèles AWS CloudFormation 1110
En savoir plus sur AWS CloudFormation 1111
Exemples de code 1112
Route 53 1113
Principes de base 1113
Enregistrement de domaine Route 53 1142
Principes de base 1149
Sécurité 1233
Protection des données 1234
Protection contre les registres de délégation suspendu 1235
Gestion des identités et des accès 1237
Authentification par des identités 1237
Contrôle d’accès 1241
Présentation de la gestion des accès 1242

Utilisation de stratégies IAM pour Route 53 ... 1249
Utilisation des rôles liés à un service ... 1262
AWS politiques gérées ... 1267
Utilisation de conditions ... 1282
Référence des autorisations d'API Route 53 ... 1292
Journalisation et surveillance ... 1293
Validation de conformité ... 1294
Résilience ... 1295
Sécurité de l'infrastructure ... 1296
Envoi des résultats à Security Hub ... 1298
Comment fonctionnent les résultats dans Security Hub ... 1298
Types de résultats envoyés par le pare-feu DNS ... 1299
Réessayer lorsque Security Hub n'est pas disponible ... 1299
Mise à jour des résultats existants dans Security Hub ... 1299
Découverte typique du pare-feu DNS ... 1300
Activation et configuration de l'intégration ... 1302
Arrêt de la transmission des résultats à Security Hub ... 1302
Surveillance ... 1303
Journalisation des requêtes DNS publiques ... 1303
Configuration de la journalisation des requêtes DNS ... 1305
Utilisation d'Amazon CloudWatch pour accéder aux journaux de requêtes DNS ... 1306
Modification de la période de conservation des journaux et exportation de journaux vers Amazon S3 ... 1307
Arrêt de la journalisation des requêtes ... 1307
Valeurs qui apparaissent dans les journaux de requête DNS ... 1308
Exemple de journal de requête ... 1309
Journalisation des requêtes Resolver ... 1310
Ressources vers lesquelles vous pouvez envoyer des journaux de requêtes Resolver ... 1311
Gestion des configurations ... 1314
Surveillance des registres de domaines ... 1322
Surveillance de vos ressources grâce aux bilans de santé d'Amazon Route 53 et à Amazon CloudWatch ... 1322
Métriques et dimensions pour les surveillances d'état ... 1322
Surveillance des zones hébergées à l'aide d'Amazon CloudWatch ... 1325
CloudWatch métriques pour les zones hébergées publiques de la Route 53 ... 1326
CloudWatch dimension pour les métriques de la zone hébergée publique Route 53 ... 1327

Surveillance des points de terminaison Route 53 Resolver avec Amazon CloudWatch 1327
Métriques et dimensions pour Resolver 1328
Surveillance des groupes de règles du pare-feu DNS Route 53 Resolver avec Amazon CloudWatch 1333
Métriques et dimensions pour le pare-feu DNS 1333
Gestion des événements du pare-feu DNS à l'aide de EventBridge 1336
Événements du pare-feu DNS Route 53 Resolver 1337
Envoi d'événements liés au pare-feu DNS 1338
Autorisations 1341
Ressources supplémentaires 1341
Référence détaillée du pare-feu DNS pour les événements 1341
Journalisation des appels d'API Amazon Route 53 avec AWS CloudTrail 1349
Informations sur la Route 53 dans CloudTrail 1350
Affichage des événements Route 53 avec l'historique des événements 1351
Compréhension des entrées des fichiers journaux Route 53 1351
Résolution des problèmes 1359
Mon domaine n'est pas disponible sur Internet 1360
Vous avez enregistré un nouveau domaine, mais vous n'avez pas cliqué sur le lien figurant dans l'e-mail de confirmation 1361
Vous avez transféré l'enregistrement de domaine à Amazon Route 53, mais vous n'avez pas transféré le service DNS 1361
Vous avez transféré l'enregistrement de domaine et spécifié des serveurs de noms incorrects dans les paramètres du domaine 1363
Vous avez transféré le service DNS en premier, mais vous n'avez pas attendu assez longtemps avant de transférer l'enregistrement de domaine 1364
Vous avez supprimé la zone hébergée que Route 53 utilise pour acheminer le trafic Internet pour le domaine. 1365
Votre domaine a été suspendu 1366
Mon domaine est suspendu (le statut est ClientHold) 1366
Vous avez enregistré un nouveau domaine, mais vous n'avez pas cliqué sur le lien figurant dans l'e-mail de confirmation 1367
Vous avez désactivé le renouvellement automatique du domaine et celui-ci a expiré 1368
Vous avez modifié l'adresse e-mail du contact inscrit, mais vous n'avez pas vérifié que la nouvelle adresse e-mail est valide 1368
Nous ne sommes pas parvenus à traiter votre paiement pour le renouvellement automatique du domaine qui a expiré 1369

Nous avons suspendu le domaine en raison d'une violation de la politique d'utilisation acceptable d' AWS ... 1369
Nous avons suspendu le domaine en raison d'une décision judiciaire ... 1369
Le transfert de mon domaine à Amazon Route 53 a échoué ... 1370
Vous n'avez pas cliqué sur le lien figurant dans l'e-mail d'autorisation ... 1370
Le code d'autorisation que vous avez obtenu à partir du bureau d'enregistrement n'est pas valide ... 1370
Erreur « Parameters in request are not valid » (Les paramètres de la demande ne sont pas valides) lors de la tentative de transfert d'un domaine .es vers Amazon Route 53 ... 1371
Le nom de domaine internationalisé que vous transférez vers Amazon Route 53 est-il répertorié dans punycode ? ... 1371
J'ai modifié les paramètres DNS, mais ils ne sont pas entrés en vigueur ... 1371
Vous avez transféré le service DNS à Amazon Route 53 au cours des dernières 48 heures, par conséquent, DNS utilise encore votre service DNS précédent ... 1372
Vous avez récemment transféré le service DNS à Amazon Route 53, mais vous n'avez pas mis à jour les serveurs de noms avec le serveur d'inscriptions (registrar) de domaine ... 1372
Les résolveurs DNS utilisent toujours les anciens paramètres pour l'enregistrement ... 1374
Vous avez plusieurs zones hébergées portant le même nom et vous avez mis à jour celle qui n'est pas associée au domaine ... 1375
Mon navigateur affiche le message d'erreur « Server not found » ... 1377
Vous n'avez pas créé d'enregistrement pour le nom de domaine ou de sous-domaine ... 1377
Vous avez créé un enregistrement mais vous avez spécifié une valeur incorrecte ... 1377
La ressource vers laquelle vous acheminez le trafic n'est pas disponible ... 1377
Je ne peux pas acheminer le trafic vers un compartiment Amazon S3 qui est configuré pour l'hébergement de site web ... 1378
J'ai été facturé deux fois pour la même zone hébergée ... 1378
Plusieurs factures m'ont été facturées pour mon domaine ... 1379
Mon AWS compte est fermé ou définitivement, et mon domaine est enregistré auprès de Route 53 ... 1379
Plages d'adresses IP ... 1381
Plages d'adresses IP de serveurs de noms Route 53 ... 1381
Plages d'adresses IP utilisées par les surveillances de l'état de Route 53 ... 1381
Référencement de listes de préfixes ... 1382
Plages d'adresses IP internes utilisées par les surveillances de l'état de Route 53 ... 1382
Balisage de ressources ... 1383
Didacticiels ... 1385

Utilisation d'Amazon Route 53 comme service DNS pour des sous-domaines sans migration du domaine parent ... 1386
Création d'un sous-domaine qui utilise Amazon Route 53 en tant que service DNS sans migration du domaine parent ... 1387
Migration d'un service DNS pour un sous-domaine vers Amazon Route 53 sans migration du domaine parent ... 1390
Transition vers le routage basé sur la latence dans Amazon Route 53 ... 1395
Ajout d'une autre région à votre routage basé sur la latence dans Amazon Route 53 ... 1398
Utilisation de la latence et des enregistrements pondérés dans Amazon Route 53 pour acheminer le trafic vers plusieurs EC2 instances Amazon dans une région ... 1400
Gestion de plus de 100 enregistrements pondérés dans Amazon Route 53 ... 1401
Pondération des réponses pour la tolérance aux pannes pour plusieurs enregistrements dans Amazon Route 53 ... 1402
Bonnes pratiques ... 1405
Bonnes pratiques relatives à Amazon Route 53 DNS ... 1406
Bonnes pratiques relatives à Resolver ... 1409
Évitez les configurations de boucle avec les points de terminaison Resolver. ... 1410
Mise à l'échelle du point de terminaison Resolver ... 1410
Haute disponibilité pour les points de terminaison Resolver ... 1412
Parcours de zone DNS ... 1412
Bonnes pratiques relatives aux vérifications de l'état d'Amazon Route 53 ... 1413
Quotas ... 1415
Utilisation de Service Quotas pour afficher et gérer les quotas ... 1415
Quotas applicables aux entités ... 1415
Quotas applicables aux domaines ... 1416
Quotas applicables aux zones hébergées ... 1416
Quotas applicables aux enregistrements ... 1418
Quotas sur Route 53 Resolver ... 1418
Quotas applicables aux surveillances de l'état ... 1426
Quotas applicables aux configurations de journalisation des requêtes ... 1426
Quotas applicables aux stratégies de flux de trafic et d'enregistrements de stratégies ... 1427
Quotas applicables aux ensembles de délégations réutilisables ... 1427
Quotas sur les profils de la Route 53 ... 1427
Quotas maximums pour les demandes d'API ... 1428
Nombre d'éléments et de caractères dans les demandes `ChangeResourceRecordSets` 1429
Fréquence des demandes d'API Amazon Route 53 ... 1429

Fréquence des demandes d'API Route 53 Resolver 1430
Informations connexes 1431
AWS ressources 1431
Bibliothèques et outils tiers 1432
Interfaces utilisateur graphiques 1433
Historique du document 1434
Sorties en 2025 1434
2024 sorties 1436
Versions de 2023 1438
Publications de 2022 1439
Versions de 2021 1440
Versions de 2020 1441
Versions 2018 1441
Versions 2017 1443
Versions 2016 1445
Versions 2015 1449
Versions 2014 1452
Versions 2013 1456
Version 2012 1457
Versions 2011 1457
Version 2010 1458
..... mcdlix

Qu'est-ce qu'Amazon Route 53 ?

Amazon Route 53 est un service web de système de noms de domaine (DNS) hautement disponible et évolutif. Vous pouvez utiliser Route 53 pour effectuer trois fonctions importantes dans n'importe quelle combinaison : l'enregistrement de domaine, le routage DNS et la surveillance de l'état.

Si vous choisissez d'utiliser Route 53 pour les trois fonctions, assurez-vous de suivre l'ordre ci-dessous :

1. Enregistrer des noms de domaine

   Votre site web a besoin d'un nom, comme exemple.com. Route 53 vous permet d'enregistrer un nom pour votre site web ou votre application web, appelé nom de domaine.

   - Pour avoir une présentation, consultez Fonctionnement de l'enregistrement de domaine.
   - Pour accéder à une procédure, consultez Enregistrement d'un nouveau domaine.
   - Pour visionner un didacticiel qui vous guide dans l'enregistrement d'un domaine et la création d'un site Web basique dans un compartiment Amazon S3, consultez Mise en route avec Amazon Route 53.

2. Acheminer le trafic Internet vers les ressources pour votre domaine

   Lorsqu'un utilisateur ouvre un navigateur Web et saisit votre nom de domaine (exemple.com) ou votre nom de sous-domaine (acme.exemple.com) dans la barre d'adresse, Route 53 permet de connecter le navigateur avec votre site Web ou avec votre application Web.

   - Pour avoir une présentation, consultez Acheminement du trafic Internet vers votre site web ou votre application web.
   - Pour connaître les procédures, consultez Configuration d'Amazon Route 53 en tant que service DNS.
   - Pour connaître la procédure à suivre pour acheminer des e-mails vers Amazon WorkMail, consultezAcheminement du trafic vers Amazon WorkMail.

3. Vérifier l'état de santé de vos ressources

   Route 53 envoie les demandes automatiques, via Internet, à une ressource, comme un serveur Web, afin de vérifier qu'elle est accessible, disponible et fonctionnelle. Vous pouvez également choisir de recevoir des notifications lorsque la ressource n'est pas disponible et choisir d'acheminer le trafic Internet à l'écart des ressources non saines.

- Pour avoir une présentation, consultez Comment Amazon Route 53 vérifie l'état de vos ressources.
- Pour connaître les procédures, consultez Création de bilans de santé pour Amazon Route 53 .

Autres fonctionnalités de la Route 53

En plus d'être un service Web de système de noms de domaine (DNS), Route 53 offre les fonctionnalités suivantes :

Route 53 Resolver

Bénéficiez d'un DNS récursif pour votre Amazon VPCs in Régions AWS, VPCs in AWS Outposts racks ou tout autre réseau sur site. Créez des règles de transfert conditionnelles et des points de terminaison Route 53 pour résoudre les noms personnalisés maîtrisés dans les zones hébergées privées Route 53 ou sur vos serveurs DNS locaux.

Pour plus d'informations, consultezQu'est-ce que c'est Amazon Route 53 Resolver ?.

Amazon Route 53 Resolver sur les Outposts

Connectez le résolveur Route 53 sur les racks Outpost aux serveurs DNS de vos centres de données locaux via les points de terminaison Route 53 Resolver. Cela permet de résoudre les requêtes DNS entre les racks Outposts et vos autres ressources locales.

Pour plus d'informations, consultezQu'est-ce que Amazon Route 53 sur Outposts ?.

Route 53 Resolver DNS Firewall

Protégez vos requêtes DNS récursives dans le résolveur Route 53. Créez des listes de domaines et établissez des règles de pare-feu qui filtrent le trafic DNS sortant en fonction de ces règles.

Pour plus d'informations, consultezUtilisation du pare-feu DNS pour filtrer le trafic DNS sortant.

Flux de trafic

Easy-to-use et gestion rentable du trafic mondial : orientez les utilisateurs finaux vers le meilleur point de terminaison pour votre application en fonction de la géoproximité, de la latence, de l'état de santé et d'autres considérations.

Pour plus d'informations, consultezUtiliser Traffic Flow pour acheminer le trafic DNS.

Profils Amazon Route 53

Avec les profils Route 53, vous pouvez appliquer et gérer des configurations Route 53 liées au DNS dans de nombreuses VPCs configurations différentes. Compte AWS

Pour plus d'informations, consultezQue sont les profils Amazon Route 53 ?.

Rubriques

- Fonctionnement de l'enregistrement de domaine
- Acheminement du trafic Internet vers votre site web ou votre application web
- Comment Amazon Route 53 vérifie l'état de vos ressources
- Concepts Amazon Route 53
- Comment démarrer avec Amazon Route 53
- Accès à Amazon Route 53
- AWS Identity and Access Management
- Tarification et facturation Amazon Route 53
- Utilisation de Route 53 avec un AWS SDK

Fonctionnement de l'enregistrement de domaine

Si vous souhaitez créer un site web ou une application web, vous commencez par enregistrer le nom de votre site web, appelé domain name. Votre nom de domaine est le nom, comme example.com, que vos utilisateurs saisissent dans un navigateur pour afficher votre site web.

Voici une présentation de la procédure d'enregistrement d'un nom de domaine avec Amazon Route 53 :

1. Vous choisissez un nom de domaine et confirmez qu'il est disponible, ce qui signifie que personne d'autre n'a enregistré le nom de domaine que vous voulez.

   Si le nom de domaine souhaité est déjà en cours d'utilisation, vous pouvez essayer d'autres noms ou tenter de remplacer uniquement le domaine de premier niveau, tel que .com, par un autre domaine de premier niveau, comme .ninja ou .hockey. Pour obtenir une liste des domaines de premier niveau pris en charge par Route 53, consultez Domaines que vous pouvez enregistrer avec Amazon Route 53.

2. Vous enregistrez le nom de domaine avec Route 53. Lorsque vous enregistrez un domaine, vous fournissez les noms et les informations sur le contact pour le propriétaire du domaine et d'autres contacts.

   Lorsque vous enregistrez un domaine avec Route 53, le service devient automatiquement le service DNS du domaine en procédant comme suit :

   - Il crée une hosted zone qui a le même nom que votre nom de domaine.
   - Il affecte un ensemble de quatre serveurs de noms à la zone hébergée. Lorsqu'un navigateur est utilisé pour accéder à votre site web, par exemple www.example.com, ces serveurs de noms indiquent au navigateur où trouver les ressources, par exemple un serveur web ou un compartiment Amazon S3. (Amazon S3 est un stockage d'objets pour stocker et extraire n'importe quel volume de données à partir de n'importe quel emplacement sur le web. Un compartiment est un conteneur d'objets stockés dans S3.)
   - Il récupère les serveurs de noms de la zone hébergée et les ajoute au domaine.

   Pour de plus amples informations, veuillez consulter Acheminement du trafic Internet vers votre site web ou votre application web.

3. A la fin du processus d'enregistrement, nous envoyons vos informations au bureau d'enregistrement du domaine. Le domain registrar est Amazon Registrar, Inc. ou notre partenaire, Gandi. Pour déterminer le bureau d'enregistrement pour votre domaine, consultez Identification de votre bureau d'enregistrement.
4. Le bureau d'enregistrement envoie vos informations dans le registre pour le domaine. Un registre est une entreprise qui vend des enregistrements de domaine pour un ou plusieurs domaines de premier niveau, comme .com.
5. Le registre stocke les informations concernant votre domaine dans leur propre base de données et stocke également certaines de ces informations dans la base de données publique WHOIS.

Pour plus d'informations sur la façon d'enregistrer un nom de domaine, consultez Enregistrement d'un nouveau domaine.

Si vous avez déjà enregistré un nom de domaine avec un autre bureau d'enregistrement, vous pouvez choisir de transférer l'enregistrement de domaine vers Route 53. L'utilisation d'autres fonctionnalités de Route 53 n'est pas nécessaire. Pour de plus amples informations, veuillez consulter Transfert d'un enregistrement de domaine vers Amazon Route 53.

Acheminement du trafic Internet vers votre site web ou votre application web

Tous les ordinateurs connectés à Internet, depuis votre téléphone intelligent ou votre ordinateur portable, se connectent aux serveurs qui diffusent le contenu des sites Web de vente au détail massifs, communiquent entre eux à l'aide de numéros. Ces numéros, connus sous le nom adresses IP, sont dans l'un des formats suivants :

- Format du protocole Internet version 4 (IPv4), tel que 192.0.2.44
- Format du protocole Internet version 6 (IPv6), tel que 2001:0 db 8:85 a 3:0000:0000:abcd : 0001:2345

Lorsque vous ouvrez un navigateur et accédez à un site web, vous n'avez pas à mémoriser et à saisir une telle chaîne de caractères. Au lieu de cela, vous pouvez saisir un nom de domaine comme exemple.com et vous retrouver au bon endroit. Un service DNS comme Amazon Route 53 permet d'établir la connexion entre les noms de domaine et les adresses IP.

Rubriques

- Comment configurer Amazon Route 53 pour acheminer le trafic Internet pour votre domaine
- Comment Amazon Route 53 achemine le trafic de votre domaine

Comment configurer Amazon Route 53 pour acheminer le trafic Internet pour votre domaine

Voici une présentation démontrant comment utiliser la console Amazon Route 53 pour enregistrer un nom de domaine et configurer Route 53 pour acheminer le trafic Internet à votre site web ou une application web.

1. Vous enregistrez le nom de domaine que vos utilisateurs doivent utiliser pour accéder à votre contenu. Pour avoir une présentation, consultez Fonctionnement de l'enregistrement de domaine.
2. Après avoir enregistré votre nom de domaine, Route 53 crée automatiquement une zone hébergée publique portant le même nom que le domaine. Pour de plus amples informations, veuillez consulter Utilisation de zones hébergées publiques.
3. Pour acheminer le trafic vers vos ressources, vous créez des enregistrements, également appelés jeux d'enregistrements de ressources, dans votre zone hébergée. Chaque enregistrement

comporte des informations sur la façon dont vous souhaitez acheminer le trafic pour votre domaine, comme suit :

Nom

Le nom de l'enregistrement correspond au nom de domaine (example.com) ou au nom de sous-domaine (www.example.com, retail.example.com) pour lequel vous voulez que Route 53 achemine le trafic.

Le nom de chaque enregistrement dans une zone hébergée doit se terminer par le nom de la zone hébergée. Par exemple, si le nom de la zone hébergée est example.com, tous les noms d'enregistrements doivent se terminer par example.com. La console Route 53 le fait pour vous automatiquement.

Type

Le type d'enregistrement détermine généralement le type de ressource vers lequel vous souhaitez que le trafic soit acheminé. Par exemple, pour acheminer le trafic vers un serveur d'e-mail, vous spécifiez MX pour le Type. Pour acheminer le trafic vers un serveur Web doté d'une adresse IPv4 IP, vous devez spécifier A pour Type.

Valeur

La valeur est étroitement liée au type. Si vous indiquez un type MX, vous spécifiez les noms d'un ou plusieurs serveurs de messagerie comme valeur. Si vous spécifiez A pour Type, vous spécifiez une adresse IP au IPv4 format, tel que 192.0.2.136.

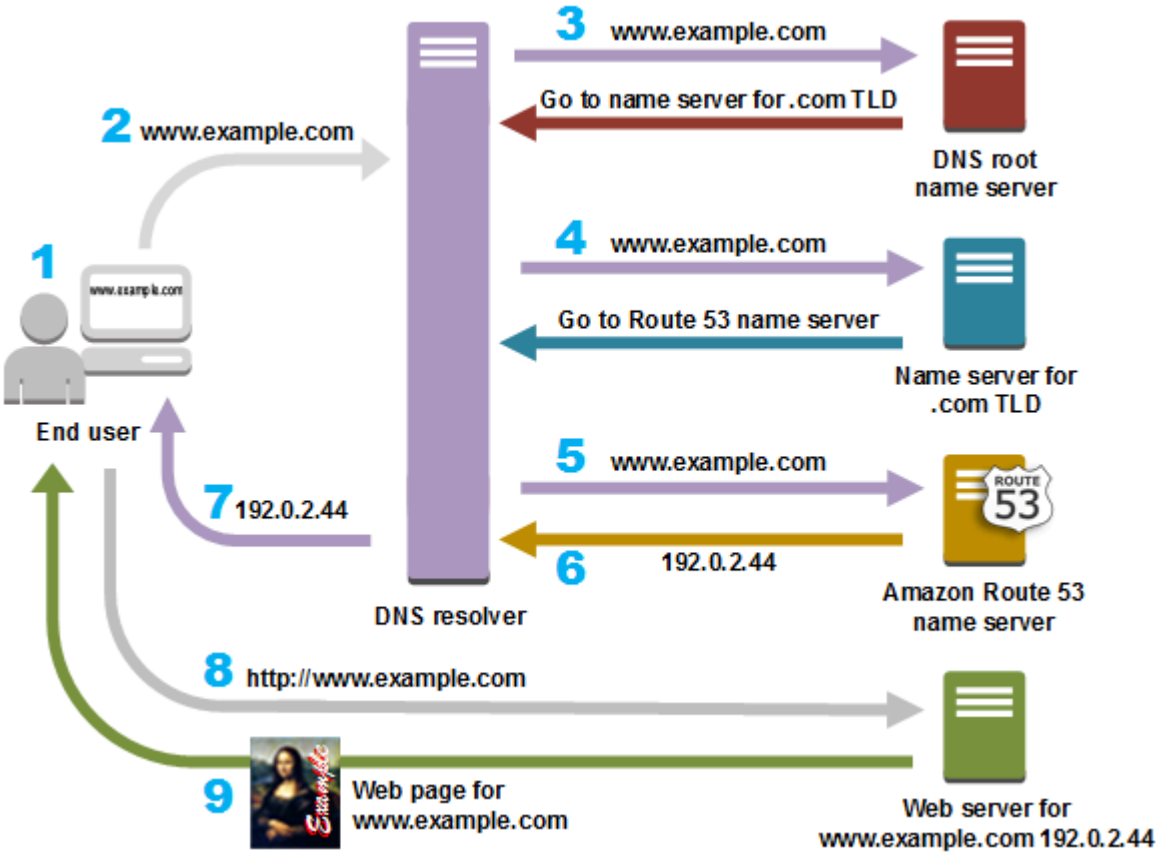
Pour plus d'informations sur les enregistrements , consultez la section Utilisation des enregistrements.

Vous pouvez également créer des enregistrements Route 53 spéciaux, appelés enregistrements d'alias, qui acheminent le trafic vers les compartiments Amazon S3, les CloudFront distributions Amazon et d'autres AWS ressources. Pour plus d'informations, consultez Choix entre des enregistrements avec ou sans alias et Acheminement du trafic Internet vers vos AWS ressources.

Pour plus d'informations sur le routage de votre trafic Internet vers vos ressources, consultez Configuration d'Amazon Route 53 en tant que service DNS.

Comment Amazon Route 53 achemine le trafic de votre domaine

Une fois que vous avez configuré Amazon Route 53 pour acheminer le trafic Internet vers vos ressources, telles que des serveurs web ou des compartiments Amazon S3, voici ce qui se passe en quelques millisecondes lorsqu'un utilisateur demande du contenu pour www.example.com :



1. Un utilisateur ouvre un navigateur web, saisit www.example.com dans la barre d'adresse et appuie sur Entrée.
2. La demande pour www.example.com est acheminée vers un résolveur DNS, qui est généralement géré par le fournisseur de services Internet de l'utilisateur, par exemple, un fournisseur de services Internet par câble, un fournisseur d'accès DSL à large bande ou un réseau d'entreprise.
3. Le résolveur DNS du FAI transmet la demande pour www.example.com à un serveur de noms racine DNS.
4. Le résolveur DNS transmet à nouveau la demande pour www.example.com, mais cette fois-ci, aux serveurs de noms TLD pour les domaines .com. Le serveur de noms de domaines .com répond à la demande avec les noms des quatre serveurs de noms Route 53 qui sont associés au domaine example.com.

Le résolveur DNS met en cache (stocke) les quatre serveurs de noms Route 53. La prochaine fois que quelqu'un accèdera à example.com, le résolveur ignore les étapes 3 et 4, car il a déjà les serveurs de noms pour example.com. Les serveurs de noms restent généralement en cache pendant deux jours.

5. Le résolveur DNS choisit un serveur de noms Route 53 et transmet la demande pour www.example.com à ce serveur de noms.
6. Le serveur de noms Route 53 recherche l'enregistrement www.example.com dans la zone hébergée example.com. Il obtient la valeur associée, par exemple l'adresse IP d'un serveur web, 192.0.2.44, puis il renvoie l'adresse IP au résolveur DNS.
7. Le résolveur DNS a finalement l'adresse IP dont l'utilisateur a besoin. Le résolveur renvoie cette valeur au navigateur web.

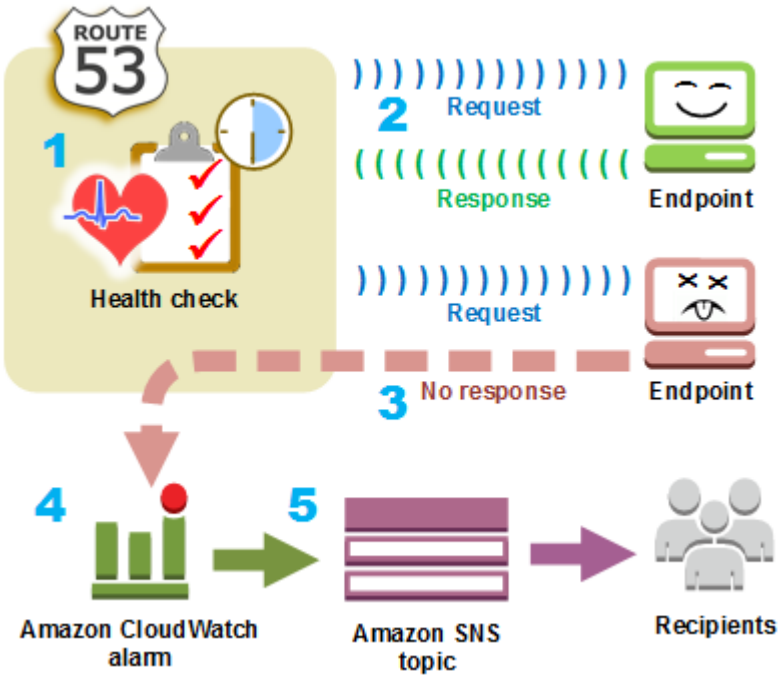
> **Note**
>
> Le résolveur DNS met également en cache l'adresse IP de example.com pendant un laps de temps défini, afin qu'il puisse répondre plus rapidement lors du prochain accès à example.com. Pour de plus amples informations, veuillez consulter time to live (TTL).

8. Le navigateur web envoie une demande pour www.example.com à l'adresse IP figurant dans le résolveur DNS. C'est là que se trouve votre contenu, par exemple, un serveur Web exécuté sur une EC2 instance Amazon ou un compartiment Amazon S3 configuré comme point de terminaison de site Web.
9. Le serveur web ou une autre ressource à l'adresse 192.0.2.44 retourne la page web de www.example.com vers le navigateur web, et celui-ci affiche la page.

Comment Amazon Route 53 vérifie l'état de vos ressources

Les surveillances d'état Amazon Route 53 contrôlent l'état de vos ressources, telles que les serveurs web et les serveurs de messagerie. Vous pouvez éventuellement configurer les CloudWatch alarmes Amazon pour vos bilans de santé, afin de recevoir une notification lorsqu'une ressource devient indisponible.

Voici une présentation du fonctionnement de la vérification du statut si vous voulez être averti lorsqu'une ressource devient indisponible :



1. Vous créez une surveillance de l'état et spécifiez des valeurs qui définissent la façon dont vous voulez que la surveillance de l'état se déroule, comme indiqué ci-après :
   - L'adresse IP ou le nom de domaine du point de terminaison, tel qu'un serveur web, que Route 53 doit contrôler. (Vous pouvez également surveiller l'état d'autres bilans de santé ou l'état d'une CloudWatch alarme.)
   - Le protocole qu'Amazon Route 53 doit utiliser pour effectuer la vérification : HTTP, HTTPS ou TCP.
   - À quelle fréquence, voulez-vous que Route 53 envoie une demande au point de terminaison. Il s'agit de l'intervalle entre les demandes.
   - Quel est le nombre d'échecs consécutifs du point de terminaison au-delà duquel Route 53 considère que ce point de terminaison est non sain. C'est le seuil d'échec.
   - Le cas échéant, comment souhaitez-vous être informé quand Route 53 détecte un point de terminaison non sain. Lorsque vous configurez la notification, Route 53 définit automatiquement une CloudWatch alarme. CloudWatch utilise Amazon SNS pour informer les utilisateurs qu'un point de terminaison est défectueux.
2. Route 53 commence à envoyer des demandes au point de terminaison selon l'intervalle spécifié dans la surveillance de l'état.

   Si le point de terminaison répond aux demandes, Route 53 considère que ce point de terminaison est sain et n'entreprend aucune action.

3. Si le point de terminaison ne répond pas à une demande, Route 53 commence à compter le nombre de demandes consécutives auxquelles le point de terminaison ne répond pas :
   - Si le nombre atteint la valeur spécifiée dans le seuil d'échec, Route 53 considère le point de terminaison comme étant non sain.
   - Si le point de terminaison recommence à répondre avant que le décompte n'atteigne le seuil d'échec, Route 53 remet le compte à 0 et CloudWatch ne vous contacte pas.
4. Si Route 53 considère que le point de terminaison est défectueux et si vous avez configuré une notification pour le contrôle de santé, Route 53 le signale CloudWatch.

   Si vous n'avez pas configuré de notification, vous pouvez toujours voir le statut de vos surveillances de l'état de Route 53 dans la console Route 53. Pour de plus amples informations, veuillez consulter Surveillance du statut de la vérification de l'état et obtention de notifications.
5. Si vous avez configuré la notification pour le bilan de santé, CloudWatch déclenchez une alarme et utilisez Amazon SNS pour envoyer une notification aux destinataires spécifiés.

Outre la surveillance de l'état d'un point de terminaison spécifié, vous pouvez configurer une surveillance de l'état sur plusieurs points de terminaison, afin d'être informé lorsqu'un nombre spécifique de ressources, comme deux serveurs web sur cinq, est indisponible. Vous pouvez également configurer un bilan de santé pour vérifier l'état d'une CloudWatch alarme afin d'être averti sur la base d'un large éventail de critères, et pas seulement de savoir si une ressource répond aux demandes.

Si vous disposez de plusieurs ressources exécutant la même fonction, par exemple des serveurs web ou des serveurs de base de données, et que vous voulez que Route 53 achemine le trafic uniquement vers les ressources saines, vous pouvez configurer un basculement DNS en associant une surveillance de l'état avec chaque enregistrement pour cette ressource. Si une surveillance de l'état détermine que la ressource sous-jacente n'est pas saine, Route 53 n'achemine pas le trafic vers l'enregistrement associé.

Pour plus d'informations sur l'utilisation de Route 53 pour contrôler l'état de vos ressources, consultez Création de bilans de santé pour Amazon Route 53 .

Concepts Amazon Route 53

Voici une présentation des concepts qui sont présentés dans le Guide de l'utilisateur du développeur Amazon Route 53.

Rubriques

- Concepts d'enregistrement de domaine
- Concepts du système de noms de domaine (DNS)
- Concepts de plan de données et contrôle
- Concepts des surveillances de l'état

Concepts d'enregistrement de domaine

Voici une présentation des concepts qui sont liés à l'enregistrement de domaines.

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

nom de domaine

Le nom, tel que example.com, que l'utilisateur tape dans la barre d'adresse d'un navigateur web pour accéder à un site web ou une application web. Pour que votre site web ou votre application web soit disponible sur Internet, vous devez d'abord enregistrer un nom de domaine. Pour de plus amples informations, veuillez consulter Fonctionnement de l'enregistrement de domaine.

registre de domaine

Entreprise accréditée par l'ICANN (Internet Corporation for Assigned Names and Numbers) pour traiter les enregistrements de domaines de premier niveau spécifiques (TLDs). Pour déterminer le bureau d'enregistrement de votre domaine, consultez Identification de votre bureau d'enregistrement.

registre de domaine

Une société qui possède le droit de vendre des domaines qui ont un domaine de premier niveau spécifique. Par exemple, VeriSignest-ce le registre qui détient le droit de vendre des domaines dotés d'un TLD .com. Un registre de domaine définit les règles d'enregistrement d'un domaine, telles que les conditions de résidence d'un TLD géographique. Un registre de domaine gère également la base de données faisant autorité pour tous les noms de domaine ayant le même

TLD. La base de données du registre contient des informations telles que les informations sur les contacts et les serveurs de noms de chaque domaine.

revendeur de domaine

Une société qui vend des noms de domaine pour des bureaux d'enregistrement comme Amazon Registrar. Amazon Route 53 est un revendeur de domaine pour Amazon Registrar et pour notre partenaire, Gandi.

domaine de premier niveau (TLD)

La dernière partie d'un nom de domaine, telle que .com, .org ou .ninja. Il existe deux types de domaines de niveau supérieur :

Domaines de premier niveau génériques

Ils donnent TLDs généralement aux utilisateurs une idée de ce qu'ils trouveront sur le site Web. Par exemple, les noms de domaine ayant un TLD de .bike sont souvent associés à des sites web d'entreprises ou d'organisations dans le secteur des motos et des bicyclettes. A quelques exceptions près, vous pouvez utiliser n'importe quel TLD générique, ainsi un club cycliste pourrait utiliser le TLD .hockey pour son nom de domaine.

Domaines géographiques de premier niveau

Ils TLDs sont associés à des zones géographiques telles que des pays ou des villes. Certains registres géographiques TLDs imposent des exigences de résidence, tandis que d'autres autorisent ou même encouragent l'utilisation en tant que TLD générique. the section called “.io (Territoire Britannique de l'Océan Indien)”

Pour obtenir la liste des noms de domaine TLDs que vous pouvez utiliser lorsque vous enregistrez un nom de domaine auprès de Route 53, consultezDomaines que vous pouvez enregistrer avec Amazon Route 53.

Concepts du système de noms de domaine (DNS)

Voici une présentation des concepts qui sont liés au système de noms de domaine (DNS).

- 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)

enregistrement d'alias

Type d'enregistrement que vous pouvez créer avec Amazon Route 53 pour acheminer le trafic vers AWS des ressources telles que les CloudFront distributions Amazon et les compartiments Amazon S3. Pour de plus amples informations, veuillez consulter Choix entre des enregistrements avec ou sans alias.

serveur de noms faisant autorité

Un serveur de noms qui contient des informations définitives sur une partie du système de noms de domaine (DNS) et qui répond aux demandes provenant d'un résolveur DNS en retournant les informations adéquates. Par exemple, un serveur de noms faisant autorité pour le domaine de premier niveau (TLD) .com connait les noms des serveurs de noms de chaque domaine .com enregistré. Lorsqu'un serveur de noms faisant autorité .com reçoit une demande pour example.com, de la part d'un résolveur DNS, il répond avec les noms des serveurs de noms du service DNS pour le domaine example.com.

Les serveurs de noms Route 53 sont des serveurs de noms faisant autorité pour chaque domaine qui utilise Route 53 comme service DNS. Les serveurs de noms savent comment vous souhaitez acheminer le trafic de votre domaine et des sous-domaines en fonction des enregistrements que vous avez créés dans la zone hébergée du domaine. (Les serveurs de noms Route 53 stockent les zones hébergées pour les domaines qui utilisent Route 53 comme service DNS.)

Par exemple, si un serveur de noms Route 53 reçoit une demande pour www.example.com, il trouve cet enregistrement et renvoie l'adresse IP, par exemple 192.0.2.33, qui est spécifiée dans l'enregistrement.

Bloc d'adresse CIDR

Un bloc d'adresse CIDR est une plage IP utilisée avec le routage basé sur IP. Dans Route 53, vous pouvez spécifier un bloc CIDR de /0 à /24 pour IPv4 et/0 à /48 pour. IPv6 Par exemple, un bloc IPv4 CIDR /24 inclut 256 adresses IP contiguës. Vous pouvez regrouper des jeux de blocs CIDR (ou des plages IP) en emplacements CIDR, qui sont à leur tour regroupés en collections CIDR réutilisables.

requête DNS

Il s'agit généralement d'une demande soumise par un appareil, tel qu'un ordinateur ou un smartphone, à un système de noms de domaine (DNS) pour une ressource qui est associée à un nom de domaine. L'exemple le plus courant d'une requête DNS est lorsqu'un utilisateur ouvre un navigateur et tape le nom de domaine dans la barre d'adresse. La réponse à une requête DNS est généralement l'adresse IP qui est associée à une ressource telle qu'un serveur web. L'appareil qui a lancé la demande utilise l'adresse IP pour communiquer avec la ressource. Par exemple, un navigateur peut utiliser l'adresse IP pour obtenir une page web à partir d'un serveur web.

résolveur DNS

Il s'agit d'un serveur DNS, souvent géré par un fournisseur de services Internet, qui agit comme un intermédiaire entre les requêtes des utilisateurs et les serveurs de noms DNS. Lorsque vous ouvrez un navigateur et entrez un nom de domaine dans la barre d'adresse, votre requête va d'abord vers un résolveur DNS. Le résolveur communique avec les serveurs de noms DNS pour obtenir l'adresse IP de la ressource correspondante, telle qu'un serveur web. Un résolveur DNS est également connu comme un serveur de noms récursif, car il envoie des demandes à une séquence de serveurs de noms DNS faisant autorité jusqu'à ce qu'il obtienne la réponse (généralement une adresse IP), qu'il renvoie à un appareil de l'utilisateur, par exemple, un navigateur web sur un ordinateur portable.

Système de nom de domaine (DNS)

Un réseau mondial de serveurs qui permet aux ordinateurs, smartphones, tablettes et autres appareils IP de communiquer entre eux. Le système de noms de domaine traduit des noms faciles à comprendre, comme example.com, par des chiffres, appelés adresses IP, qui permettent aux ordinateurs d'entrer en contact les uns avec les autres sur Internet.

Voir aussi IP address.

Zone hébergée

Un conteneur d'enregistrements qui comprennent des informations sur la façon dont vous voulez acheminer le trafic pour un domaine (comme, example.com) et tous ses sous-domaines (comme, www.example.com, retail.example.com et seattle.accounting.example.com). Une zone hébergée a le même nom que le domaine correspondant.

Par exemple, la zone hébergée pour example.com peut comprendre un enregistrement qui contient des informations sur le routage du trafic de www.example.com vers un serveur web qui a l'adresse IP 192.0.2.243, ainsi qu'un enregistrement qui contient des informations sur l'e-mail de routage de example.com vers deux serveurs de messagerie, mail1.example.com et mail2.example.com. Chaque serveur de messagerie nécessite également son propre enregistrement.

Voir aussi record (DNS record).

Adresse IP

Numéro attribué à un appareil sur Internet, tel qu'un ordinateur portable, un smartphone ou un serveur Web, qui permet à l'appareil de communiquer avec d'autres appareils sur Internet. Les adresses IP se présentent dans l'un des formats suivants :

- Format du protocole Internet version 4 (IPv4), tel que 192.0.2.44
- Format du protocole Internet version 6 (IPv6), tel que 2001:0 db 8:85 a 3:0000:0000:abcd : 0001:2345

Route 53 prend en charge les deux IPv4 et les IPv6 adresses aux fins suivantes :

- Vous pouvez créer des enregistrements de type A, pour les IPv4 adresses, ou de type AAAA, pour les IPv6 adresses.
- Vous pouvez créer des bilans de santé qui envoient des demandes à des adresses IPv4 ou à IPv6 des adresses.
- Si un résolveur DNS se trouve sur un IPv6 réseau, il peut utiliser l'un ou l'autre IPv4 ou IPv6 envoyer des demandes à Route 53.

serveurs de noms

Il s'agit de serveurs dans le système de noms de domaine (DNS) qui permettent de traduire les noms de domaine en adresses IP que les ordinateurs utilisent pour communiquer entre eux. Les serveurs de noms sont des serveurs de noms récursifs (également appelés DNS resolver) ou authoritative name server.

Pour une présentation sur la façon dont DNS achemine le trafic vers vos ressources, y compris le rôle de Route 53 dans le processus, consultez Comment Amazon Route 53 achemine le trafic de votre domaine.

Private DNS

Version locale du système de noms de domaine (DNS) qui vous permet d'acheminer le trafic d'un domaine et de ses sous-domaines vers des EC2 instances Amazon au sein d'un ou de plusieurs clouds privés virtuels Amazon (VPCs). Pour de plus amples informations, veuillez consulter Utilisation des zones hébergées privées.

enregistrement (enregistrement DNS)

Un objet dans une zone hébergée que vous utilisez pour définir la façon dont vous souhaitez acheminer le trafic d'un domaine ou d'un sous-domaine. Par exemple, vous pouvez créer des enregistrements pour example.com et www.example.com qui acheminent le trafic vers un serveur web qui possède une adresse IP de 192.0.2.234.

Pour plus d'informations sur les enregistrements, y compris les informations sur les fonctions qui sont fournies par des enregistrements spécifiques à Route 53, consultez Configuration d'Amazon Route 53 en tant que service DNS.

serveur de noms récursif

Consultez DNS resolver.

ensemble de délégations réutilisables

Un ensemble de quatre serveurs de noms faisant autorité que vous pouvez utiliser avec plusieurs zones hébergées. Par défaut, Route 53 attribue une sélection aléatoire de serveurs de noms pour chaque nouvelle zone hébergée. Pour faciliter la migration d'un service DNS vers Route 53 pour un grand nombre de domaines, vous pouvez créer un ensemble de délégations réutilisables et ensuite l'associer à de nouvelles zones hébergées. (Vous ne pouvez pas modifier les serveurs de noms qui sont associés à une zone hébergée existante.)

Vous créez un ensemble de délégations réutilisables et l'associez à une zone hébergée, par programmation ; l'utilisation de la console Route 53 n'est pas prise en charge. Pour plus d'informations, consultez CreateHostedZoneet consultez CreateReusableDelegationSetle manuel Amazon Route 53 API Reference. La même fonctionnalité est également disponible dans le AWS SDKs, le AWS Command Line Interface, et AWS Tools for Windows PowerShell.

stratégie de routage

Paramètre d'enregistrements qui détermine la façon dont Route 53 répond aux requêtes DNS. Route 53 prend en charge les stratégies de routage suivantes :

- Simple routing policy (Stratégie de routage simple) : utilisez cette stratégie pour acheminer du trafic Internet vers une seule ressource qui exécute une fonction donnée pour votre domaine, comme, par exemple, un serveur web qui diffuse le contenu du site web example.com.
- Failover routing policy (Stratégie de routage par basculement) : utilisez une stratégie de routage par basculement pour configurer le basculement actif-passif.
- Stratégie de routage de géolocalisation : utilisez cette stratégie lorsque vous souhaitez acheminer du trafic Internet en fonction de l'emplacement de vos utilisateurs.
- Stratégie de routage par proximité géographique : utilisez cette stratégie lorsque vous souhaitez acheminer du trafic en fonction de l'emplacement de vos ressources et, éventuellement, détourner le trafic de vos ressources à un emplacement donné vers les ressources d'un autre emplacement.
- Latency routing policy (Stratégie de routage avec latence) : utilisez la stratégie de routage avec latence lorsque vous disposez de ressources à plusieurs emplacements et que vous souhaitez acheminer le trafic vers la ressource qui fournit la latence optimale.
- IP-based routing policy (Politique de routage basée sur IP) – utilisez la politique de routage basée sur IP lorsque vous voulez acheminer le trafic en fonction de l'emplacement de vos utilisateurs, et que vous disposez des adresses IP d'où provient le trafic.
- Multivalue answer routing policy (Stratégie de routage de réponse multivaleur) : utilisez la stratégie de routage de réponse multivaleur lorsque vous souhaitez que Route 53 réponde aux requêtes DNS avec jusqu'à huit enregistrements sains sélectionnés de manière aléatoire.
- Weighted routing policy (Stratégie de routage pondéré) : utilisez la stratégie de routage pondéré pour acheminer le trafic vers plusieurs ressources selon les proportions que vous spécifiez.

Pour de plus amples informations, veuillez consulter Sélection d'une stratégie de routage.

sous-domaine

Un nom de domaine qui a une ou plusieurs étiquettes ajoutées au nom de domaine enregistré. Par exemple, si vous enregistrez le nom de domaine example.com, www.example.com est alors un sous-domaine. Si vous créez la zone hébergée accounting.example.com pour le domaine example.com, alors seattle.accounting.example.com est un sous-domaine.

Pour acheminer le trafic d'un sous-domaine, créez un enregistrement en lui attribuant le nom de votre choix, comme www.example.com et spécifiez les valeurs applicables, telles que l'adresse IP d'un serveur web.

Durée de vie (TTL)

La durée de temps, en secondes, au-delà de laquelle vous souhaitez qu'un résolveur DNS mette en cache (stocke) les valeurs d'un enregistrement avant de soumettre une autre demande à Route 53 pour obtenir les valeurs actuelles de cet enregistrement. Si le résolveur DNS reçoit une autre demande pour le même domaine avant l'expiration de la durée de vie, le résolveur renvoie la valeur mise en cache.

Une durée de vie plus longue réduit vos coûts de Route 53, qui sont en partie basés sur le nombre de requêtes DNS auxquelles Route 53 répond. Une durée de vie plus courte réduit le temps que les résolveurs DNS mettent pour acheminer le trafic vers des ressources plus anciennes une fois que vous avez modifié les valeurs dans un enregistrement, par exemple, en remplaçant l'adresse IP d'un serveur web par www.example.com.

Concepts de plan de données et contrôle

Voici une présentation des concepts liés à la manière dont Amazon Route 53 divise ses fonctionnalités en plan de données et contrôle. Le service Route 53, comme la plupart des Services AWS, inclut un plan de contrôle qui vous permet d'effectuer des opérations de gestion telles que la création, la mise à jour et la suppression de ressources et un plan de données fournissant les fonctionnalités principales du service. Bien que les deux fonctionnalités soient conçues pour être fiables, les plans de contrôle sont optimisés pour assurer la cohérence des données, tandis que les plans de données sont optimisés pour assurer la disponibilité. La conception résiliente du plan de données lui permet de maintenir la disponibilité, même lors d'événements perturbateurs rares, au cours desquels le plan de contrôle peut devenir indisponible. C'est pourquoi nous vous recommandons d'utiliser des fonctions de plan de données lorsque la disponibilité est importante.

Pour les DNS publics et privés de Route 53 et les contrôles de santé, le plan de contrôle est situé dans le Région AWS us-east-1 et les plans de données sont distribués dans le monde entier.

Amazon Route 53 est divisé en plans de données et contrôle comme suit :

- Pour les DNS publics et privés Route 53, le plan de contrôle comprend la Route 53 APIs, qui vous permet de gérer les entrées DNS, y compris la Route 53 et le Traffic FlowAPIs. La console Route 53 se trouve dans l' Région AWS us-east-1, mais AWS s'il est déterminé qu'il existe un

dysfonctionnement dans cette région, la console Route 53 sera desservie par l'us-west-2. Région AWS Le plan de données est le service DNS faisant autorité qui s'exécute sur plus de 200 emplacements de Points de Présence (PdP), répondant aux requêtes DNS en fonction de vos zones hébergées et vos données de surveillance de l'état.

- Pour les bilans de santé de la Route 53, le plan de contrôle comprend la Route 53 APIs que vous pouvez utiliser pour créer, mettre à jour et supprimer des bilans de santé. La console de vérification de l'état de la Route 53 se trouve dans l' Région AWS us-east-1, mais AWS s'il est déterminé qu'il existe un dysfonctionnement dans cette région, la console des bilans de santé de la Route 53 sera desservie par l'us-west-2. Région AWS Le plan de données est le service distribué à l'échelle mondiale qui effectue les surveillances de l'état, agrège les résultats et les transmet aux plans de données du DNS public et privé de Route 53 et à AWS Global Accelerator.
- En effet Amazon Route 53 Resolver, le plan de contrôle comprend le résolveur Route 53 APIs qui vous permet de gérer les paramètres Amazon VPC, les règles du résolveur, les politiques de journalisation des requêtes et les politiques de pare-feu DNS. Le plan de données est le service de resolveur DNS qui répond aux requêtes DNS de votre VPC, aux points de terminaison qui transmettent des requêtes à d'autres résolveurs et au plan de données de pare-feu du DNS qui applique des politiques de filtrage des requêtes DNS. Resolver est un service régional dont les plans de contrôle et de données fonctionnent indépendamment dans chacun Région AWS d'eux.
- Les enregistrements de domaine Route 53 sont gérés uniquement sur le plan de contrôle dans la Région AWS us-east-1.

Pour plus d'informations sur les plans de données, les plans de contrôle et sur la manière dont AWS les services sont conçus pour atteindre les objectifs de haute disponibilité, consultez le document Static stability using Availability Zones paper publié dans la bibliothèque Amazon Builders' Library.

Concepts des surveillances de l'état

Voici une présentation des concepts liés à la surveillance de l'état d'Amazon Route 53.

- DNS failover
- endpoint
- health check

basculement DNS

Une méthode pour acheminer le trafic à l'écart des ressources non saines et vers des ressources saines. Lorsque vous avez plusieurs ressources exécutant la même fonction : par exemple, plusieurs serveurs web ou plusieurs serveurs de messagerie, vous pouvez configurer les surveillances d'état de Route 53; pour vérifier l'état de vos ressources et configurer des enregistrements dans votre zone hébergée afin d'acheminer le trafic uniquement vers des ressources saines.

Pour de plus amples informations, veuillez consulter Configuration du basculement DNS.

point de terminaison

La ressource, par exemple un serveur web ou un serveur de messagerie, pour laquelle vous configurez une surveillance de l'état. Vous pouvez spécifier un point de terminaison par IPv4 adresse (192.0.2.243), par IPv6 adresse (2001:0 db 8:85 a 3:0000:0000:abcd : 0001:2345) ou par nom de domaine (exemple.com).

> **Note**
>
> Vous pouvez également créer des bilans de santé qui surveillent l'état d'autres bilans de santé ou qui surveillent l'état d'alarme CloudWatch d'une alarme.

surveillance de l'état

Un composant Route 53 qui vous permet d'effectuer les opérations suivantes :

- Vérifier si un point de terminaison spécifié, tel qu'un serveur web, est sain
- Etre averti, le cas échéant, quand un point de terminaison devient non sain
- Configurer également le basculement DNS, qui permet de rediriger le trafic Internet à partir d'une ressource non saine vers une ressource saine

Pour plus d'informations sur la création et l'utilisation des surveillances de l'état, consultez Création de bilans de santé pour Amazon Route 53 .

Comment démarrer avec Amazon Route 53

Pour de plus amples informations sur la mise en route avec Amazon Route 53, veuillez consulter les rubriques suivantes dans ce guide :

- Configurer Amazon Route 53, qui explique comment s'inscrire AWS, comment sécuriser l'accès à votre AWS compte et comment configurer un accès programmatique à Route 53
- Mise en route avec Amazon Route 53, qui décrit comment enregistrer un nom de domaine, comment créer un compartiment Amazon S3 et le configurer pour qu'il héberge un site web, et comment acheminer le trafic Internet vers le site web

Accès à Amazon Route 53

Vous pouvez accéder à Amazon Route 53 de la manière suivante :

- AWS Management Console— Les procédures décrites dans ce guide expliquent comment utiliser le AWS Management Console pour effectuer des tâches.
- AWS SDKs— Si vous utilisez un langage de programmation qui AWS fournit un SDK pour, vous pouvez utiliser un SDK pour accéder à Route 53. SDKs simplifiez l'authentification, intégrez facilement votre environnement de développement et offrez un accès facile aux commandes Route 53. Pour plus d'informations, consultez Outils pour Amazon Web Services.
- API Route 53 - Si vous utilisez un langage de programmation qui n'a pas de kit SDK disponible, veuillez consulter le document Référence d'API Amazon Route 53 pour de plus amples informations sur les actions d'API et sur la façon de créer des demandes d'API.
- AWS Command Line Interface – Pour plus d'informations, consultez Préparation de l'installation de l' AWS Command Line Interface dans le Guide de l'utilisateur AWS Command Line Interface .
- AWS Tools for Windows PowerShell – Pour plus d'informations, consultez Configuration de AWS Tools for Windows PowerShell dans le Guide de l'utilisateur Outils AWS pour PowerShell .

AWS Identity and Access Management

Amazon Route 53 s'intègre à AWS Identity and Access Management (IAM), un service qui permet à votre entreprise d'effectuer les opérations suivantes :

- Créez des utilisateurs et des groupes sous le AWS compte de votre organisation
- Partagez facilement les ressources de votre AWS compte entre les utilisateurs du compte
- Attribuer des informations d'identification de sécurité uniques à chaque utilisateur
- Contrôler de façon détaillée l'accès utilisateur aux services et ressources

Par exemple, vous pouvez utiliser IAM avec Route 53 pour contrôler quels utilisateurs de votre AWS compte peuvent créer une nouvelle zone hébergée ou modifier des enregistrements.

Pour obtenir des informations générales sur IAM, consultez les ressources suivantes :

- Identity and Access Management dans Amazon Route 53
- Identity and Access Management (IAM)
- Guide de l'utilisateur IAM

Tarification et facturation Amazon Route 53

Comme pour les autres AWS produits, il n'existe aucun contrat ou engagement minimum pour utiliser Amazon Route 53. Vous payez uniquement les zones hébergées que vous configurez et le nombre de requêtes DNS auxquelles Route 53 répond. Pour plus d'informations, consultez Tarification Amazon Route 53.

Pour plus d'informations sur la facturation AWS des services, notamment sur la façon de consulter votre facture et de gérer votre compte et vos paiements, consultez le guide de AWS Billing l'utilisateur.

Utilisation de Route 53 avec un AWS SDK

AWS des kits de développement logiciel (SDKs) sont disponibles pour de nombreux langages de programmation courants. Chaque SDK fournit une API, des exemples de code et de la documentation qui facilitent la création d'applications par les développeurs dans leur langage préféré.

Documentation SDK	Exemples de code
AWS SDK pour C++	AWS SDK pour C++ exemples de code
AWS CLI	AWS CLI exemples de code
AWS SDK pour Go	AWS SDK pour Go exemples de code
AWS SDK pour Java	AWS SDK pour Java exemples de code
AWS SDK pour JavaScript	AWS SDK pour JavaScript exemples de code

Documentation SDK	Exemples de code
AWS SDK pour Kotlin	AWS SDK pour Kotlin exemples de code
AWS SDK pour .NET	AWS SDK pour .NET exemples de code
AWS SDK pour PHP	AWS SDK pour PHP exemples de code
Outils AWS pour PowerShell	Outils AWS pour PowerShell exemples de code
AWS SDK pour Python (Boto3)	AWS SDK pour Python (Boto3) exemples de code
AWS SDK pour Ruby	AWS SDK pour Ruby exemples de code
Kit AWS SDK pour Rust	Kit AWS SDK pour Rust exemples de code
AWS SDK pour SAP ABAP	AWS SDK pour SAP ABAP exemples de code
Kit AWS SDK pour Swift	Kit AWS SDK pour Swift exemples de code

Pour plus d'exemples avec Route 53, consultez Exemples de code pour Route 53 utilisant AWS SDKs.

> **Exemple de disponibilité**
>
> Vous n’avez pas trouvé ce dont vous avez besoin ? Demandez un exemple de code en utilisant le lien Provide feedback (Fournir un commentaire) en bas de cette page.

Mise en route avec Amazon Route 53

Enregistrez un domaine avec Amazon Route 53 et configurez Route 53 pour répondre à des requêtes DNS qui sont résolues par le biais d'un site web statique. Le premier didacticiel héberge un site Web statique dans un compartiment Amazon S3 ouvert, et le second utilise la CloudFront distribution Amazon pour diffuser le site Web avec SSL/TLS.

Coût estimé

- Des frais annuels s'appliquent à l'enregistrement d'un domaine, s'élevant de 9 USD à plusieurs centaines de dollars, en fonction du domaine de premier niveau, .com par exemple. Pour plus d'informations, consultez Tarification Route 53 pour l'enregistrement de domaine. Ces frais ne sont pas remboursables.
- Lorsque vous enregistrez un domaine, nous créons automatiquement une zone hébergée portant le même nom que le domaine. Utilisez la zone hébergée pour spécifier l'emplacement vers lequel vous souhaitez que Route 53 achemine le trafic de votre domaine.
- Au cours de ce didacticiel, vous allez créer un compartiment Amazon S3 et télécharger un exemple de page web. Si vous êtes un nouveau AWS client, vous pouvez commencer à utiliser Amazon S3 gratuitement. Si vous êtes déjà AWS client, les frais sont basés sur la quantité de données que vous stockez, sur le nombre de demandes relatives à vos données et sur la quantité de données transférées. Pour plus d’informations, consultez Tarification Amazon S3.
- CloudFront les frais sont basés sur le nombre de demandes relatives à vos données, le nombre d'emplacements périphériques que vous utilisez et le volume de données transférées. Pour plus d’informations, consultez Tarification d’CloudFront .

Rubriques

- Configurer Amazon Route 53
- Utilisation de votre domaine pour un site web statique dans un compartiment Amazon S3
- Utiliser une CloudFront distribution Amazon pour diffuser un site Web statique

Configurer Amazon Route 53

La présentation et les procédures de cette section vous aideront à démarrer AWS.

Rubriques

- Inscrivez-vous pour un Compte AWS
- Création d’un utilisateur doté d’un accès administratif
- Télécharger les outils

Inscrivez-vous pour un Compte AWS

Si vous n'en avez pas Compte AWS, procédez comme suit pour en créer un.

Pour vous inscrire à un Compte AWS

1. Ouvrez l'https://portal.aws.amazon.com/billing/inscription.
2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d’inscription, vous recevrez un appel téléphonique ou un SMS et vous saisirez un code de vérification en utilisant le clavier numérique du téléphone.

   Lorsque vous vous inscrivez à un Compte AWS, un Utilisateur racine d'un compte AWSest créé. Par défaut, seul l’utilisateur racine a accès à l’ensemble des Services AWS et des ressources de ce compte. La meilleure pratique de sécurité consiste à attribuer un accès administratif à un utilisateur, et à utiliser uniquement l’utilisateur racine pour effectuer les tâches nécessitant un accès utilisateur racine.

AWS vous envoie un e-mail de confirmation une fois le processus d'inscription terminé. À tout moment, vous pouvez consulter l'activité actuelle de votre compte et gérer votre compte en accédant à https://aws.amazon.com/et en choisissant Mon compte.

Création d’un utilisateur doté d’un accès administratif

Une fois que vous vous êtes inscrit à un utilisateur administratif Compte AWS, que vous Utilisateur racine d'un compte AWS l'avez sécurisé AWS IAM Identity Center, que vous l'avez activé et que vous en avez créé un, afin de ne pas utiliser l'utilisateur root pour les tâches quotidiennes.

Sécurisez votre Utilisateur racine d'un compte AWS

1. Connectez-vous en AWS Management Consoletant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.

Pour obtenir de l'aide pour vous connecter en utilisant l'utilisateur racine, consultez Connexion en tant qu'utilisateur racine dans le Guide de l'utilisateur Connexion à AWS .

2. Activez l'authentification multifactorielle (MFA) pour votre utilisateur racine.

   Pour obtenir des instructions, voir Activer un périphérique MFA virtuel pour votre utilisateur Compte AWS root (console) dans le guide de l'utilisateur IAM.

Création d'un utilisateur doté d'un accès administratif

1. Activez IAM Identity Center.

   Pour obtenir des instructions, consultez Activation d' AWS IAM Identity Center dans le Guide de l'utilisateur AWS IAM Identity Center .

2. Dans IAM Identity Center, octroyez un accès administratif à un utilisateur.

   Pour un didacticiel sur l'utilisation du Répertoire IAM Identity Center comme source d'identité, voir Configurer l'accès utilisateur par défaut Répertoire IAM Identity Center dans le Guide de AWS IAM Identity Center l'utilisateur.

Connexion en tant qu'utilisateur doté d'un accès administratif

- Pour vous connecter avec votre utilisateur IAM Identity Center, utilisez l'URL de connexion qui a été envoyée à votre adresse e-mail lorsque vous avez créé l'utilisateur IAM Identity Center.

  Pour obtenir de l'aide pour vous connecter en utilisant un utilisateur d'IAM Identity Center, consultez la section Connexion au portail AWS d'accès dans le guide de l'Connexion à AWS utilisateur.

Attribution d'un accès à d'autres utilisateurs

1. Dans IAM Identity Center, créez un ensemble d'autorisations qui respecte la bonne pratique consistant à appliquer les autorisations de moindre privilège.

   Pour obtenir des instructions, consultez Création d'un ensemble d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .

2. Attribuez des utilisateurs à un groupe, puis attribuez un accès par authentification unique au groupe.

Pour obtenir des instructions, consultez Ajout de groupes dans le Guide de l'utilisateur AWS IAM Identity Center .

Télécharger les outils

AWS Management Console Il inclut une console pour Amazon Route 53, mais si vous souhaitez accéder aux services par programmation, consultez ce qui suit :

- Le guide de l'API décrit les opérations prises en charge par les services et fournit des liens vers la documentation associée au kit SDK et à la CLI :
  - Référence API Amazon Route 53
- Pour appeler une API sans avoir à gérer des détails de bas niveau tels que l'assemblage de requêtes HTTP brutes, vous pouvez utiliser un AWS SDK. Ils AWS SDKs fournissent des fonctions et des types de données qui encapsulent les fonctionnalités des AWS services. Pour télécharger un AWS SDK et accéder aux instructions d'installation, consultez la page correspondante :
  - Java
  - JavaScript
  - .NET
  - Node.js
  - PHP
  - Python
  - Ruby

  Pour une liste complète AWS SDKs, consultez la section Outils pour Amazon Web Services.
- Vous pouvez utiliser le AWS Command Line Interface (AWS CLI) pour contrôler plusieurs AWS services à partir de la ligne de commande. Vous pouvez également automatiser vos commandes à l'aide de scripts. Pour de plus amples informations, veuillez consulter AWS Command Line Interface.
- AWS Tools for Windows PowerShell soutient ces AWS services. Pour plus d'informations, consultez le Guide de référence des cmdlets Outils AWS pour PowerShell.

Utilisation de votre domaine pour un site web statique dans un compartiment Amazon S3

Ce didacticiel de mise en route vous explique comment effectuer les tâches suivantes :

- Enregistrer un nom de domaine, par exemple, example.com
- Créer un compartiment Amazon S3 et le configurer pour qu'il héberge un site web
- Créer un exemple de site web et enregistrer le fichier dans votre compartiment S3
- Configurer Amazon Route 53 pour acheminer le trafic vers votre nouveau site web

Lorsque vous aurez terminé, vous serez en mesure d'ouvrir un navigateur, de saisir le nom de votre domaine et d'afficher votre site web.

> **Note**
>
> Vous pouvez également transférer un domaine existant vers Route 53, mais le processus est plus complexe et plus long que l'enregistrement d'un nouveau domaine. Pour de plus amples informations, veuillez consulter Transfert d'un enregistrement de domaine vers Amazon Route 53.

Rubriques

- Prérequis
- Étape 1 : Enregistrer un domaine
- Étape 2 : créer un compartiment S3 pour votre domaine racine
- Étape 3 (facultatif) : créer un autre compartiment S3, pour votre sous-domaine
- Étape 4 : configurer votre compartiment de domaine racine pour l'hébergement de site web
- Étape 5 :(facultatif) : configurer votre compartiment de sous-domaine pour la redirection de site web
- Étape 6 : télécharger l'index pour créer le contenu du site web
- Étape 7 : Modifier les paramètres de blocage de l'accès public S3
- Étape 8 : Attacher une stratégie de compartiment
- Étape 9 : Tester le point de terminaison de domaine

- Étape 10 : acheminer le trafic DNS pour votre domaine vers le compartiment de votre site web
- Étape 11 : tester votre site web
- Étape 12 (facultatif) : utilisez Amazon CloudFront pour accélérer la diffusion de votre contenu

Prérequis

Avant de commencer, assurez-vous d'avoir terminé les étapes de Configurer Amazon Route 53.

Étape 1 : Enregistrer un domaine

Pour utiliser un nom de domaine (par exemple, example.com), vous devez trouver un nom de domaine qui n'est pas déjà utilisé et l'enregistrer. Lorsque vous enregistrez un nom de domaine, vous le réserver pour votre usage exclusif partout sur Internet, en général pour une durée d'un an. Par défaut, nous renouvelons automatiquement le nom de votre domaine au bout d'un an, mais vous pouvez désactiver le renouvellement automatique. Pour de plus amples informations, veuillez consulter Enregistrement d'un nouveau domaine.

Étape 2 : créer un compartiment S3 pour votre domaine racine

Amazon S3 vous permet de stocker et de récupérer vos données depuis n'importe quel emplacement sur Internet. Pour organiser vos données, vous créez des compartiments et charger vos données dans les compartiments à l'aide d' AWS Management Console. Vous pouvez utiliser Amazon S3 pour héberger un site web statique dans un compartiment. La procédure suivante explique comment créer un compartiment.

Pour créer un compartiment S3 pour votre domaine racine

1. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Choisissez Créer un compartiment.
3. Entrez les valeurs suivantes :

   Nom du compartiment

   Entrez le nom de votre domaine, par exemple example.com.

   Région

   Choisissez la région la plus proche de la majorité de vos utilisateurs.

Notez la région que vous choisissez, car vous en aurez besoin ultérieurement dans le processus.

4. Pour accepter les paramètres par défaut et créer le compartiment, choisissez Create bucket (Créer un compartiment).

Étape 3 (facultatif) : créer un autre compartiment S3, pour votre sous-domaine

Dans la procédure précédente, vous avez créé un compartiment pour votre nom de domaine, par exemple, example.com. Vos utilisateurs peuvent ainsi accéder à votre site web à l'aide de votre nom de domaine, par exemple, example.com.

Si vous souhaitez également que vos utilisateurs puissent utiliser www. *your-domain-name*, tel que www.example.com, pour accéder à votre exemple de site Web, créez un deuxième compartiment S3. Configurez le second compartiment de manière à ce qu'il achemine le trafic vers le premier compartiment.

Pour créer un compartiment S3 pour www. your-domain-name

1. Choisissez Créer un compartiment.
2. Entrez les valeurs suivantes :

   Nom du compartiment

   Entrez www. ***your-domain-name***. Par exemple, si vous avez enregistré le nom de domaine example.com, entrez www.example.com.

   Région

   Choisissez la même région que celle dans laquelle vous avez créé le premier compartiment.
3. Pour accepter les paramètres par défaut et créer le compartiment, choisissez Créer.

Étape 4 : configurer votre compartiment de domaine racine pour l'hébergement de site web

Maintenant que vous disposez d'un compartiment S3, vous pouvez le configurer pour l'hébergement de site web.

Pour autoriser l'hébergement de site web sur votre compartiment S3

1. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la liste Buckets (Compartiments), choisissez le nom du compartiment pour lequel vous souhaitez activer l'hébergement de sites web statiques.
3. Choisissez Propriétés.
4. Sous Static website hosting (Hébergement de site web statique), choisissez Enable (Activer).
5. Choisissez Use this bucket to host a website (Utiliser ce compartiment pour héberger un site web).
6. Sous Static website hosting (Hébergement de site web statique), choisissez Enable (Activer).
7. Dans Index document (Document d'index), entrez le nom du document d'index, généralement `index.html`.

   Le nom du document d'index est sensible à la casse et doit correspondre exactement au nom de fichier du document d'index HTML que vous prévoyez de charger dans votre compartiment S3. Lorsque vous configurez un compartiment pour l'hébergement d'un site web, vous devez indiquer un document d'index. Amazon S3 renvoie ce document d'index lorsque des demandes sont faites dans le domaine racine ou dans n'importe quel sous-dossier.
8. (Facultatif) Si vous souhaitez fournir votre propre document d'erreur personnalisé pour les erreurs de classe 4XX, saisissez le nom du fichier du document d'erreur personnalisé dans Error document (Document d'erreur).

   Si vous ne spécifiez pas de document d'erreur personnalisé et qu'une erreur se produit, Amazon S3 renvoie un document d'erreur HTML par défaut.
9. (Facultatif) Si vous souhaitez spécifier des règles de redirection avancées, décrivez les règles à l'aide du langage XML dans Redirection rules (Règles de redirection).

   Pour plus d'informations, veuillez consulter la section Configuration des redirections conditionnelles avancées dans le Guide de l'utilisateur de la console Amazon Simple Storage Service.
10. Sélectionnez Enregistrer les modifications.
11. Sous Static website hosting (Hébergement de site web statique), notez la valeur de Endpoint (Point de terminaison).

    Endpoint (Point de terminaison) correspond au point de terminaison du site web Amazon S3 de votre compartiment. Une fois que vous avez terminé de configurer votre compartiment en tant

que site web statique, vous pouvez utiliser ce point de terminaison pour tester votre site web, comme illustré dans Étape 9 : Tester le point de terminaison de domaine.

Après avoir suivi les étapes suivantes pour modifier les paramètres d'accès public et ajouter une politique de compartiment qui autorise l'accès public en lecture, vous pouvez utiliser le point de terminaison du site web pour accéder à votre site web.

Étape 5 :(facultatif) : configurer votre compartiment de sous-domaine pour la redirection de site web

Maintenant que vous avez configuré le compartiment de votre domaine racine pour l'hébergement de site web, vous pouvez éventuellement configurer le compartiment de votre sous-domaine pour rediriger toutes les demandes vers le domaine racine. Par exemple, vous pouvez configurer toutes les demandes pour que `www.example.com` soit redirigé vers `example.com`.

Pour configurer une redirection

1. Dans la console Amazon S3, dans la liste Buckets (Compartiments), choisissez le nom de compartiment de votre sous-domaine (par exemple, `www.example.com`).
2. Choisissez Propriétés.
3. Sous Static website hosting (Hébergement de site web statique), choisissez Edit (Modifier).
4. Choisissez Redirect requests for an object (Rediriger les demandes pour un objet).
5. Dans la zone Target bucket (Compartiment cible), entrez votre domaine racine, par exemple, **`example.com`**.
6. Pour Protocol (Protocole), choisissez http.
7. Sélectionnez Enregistrer les modifications.

Étape 6 : télécharger l'index pour créer le contenu du site web

Lorsque vous autorisez l'hébergement de site web statique pour votre compartiment, saisissez le nom du document d'index (par exemple, **`index.html`**). Après avoir autorisé l'hébergement de site web statique pour le compartiment, téléchargez un fichier HTML avec le nom du document de cet index dans votre compartiment.

Pour télécharger un fichier d'index

1. Copiez l'exemple de texte suivant que vous pouvez utiliser comme un simple site web d'une page pour ce didacticiel, collez-le dans un éditeur de texte et enregistrez-le sous index.html :

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

<body>

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

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

</body>

</html>
```

2. Dans la liste Compartiments, choisissez le nom du compartiment pour lequel vous souhaitez activer l'hébergement de sites web statiques.
3. Dans la console Amazon S3, choisissez le nom du compartiment que vous avez créé dans la procédure Pour autoriser l'hébergement de site web sur votre compartiment S3 (cliquez sur le nom du compartiment lié).
4. ChoisissezUpload (Télécharger), puis Add Files (Ajouter des fichiers), sélectionnez index.html à partir de l'emplacement où vous l'avez enregistré, puis choisissez Upload (Télécharger).
5. Si vous avez créé un document d'erreur, par exemple, **`404.html`**, suivez les étapes 3 à 5 pour le télécharger.

Étape 7 : Modifier les paramètres de blocage de l'accès public S3

Par défaut, Amazon S3 bloque l'accès public à votre compte et à vos compartiments. Si vous souhaitez utiliser un compartiment pour héberger un site web statique, appliquez ces étapes pour modifier vos paramètres d'accès public.

> **Warning**
>
> Avant de terminer cette étape, consultez Blocage de l'accès public pour votre stockage Amazon S3 pour garantir que vous comprenez et acceptez les risques liés à l'autorisation de l'accès public. Lorsque vous désactivez les paramètres de blocage de l'accès public pour rendre votre compartiment public, toute personne sur Internet peut accéder à votre compartiment. Nous vous recommandons de bloquer tous les accès publics à vos compartiments.

Pour acheminer le trafic vers votre site web

1. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Choisissez le nom du compartiment que vous avez configuré en tant que site web statique.
3. Choisissez Permissions.
4. Sous Block public access (bucket settings) (Bloquer l'accès public (paramètres de compartiment)), choisissez Edit (Modifier).
5. Effacez Block all public access (Bloquer tous les accès publics) et choisissez Save changes (Enregistrer les modifications).

Amazon S3 désactive les paramètres de blocage de l'accès public pour votre compartiment. Pour créer un site web public statique, vous devrez peut-être aussi modifier les paramètres de blocage de l'accès public de votre compte avant d'ajouter une stratégie de compartiment. Si les paramètres du compte pour la fonctionnalité de blocage de l'accès public sont actuellement activés, une note s'affiche sous Block public access (bucket settings) (Bloquer l'accès public (paramètres de compartiment)).

Étape 8 : Attacher une stratégie de compartiment

Après avoir modifié les paramètres de blocage de l'accès public Amazon S3, vous pouvez ajouter une politique de compartiment pour accorder un accès public en lecture à vos objets du compartiment. Lorsque vous accordez un accès public en lecture, tout le monde sur Internet peut accéder à votre compartiment.

> **Warning**
>
> Avant de terminer cette étape, consultez Blocage de l'accès public pour votre stockage Amazon S3 pour garantir que vous comprenez et acceptez les risques liés à l'autorisation de l'accès public. Lorsque vous désactivez les paramètres de blocage de l'accès public pour rendre votre compartiment public, toute personne sur Internet peut accéder à votre compartiment. Nous vous recommandons de bloquer tous les accès publics à vos compartiments.

Pour acheminer le trafic vers votre site web

1. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Dans Compartiments, choisissez le nom de votre compartiment.
3. Choisissez Permissions.
4. Sous Politique de compartiment, choisissez Modifier.
5. Copiez la stratégie de compartiment suivante et collez-la dans un éditeur de texte. Cette politique accorde à toute personne sur Internet (`"Principal":"*"`) l'autorisation d'obtenir les fichiers (`"Action":["s3:GetObject"]`) dans le compartiment S3 associé à votre nom de domaine (`"arn:aws:s3:::your-domain-name/*"`).

   JSON

```
{
   "Version":"2012-10-17",
   "Statement":[{
      "Sid":"AddPerm",
      "Effect":"Allow",
      "Principal":"*",
      "Action":[
         "s3:GetObject"
      ],
      "Resource":[
         "arn:aws:s3:::your-domain-name/*"
      ]
    }]
}
```

6. Mettez à jour la valeur de `Resource` to*`your-domain-name`*, par exemple**`example.com`**.
7. Sélectionnez Enregistrer les modifications.

Étape 9 : Tester le point de terminaison de domaine

Après avoir configuré votre compartiment de domaine pour héberger un site web public, vous pouvez tester votre point de terminaison. Vous pouvez tester le point de terminaison pour votre compartiment de domaine, car votre compartiment de sous-domaine est configuré pour rediriger le site web, et non pour l'hébergement de site web statique.

> **Note**
>
> Amazon S3 ne prend pas en charge l'accès HTTPS au site web. Si vous souhaitez utiliser le protocole HTTPS, vous pouvez utiliser Amazon CloudFront pour diffuser un site Web statique hébergé sur Amazon S3.
> Pour plus d'informations, voir Exiger le protocole HTTPS pour la communication entre les spectateurs et CloudFront.

1. Dans Compartiments, choisissez le nom de votre compartiment.
2. Choisissez Propriétés.
3. Au bas de la page, sous Héberger un site Web statique, choisissez le Point de terminaison du site Web du compartiment.

   Le document d'index s'ouvre dans une autre fenêtre du navigateur.

Étape 10 : acheminer le trafic DNS pour votre domaine vers le compartiment de votre site web

Vous disposez maintenant d'un site web d'une page dans votre compartiment S3. Pour commencer à router le trafic Internet pour votre domaine vers votre compartiment S3, exécutez la procédure suivante.

Pour acheminer le trafic vers votre site web

1. Ouvrez la console Route 53 à l'adresse https://console.aws.amazon.com/route53/.

2. Dans le panneau de navigation, choisissez Zones hébergées.

> **Note**
>
> Lorsque vous avez enregistré votre domaine, une zone hébergée portant le même nom a été créée automatiquement par Amazon Route 53. Une zone hébergée contient des informations sur la façon dont vous souhaitez que Route 53 achemine le trafic pour le domaine.

3. Dans la liste des zones hébergées, choisissez le nom de votre domaine.
4. Choisissez Create Record (Créer un registre).

> **Note**
>
> Chaque registre contient des informations sur la façon dont vous souhaitez acheminer le trafic pour un domaine (par exemple, example.com) ou un sous-domaine (par exemple, www.example.com ou test.example.com). Les registres sont stockés dans la zone hébergée de votre domaine.

5. Choisissez Switch to wizard (Passer à l'assistant).
6. Choisissez Simple routing (Routage simple), puis Next (Suivant).
7. Choisissez Define simple record (Définir un registre simple).
8. Dans Record name (Nom de registre), acceptez la valeur par défaut, à savoir le nom de votre zone hébergée et de votre domaine.
9. Dans Type d'enregistrement, choisissez A - Achemine le trafic vers une IPv4 adresse et certaines AWS ressources.
10. Dans Value/Route traffic to (Valeur/Acheminer le trafic vers), choisissez Alias to S3 website endpoint (Alias vers le point de terminaison du site web S3).
11. Choisissez la Région.
12. Choisissez le compartiment S3.

    Le nom du compartiment doit correspondre au nom qui apparaît dans la zone Nom. Dans la liste Choose S3 bucket (Choisir un compartiment S3), le nom du compartiment apparaît avec le point de terminaison de site web Amazon S3 pour la région où le compartiment a été créé, par exemple, `s3-website-us-west-1.amazonaws.com (example.com)`.

Choose S3 bucket (Choisir un compartiment S3) répertorie un compartiment si l'une des conditions suivantes est vraie :

- Vous avez configuré le compartiment en tant que site web statique.
- Le nom du compartiment est identique au nom de l'enregistrement que vous créez.
- Le AWS compte courant a créé le compartiment.

Si votre compartiment n'apparaît pas dans la liste Choose S3 bucket (Choisir un compartiment S3), saisissez le point de terminaison de site Web Amazon S3 de la Région dans laquelle le compartiment a été créé, par exemple, **`s3-website-us-west-2.amazonaws.com`**. Pour obtenir la liste complète des points de terminaison de sites Web Amazon S3, consultez Points de terminaison de sites Web Amazon S3. Pour plus d'informations sur la cible d'alias, consultez la section « Valeurs/routage du trafic vers » dans Valeurs spécifiques aux enregistrements d'alias simples.

13. Pour Évaluer l'état de la cible, choisissez Non.
14. Choisissez Définir un enregistrement simple.

(Facultatif) Pour ajouter un registre d'alias pour votre sous-domaine (**`www.example.com`**)

Si vous avez créé un compartiment pour votre sous-domaine, ajoutez également un registre d'alias pour celui-ci.

1. Sous Configure records (Configurer les registres), choisissez Define simple record (Définir un registre simple).
2. Dans Record name (Nom de registre) pour votre sous-domaine, tapez `www`.
3. Dans Type d'enregistrement, choisissez A - Achemine le trafic vers une IPv4 adresse et certaines AWS ressources.
4. Dans Value/Route traffic to (Valeur/Acheminer le trafic vers), choisissez Alias to S3 website endpoint (Alias vers le point de terminaison du site web S3).
5. Choisissez la Région.
6. Choisissez le compartiment S3, par exemple, `s3-website-us-west-2.amazonaws.com (example.com)`.

Si votre compartiment n'apparaît pas dans la liste Choose S3 bucket (Choisir un compartiment S3), saisissez le point de terminaison de site Web Amazon S3 de la Région dans laquelle le compartiment a été créé, par exemple, **`s3-website-us-west-2.amazonaws.com`**.

7. Pour Évaluer l'état de la cible, choisissez Non.
8. Choisissez Définir un enregistrement simple.
9. Dans la page Configure records (Configurer les registres), choisissez Create records (Créer des registres).

Étape 11 : tester votre site web

Pour vérifier que le site Web fonctionne correctement, ouvrez un navigateur Web et accédez à ce qui suit URLs :

- http ://*`your-domain-name`*, par exemple, `example.com` — Affiche le document d'index dans le *`your-domain-name`* compartiment
- http://www. *`your-domain-name`*par exemple, `www.example.com` — Redirige votre demande vers le bucket *`your-domain-name`*

Dans certains cas, il se peut que vous ayez besoin de vider le cache pour observer le comportement attendu.

Pour obtenir des informations plus avancées sur le routage de votre trafic Internet, consultez Configuration d'Amazon Route 53 en tant que service DNS. Pour plus d'informations sur le routage de votre trafic Internet vers AWS les ressources, consultezAcheminement du trafic Internet vers vos AWS ressources.

Étape 12 (facultatif) : utilisez Amazon CloudFront pour accélérer la diffusion de votre contenu

CloudFront est un service Web qui accélère la distribution de votre contenu Web statique et dynamique, tel que les fichiers .html, .css, .js et les fichiers image, à vos utilisateurs. CloudFront diffuse votre contenu via un réseau mondial de centres de données appelés emplacements périphériques. Lorsqu'un utilisateur demande le contenu que vous diffusez CloudFront, il est dirigé vers l'emplacement périphérique offrant le moins de latence (délai), afin que le contenu soit diffusé avec les meilleures performances possibles.

- Si le contenu se trouve déjà dans l'emplacement périphérique où la latence est la plus faible, CloudFront il est diffusé immédiatement.
- Si le contenu ne se trouve pas dans cet emplacement périphérique, il est CloudFront extrait d'un compartiment Amazon S3 ou d'un serveur HTTP (par exemple, un serveur Web) que vous avez identifié comme source de la version définitive de votre contenu.

Pour plus d'informations sur l'utilisation CloudFront pour distribuer le contenu de votre compartiment Amazon S3, consultez la section Ajouter CloudFront lorsque vous distribuez du contenu depuis Amazon S3 dans le manuel Amazon CloudFront Developer Guide.

Utiliser une CloudFront distribution Amazon pour diffuser un site Web statique

Ce didacticiel de mise en route vous explique comment effectuer les tâches suivantes :

- Enregistrez un nom de domaine, par exemple, example.com.
- Créez un certificat pour votre domaine.
- Créez deux compartiments Amazon S3 et configurez l'un d'entre eux pour héberger un site web et l'autre pour exécuter une redirection vers le sous-domaine.
- Créez un exemple de site web et enregistrez le fichier dans votre compartiment S3.
- Créez des CloudFront distributions pour les deux compartiments S3.
- Configurez Amazon Route 53 pour acheminer le trafic vers les CloudFront distributions.

Lorsque vous aurez terminé, vous pourrez ouvrir un navigateur, saisir le nom de votre domaine et afficher votre site web en toute sécurité.

Rubriques

- Prérequis
- Étape 1 : Enregistrer un domaine
- Étape 2 : demander un certificat public
- Étape 3 : créer un compartiment S3 pour héberger votre sous-domaine
- Étape 4 : créer un autre compartiment S3, pour votre domaine racine
- Étape 5 : télécharger des fichiers de site web dans votre compartiment de sous-domaine

- Étape 6 : configurer votre compartiment de domaine racine pour la redirection de site web
- Étape 7 : créer une CloudFront distribution Amazon pour votre sous-domaine
- Étape 8 : créer une CloudFront distribution Amazon pour votre domaine racine
- Étape 9 : Acheminer le trafic DNS de votre domaine vers votre distribution CloudFront
- Étape 10 : tester votre site web

Prérequis

Avant de commencer, assurez-vous d'avoir terminé les étapes de Configurer Amazon Route 53.

Étape 1 : Enregistrer un domaine

Pour utiliser un nom de domaine (par exemple, example.com), vous devez trouver un nom de domaine qui n'est pas déjà utilisé et l'enregistrer. Lorsque vous enregistrez un nom de domaine, vous le réserver pour votre usage exclusif partout sur Internet, en général pour une durée d'un an. Par défaut, nous renouvelons automatiquement le nom de votre domaine au bout d'un an, mais vous pouvez désactiver le renouvellement automatique. Pour plus d'informations, consultez Enregistrement d'un nouveau domaine.

Étape 2 : demander un certificat public

Un certificat public est requis pour que vos CloudFront distributions Amazon soient configurées afin d'obliger les utilisateurs CloudFront à utiliser le protocole HTTPS afin que les connexions soient cryptées lors des CloudFront communications avec les spectateurs.

Pour demander un certificat public AWS Certificate Manager(ACM) (console)

1. Connectez-vous à la console AWS de gestion et ouvrez la console ACM à la https://console.aws.amazon.com/acm/maison.

   > **Note**
   >
   > Assurez-vous de créer le certificat dans la région USA Est (Virginie du Nord). Cela est obligatoire pour Amazon CloudFront.

   Dans la navigation gauche, choisissez Demander un certificat et sur la page Demander un certificat, choisissez Demander un certificat public, puis Suivant.

2. Dans la section Noms de domaine, entrez votre domaine, par exemple **`example.com`**.

   Sous Ajouter un autre nom à ce certificat, entrez un astérisque devant le nom de domaine pour demander un certificat générique pour tous les sous-domaines, comme **`*.example.com`**.
3. Dans la section Méthode de validation, choisissez Validation par DNS.
4. Dans la section Algorithme de clé, choisissez RSA 2048.
5. Dans la section Ajouter des balises vous pouvez éventuellement baliser votre certificat. Les balises sont des paires clé-valeur qui servent de métadonnées pour identifier et organiser AWS les ressources.

   Choisissez Requête pour accéder à la page Certificats.
6. Une fois que votre nouveau certificat apparaît dans le statut En attente, choisissez l'ID du certificat, puis sur la page des détails du certificat, choisissez Créer un enregistrement dans Route 53 pour ajouter automatiquement les enregistrements CNAME pour vos domaines, puis choisissez Créer des enregistrements.

   La page Status du certificat doit s'ouvrir avec un rapport de bannière d'état Enregistrements DNS créés avec succès.

   Votre nouveau certificat doit rester affiché avec le statut Validation en attente pendant au moins 30 minutes.

Étape 3 : créer un compartiment S3 pour héberger votre sous-domaine

Pour créer un compartiment S3 pour www. your-domain-name

Amazon S3 vous permet de stocker et de récupérer vos données depuis n'importe quel emplacement sur Internet. Dans cette étape, vous créez un compartiment S3 pour stocker tous les fichiers de votre site web.

1. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Choisissez Créer un compartiment.
3. Entrez les valeurs suivantes :

   Nom du compartiment

   Entrez www. ***`your-domain-name`***. Par exemple, si vous avez enregistré le nom de domaine example.com, entrez www.example.com.

Région

Choisissez une région pour votre compartiment.

4. Pour accepter les paramètres par défaut et créer le compartiment, choisissez Create bucket (Créer un compartiment).

   Pour plus d'informations sur les paramètres du compartiment S3, consultez Affichage des propriétés d'un compartiment dans le Guide de l'utilisateur Amazon S3.

Étape 4 : créer un autre compartiment S3, pour votre domaine racine

Si vous souhaitez également que vos utilisateurs puissent utiliser le domaine racine,. *your-domain-name*(par exemple example.com) pour accéder à votre exemple de site Web, créez un deuxième compartiment S3. Dans ce didacticiel, vous configurez ensuite le second compartiment (domaine racine) de manière à ce qu'il achemine le trafic vers le premier compartiment.

Pour créer un compartiment S3 pour your-domain-name

1. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Choisissez Créer un compartiment.
3. Entrez les valeurs suivantes :

   Nom du compartiment

   Saisissez ***your-domain-name***. Par exemple, si vous avez enregistré le nom de domaine example.com, saisissez example.com.

   Région

   Choisissez la même région que celle dans laquelle vous avez créé le premier compartiment.

4. Pour accepter les paramètres par défaut et créer le compartiment, choisissez Create bucket (Créer un compartiment).

Étape 5 : télécharger des fichiers de site web dans votre compartiment de sous-domaine

Maintenant que vous disposez d'un compartiment S3, vous pouvez télécharger les fichiers de votre site web. Dans ce didacticiel, vous allez simplement télécharger un fichier index.html simple qui affiche du texte sur une page.

Pour activer l'hébergement de site web pour votre compartiment S3

1. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la liste Buckets (Compartiments), choisissez le nom lié du compartiment pour lequel vous souhaitez télécharger les fichiers de site web, comme **`www.example.com`**.
3. Copiez l'exemple de texte qui crée un site web simple d'une page, collez-le dans un éditeur de texte et enregistrez-le sous index.html :

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

<body>

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

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

</body>

</html>
```

4. Dans l'onglet Objects (Objets), choisissez Upload (Télécharger).
5. Sous Files and folders (Fichiers et dossiers), choisissez Add files (Ajouter des fichiers) et téléchargez les fichiers de votre site web. Pour ce didacticiel, téléchargez le fichier index.html que vous avez enregistré à l'étape 3 de cette procédure.

Étape 6 : configurer votre compartiment de domaine racine pour la redirection de site web

Maintenant que vous avez configuré le compartiment de votre domaine racine pour l'hébergement de site web, vous pouvez éventuellement configurer le compartiment de votre domaine racine pour rediriger toutes les demandes vers le sous-domaine. Par exemple, vous pouvez configurer toutes les demandes pour que `example.com` soit redirigé vers `www.example.com`.

Pour configurer une redirection

1. Dans la console Amazon S3, dans la liste Buckets (Compartiments), choisissez le nom de votre compartiment (par exemple, `example.com`).
2. Choisissez Propriétés.
3. Sous Static website hosting (Hébergement de site web statique), choisissez Edit (Modifier).
4. Sous Static website hosting (Hébergement de site web statique), sélectionnez Enable (Activer).
5. Choisissez Redirect requests for an object (Rediriger les demandes pour un objet).
6. Dans l'encadré Host name (Nom d'hôte), saisissez votre sous-domaine, par exemple, **`www.example.com`**.
7. Pour Protocole, choisissez HTTPS.
8. Sélectionnez Enregistrer les modifications.
9. Sous Static website hosting (Hébergement de site web statique), notez la valeur de Endpoint (Point de terminaison).

   Endpoint (Point de terminaison) correspond au point de terminaison du site web Amazon S3 de votre compartiment. Vous utiliserez ce point de terminaison pour configurer une CloudFront distribution Amazon.

Étape 7 : créer une CloudFront distribution Amazon pour votre sous-domaine

Dans cette étape, vous créez une distribution CloudFront pour votre sous-domaine, comme www.exemple.com, pour permettre à votre site Web d'utiliser HTTPS afin que les utilisateurs puissent l'afficher en toute sécurité.

Pour créer une distribution CloudFront

1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Choisissez Create Distribution.
3. Sous Origine, pour Domaine d'origine, choisissez le compartiment Amazon S3 que vous avez créé plus tôt. Le format ressemblera à**`www.example.com.s3.<Region>.amazonaws.com`**.

   Pour l'accès d'origine, sélectionnez Identités d'accès existantes. Pour Origin access identity (Identité d'accès à l'origine), vous pouvez choisir dans la liste ou choisir Create new OAI (Créer une nouvelle OAI) (les deux options fonctionneront).

   Sous Bucket policy (Politique de compartiment), choisissez Yes, update the bucket policy (Oui, mettre à jour la politique de compartiment).
4. Pour les paramètres sous Default Cache Behavior Settings (Paramètres de comportement du cache par défaut), sous Viewer (Utilisateur), définissez Viewer protocol policy (Politique du protocole d'utilisateur) sur Redirect HTTP to HTTPS (Rediriger HTTP vers HTTPS) et acceptez les valeurs par défaut pour les autres options.

   Pour plus d'informations sur les options de comportement du cache, consultez la section Paramètres du comportement du cache dans le guide du CloudFront développeur Amazon.
5. Dans la section Web Application Firewall (WAF), vous pouvez choisir d'activer ou de désactiver les protections de sécurité AWS WAF .
6. Pour les champs sous Settings (Paramètres), procédez comme suit :

   - Choisissez Add item (Ajouter un élément) pour Alternate domain name (CNAME) - optional (Autre nom de domaine [CNAME] – facultatif), et saisissez votre sous-domaine, comme **`www.example.com`**.
   - Pour Custom SSL Certificate (Certificat SSL personnalisé), choisissez le certificat que vous avez créé plus tôt.
   - Dans la zone de texte Default root object (Objet racine par défaut), saisissez **`index.html`**.
   - Pour le reste, acceptez les valeurs par défaut et choisissez Créer une distribution.

     Pour plus d'informations sur les options de distribution, consultez Paramètres de distribution.

7. Après avoir CloudFront créé votre distribution, la valeur de la colonne État de votre distribution passe de En cours à Déployé. Cela prend généralement quelques minutes.

Enregistrez le nom de domaine CloudFront attribué à votre distribution, qui apparaît dans la liste des distributions. Vous pouvez utiliser ce nom de domaine pour tester la distribution.

Étape 8 : créer une CloudFront distribution Amazon pour votre domaine racine

Au cours de cette étape, vous créez une CloudFront distribution pour votre domaine racine afin qu'il utilise le protocole HTTPS lorsque son URL est redirigée vers le sous-domaine.

Pour créer une distribution CloudFront

1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Choisissez Create Distribution.
3. Sous Origin Settings (Paramètres d'origine), pour Origin Domain Name (Nom de domaine d'origine), saisissez le point de terminaison du site web du compartiment. Vous pouvez l'obtenir depuis la section Static website hosting (Hébergement de site web statique) des Properties (Propriétés) du compartiment Amazon S3 que vous avez créé plus tôt.

   Pour le reste, acceptez les valeurs par défaut.
4. Dans la section Web Application Firewall (WAF), vous pouvez choisir d'activer ou de désactiver les protections de sécurité AWS WAF .
5. Pour les champs situés sous Clé de cache et requêtes d'origine, sélectionnez Politique de cache et Politique de demandes d'origine (recommandée) et dans le menu déroulant Politique de cache, choisissez CachingDisabled

   Pour le reste, acceptez les valeurs par défaut.

   Pour plus d'informations sur les options de comportement du cache, consultez la section Paramètres du comportement du cache dans le guide du CloudFront développeur Amazon.
6. Pour les champs sous Settings (Paramètres), procédez comme suit :

   - Choisissez Add item (Ajouter un élément) pour Alternate domain name (CNAME) - optional (Autre nom de domaine [CNAME] – facultatif), et saisissez votre domaine racine, comme **`example.com`**.
   - Pour Custom SSL Certificate (Certificat SSL personnalisé), choisissez le certificat que vous avez créé plus tôt.

- Pour le reste, acceptez les valeurs par défaut.

Pour plus d'informations sur les options de distribution, consultez Paramètres de distribution.

7. En bas de la page, cliquez sur Créer une distribution.
8. Après avoir CloudFront créé votre distribution, la valeur de la colonne État de votre distribution passe de En cours à Déployé. Cela prend généralement quelques minutes.

   Enregistrez le nom de domaine CloudFront attribué à votre distribution, qui apparaît dans la liste des distributions. Vous pouvez utiliser ce nom de domaine pour tester la distribution,

Étape 9 : Acheminer le trafic DNS de votre domaine vers votre distribution CloudFront

Votre compartiment S3 contient désormais un site Web d'une page qui utilise une CloudFront distribution. Pour commencer à acheminer le trafic Internet de votre domaine vers la CloudFront distribution, effectuez la procédure suivante.

Pour plus d'informations sur le routage du trafic vers CloudFront les distributions, consultezAcheminement du trafic vers une CloudFront distribution Amazon à l'aide de votre nom de domaine.

Pour acheminer le trafic vers votre site web

1. Ouvrez la console Route 53 à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le panneau de navigation, choisissez Zones hébergées.

   > **Note**
   >
   > Lorsque vous avez enregistré votre domaine, une zone hébergée portant le même nom a été créée automatiquement par Amazon Route 53. Une zone hébergée contient des informations sur la façon dont vous souhaitez que Route 53 achemine le trafic pour le domaine.

3. Dans la liste des zones hébergées, choisissez le nom de votre domaine.
4. Choisissez Create Record (Créer un registre).

Si la vue définie est Quick create record (Création rapide de registre), choisissez Switch to wizard (Passer à l'assistant).

> **Note**
>
> Chaque registre contient des informations sur la façon dont vous souhaitez acheminer le trafic pour un domaine (par exemple, example.com) ou un sous-domaine (par exemple, www.example.com ou test.example.com). Les registres sont stockés dans la zone hébergée de votre domaine.

5. Choisissez Simple routing (Routage simple), puis Next (Suivant).
6. Choisissez Define simple record (Définir un registre simple).
7. Dans Record name (Nom de registre), saisissez **`www`** pour la valeur par défaut, à savoir le nom de votre zone hébergée et de votre domaine.
8. Dans Type d'enregistrement, choisissez A - Achemine le trafic vers une IPv4 adresse et certaines AWS ressources.
9. Dans Valeur/Router le trafic vers, choisissez Alias vers la CloudFront distribution.
10. Choisissez la distribution.

    Le nom de la distribution doit correspondre au nom qui apparaît dans l'encadré Domain name (Nom de domaine) dans la liste Distributions, par exemple, `dddjjjkkk.cloudfront.net`.
11. Pour Évaluer l'état de la cible, choisissez Non.
12. Choisissez Définir un enregistrement simple.

Pour ajouter un registre d'alias pour votre domaine racine (**`example.com`**)

Ajoutez également un registre d'alias pour votre domaine racine, afin qu'il pointe vers le compartiment S3 qui redirige le trafic vers `www.example.com`. Pour plus d'informations sur le routage du trafic vers CloudFront les distributions, consultezAcheminement du trafic vers une CloudFront distribution Amazon à l'aide de votre nom de domaine.

1. Dans le panneau de navigation, choisissez Zones hébergées.
2. Dans la liste des zones hébergées, choisissez le nom de votre domaine.
3. Choisissez Create Record (Créer un registre).

Si la vue définie est Quick create record (Création rapide de registre), choisissez Switch to wizard (Passer à l'assistant).

> **Note**
>
> Chaque registre contient des informations sur la façon dont vous souhaitez acheminer le trafic pour un domaine (par exemple, example.com) ou un sous-domaine (par exemple, www.example.com ou test.example.com). Les registres sont stockés dans la zone hébergée de votre domaine.

4. Choisissez Simple routing (Routage simple), puis Next (Suivant).
5. Choisissez Define simple record (Définir un registre simple).
6. Dans Record name (Nom de registre), acceptez la valeur par défaut.
7. Dans Type d'enregistrement, choisissez A - Achemine le trafic vers une IPv4 adresse et certaines AWS ressources.
8. Dans Value/Route traffic to (Valeur/routage du trafic vers), choisissez Alias to CloudFront distribution (Alias vers la distribution).
9. Choisissez la distribution.

   Le nom de la distribution doit correspondre au nom qui apparaît dans l'encadré Domain name (Nom de domaine) dans la liste Distributions, par exemple, `dddjjjkkk.cloudfront.net`.
10. Pour Évaluer l'état de la cible, choisissez Non.
11. Choisissez Définir un enregistrement simple.
12. Dans la page Configurer des enregistrements, choisissez Créer des enregistrements.

Étape 10 : tester votre site web

Pour vérifier que le site Web fonctionne correctement, ouvrez un navigateur Web et accédez à ce qui suit URLs :

- https://www. *`your-domain-name`*, par exemple, `www.example.com` — Affiche le document d'index dans le *`www.your-domain-name`* compartiment
- https ://par *`your-domain-name`* exemple, `example.com` — Redirige votre demande vers le bucket *`www.your-domain-name`*

Dans certains cas, il se peut que vous ayez besoin de vider le cache pour observer le comportement attendu.

Pour obtenir des informations plus avancées sur le routage de votre trafic Internet, consultez Configuration d'Amazon Route 53 en tant que service DNS. Pour plus d'informations sur le routage de votre trafic Internet vers AWS les ressources, consultezAcheminement du trafic Internet vers vos AWS ressources.

Intégration à d'autres services

Vous pouvez intégrer Amazon Route 53 à d'autres AWS services pour enregistrer les demandes envoyées à l'API Route 53, surveiller l'état de vos ressources et attribuer des balises à vos ressources. En outre, vous pouvez utiliser Route 53 pour acheminer le trafic Internet vers vos ressources AWS .

Rubriques

- Journalisation, surveillance et balisage
- Acheminement du trafic vers d'autres AWS ressources

Journalisation, surveillance et balisage

AWS CloudTrail

Amazon Route 53 est intégré à AWS CloudTrail un service qui capture des informations sur chaque demande envoyée à l'API Route 53 par votre AWS compte. Vous pouvez utiliser les informations contenues dans les fichiers CloudTrail journaux pour déterminer quelles demandes ont été envoyées à Route 53, l'adresse IP source à partir de laquelle chaque demande a été faite, qui a fait la demande, quand elle a été faite, etc.

Pour de plus amples informations, veuillez consulter Journalisation des appels d'API Amazon Route 53 avec AWS CloudTrail.

Amazon CloudWatch

Vous pouvez utiliser Amazon CloudWatch pour surveiller l'état (sain ou non) de vos bilans de santé Route 53. Les vérifications de l'état surveillent l'état et les performances de vos applications web, de vos serveurs web et d'autres ressources. À intervalles réguliers que vous spécifiez, Route 53 envoie des demandes automatiques via Internet à votre application, à votre serveur ou à d'autres ressources pour vérifier qu'ils sont accessibles, disponibles et qu'ils fonctionnent.

Pour de plus amples informations, veuillez consulter Surveillance des bilans de santé à l'aide CloudWatch.

Tag Editor

Une balise est une étiquette que vous attribuez à une AWS ressource, notamment aux domaines Route 53, aux zones hébergées et aux bilans de santé. Chaque étiquette est constituée d'une

clé et d'une valeur, que vous définissez. Par exemple, vous pouvez attribuer une balise à un enregistrement de domaine qui possède la clé « Customer » et la valeur « Exemple Corp ». Vous pouvez utiliser des balises à diverses fins ; une utilisation courante consiste à classer et à suivre vos AWS coûts.

Pour de plus amples informations, veuillez consulter Balisage des ressources Amazon Route 53.

Acheminement du trafic vers d'autres AWS ressources

Vous pouvez utiliser Amazon Route 53 pour acheminer le trafic vers diverses AWS ressources.

Amazon API Gateway

Amazon API Gateway vous permet de créer, de publier, de gérer, de surveiller et de sécuriser APIs à n'importe quelle échelle. Vous pouvez créer APIs cet accès AWS ou d'autres services Web, ainsi que des données stockées dans le AWS cloud.

Vous pouvez utiliser Route 53 pour acheminer le trafic vers une API API Gateway. Pour de plus amples informations, veuillez consulter Acheminer le trafic vers une API Amazon API Gateway à l'aide de votre nom de domaine.

Amazon CloudFront

Pour accélérer la diffusion de votre contenu Web, vous pouvez utiliser Amazon CloudFront, le réseau de diffusion de AWS contenu (CDN). CloudFront peut diffuser l'intégralité de votre site Web, y compris le contenu dynamique, statique, en streaming et interactif, en utilisant un réseau mondial de sites périphériques. CloudFront achemine les demandes relatives à votre contenu vers l'emplacement périphérique offrant à vos utilisateurs la latence la plus faible. Vous pouvez utiliser Route 53 pour acheminer le trafic de votre domaine vers votre CloudFront distribution. Pour de plus amples informations, veuillez consulter Acheminement du trafic vers une CloudFront distribution Amazon à l'aide de votre nom de domaine.

Amazon EC2

Amazon EC2 fournit une capacité de calcul évolutive dans le AWS cloud. Vous pouvez lancer un environnement informatique EC2 virtuel (une instance) à l'aide d'un modèle préconfiguré (Amazon Machine Image, ou AMI). Lorsque vous lancez une EC2 instance, le système d'exploitation (Linux ou Microsoft Windows) et les logiciels supplémentaires inclus dans l'AMI, tels que le serveur Web ou le logiciel de base de données, sont EC2 automatiquement installés.

Si vous hébergez un site Web ou exécutez une application Web sur une EC2 instance, vous pouvez acheminer le trafic de votre domaine, tel que example.com, vers votre serveur à l'aide de Route 53. Pour de plus amples informations, veuillez consulter Acheminement du trafic vers une EC2 instance Amazon.

AWS Elastic Beanstalk

Si vous déployez et gérez des applications dans le AWS cloud, vous pouvez utiliser Route 53 pour acheminer le trafic DNS de votre domaine, tel que example.com, vers un environnement Elastic Beanstalk. AWS Elastic Beanstalk Pour de plus amples informations, veuillez consulter Acheminement du trafic vers un AWS Elastic Beanstalk environnement.

Elastic Load Balancing

Si vous hébergez un site Web sur plusieurs EC2 instances Amazon, vous pouvez répartir le trafic vers votre site Web entre les instances à l'aide d'un équilibreur de charge Elastic Load Balancing (ELB). Le service ELB adapte automatiquement l'équilibreur de charge au fur et à mesure que le trafic vers votre site web change au fil du temps. L'équilibreur de charge peut également surveiller l'état de ses instances enregistrées et n'acheminer le trafic de domaine qu'aux instances saines.

Vous pouvez utiliser Route 53 pour acheminer le trafic pour votre domaine vers votre Classic Load Balancer, Application Load Balancer ou Network Load Balancer. Pour de plus amples informations, veuillez consulter Routage du trafic vers un équilibreur de charge ELB.

Amazon Lightsail

Amazon Lightsail fournit des capacités et fonctionnalités de calcul, de stockage et de capacité réseau pour déployer et gérer des sites web, des applications web et des bases de données dans le cloud pour un prix mensuel faible et prévisible.

Si vous utilisez Lightsail, vous pouvez utiliser Route 53 pour acheminer le trafic vers votre instance Lightsail. Pour de plus amples informations, consultez Utilisation de Route 53 pour pointer un domaine vers une instance Amazon Lightsail.

Amazon S3

Amazon Simple Storage Service (Amazon S3) offre un stockage dans le cloud extrêmement évolutif, durable et sécurisé. Vous pouvez configurer un compartiment S3 pour héberger un site web statique qui peut inclure des pages web et des scripts côté client. (S3 ne prend pas en charge le scripting côté serveur). Vous pouvez utiliser Route 53 pour acheminer le trafic vers un compartiment Amazon S3. Pour plus d’informations, consultez les rubriques suivantes :

- Pour plus d'informations sur le routage du trafic vers un compartiment, consultez Routage du trafic vers un site Web hébergé dans un compartiment Amazon S3.
- Pour obtenir une description plus détaillée de l'hébergement d'un site web statique dans un compartiment S3, consultez Mise en route avec Amazon Route 53.

Amazon Virtual Private Cloud (Amazon VPC)

Un point de terminaison d'interface vous permet de vous connecter à des services alimentés par AWS PrivateLink. Ces services incluent certains AWS services, des services hébergés par d'autres AWS clients et partenaires eux-mêmes VPCs (appelés services de point de terminaison) et des services AWS Marketplace partenaires pris en charge.

Vous pouvez utiliser Route 53 pour acheminer le trafic vers un point de terminaison d'interface. Pour de plus amples informations, veuillez consulter Acheminer le trafic vers un point de terminaison d'interface Amazon Virtual Private Cloud à l'aide de votre nom de domaine.

Amazon WorkMail

Si vous utilisez Amazon WorkMail pour vos e-mails professionnels et que vous utilisez Route 53 comme service DNS, vous pouvez utiliser Route 53 pour acheminer le trafic vers votre domaine de WorkMail messagerie Amazon. Pour de plus amples informations, veuillez consulter Acheminement du trafic vers Amazon WorkMail.

Pour plus d’informations, consultez Acheminement du trafic Internet vers vos AWS ressources.

Format de nom de domaine DNS

Les noms de domaine (y compris les noms de domaine, les zones hébergées et les enregistrements) sont une série d'étiquettes séparées par des points. La taille de chaque étiquette peut aller jusqu'à 63 octets. La longueur totale d'un nom de domaine ne peut pas dépasser 255 octets, y compris les points. Amazon Route 53 prend en charge tous les noms de domaine valides.

Les conventions de dénomination diffèrent si vous enregistrez un nom de domaine ou si vous spécifiez le nom d'une zone hébergée ou d'un enregistrement. Consultez la rubrique applicable.

Rubriques

- Mise en forme des noms de domaine pour l'enregistrement de noms de domaine
- Mise en forme des noms de domaine pour les zones hébergées et les enregistrements
- Utilisation d'un astérisque (*) dans les noms des zones hébergées et des enregistrements
- Mise en forme des noms de domaine internationalisés

Mise en forme des noms de domaine pour l'enregistrement de noms de domaine

Pour un enregistrement de nom de domaine, un nom de domaine peut uniquement contenir les caractères a-z, 0-9 et – (trait d'union). Vous ne pouvez pas spécifier un trait d'union au début ou à la fin d'une étiquette.

Pour plus d'informations sur la façon d'enregistrer un nom de domaine internationalisé (IDN), consultez Mise en forme des noms de domaine internationalisés.

Mise en forme des noms de domaine pour les zones hébergées et les enregistrements

Pour les zones hébergées et les enregistrements, le nom de domaine peut inclure n'importe quel caractère ASCII imprimable de la liste suivante (à l'exception des espaces) :

- a-z
- 0-9

- - (trait d'union)
- ! " # $ % & ' ( ) * + , - / : ; < = > ? @ [\ ] ^ _ ` { | } ~ .

Amazon Route 53 stocke les caractères alphabétiques sous forme de lettres minuscules (a-z), quelle que soit la manière dont vous les spécifiez : lettres majuscules, lettres minuscules ou lettres correspondantes sous forme de codes d'échappement.

Si votre nom de domaine contient l'un des caractères suivants, vous devez les spécifier à l'aide de codes d'échappement au format \ *three-digit octal code* :

- Caractères 000 à 040 octal (0 à 32 décimal, 0x00 à 0x20 hexadécimal)
- Caractères 177 à 377 octal (127 à 255 décimal, 0x7F à 0xFF hexadécimal)
- . (point), caractère 056 octal (46 décimal, 0x2E hexadécimal), lorsqu'il s'agit d'un caractère dans un nom de domaine. Lorsque vous utilisez . comme délimiteur entre les étiquettes, vous n'avez pas besoin d'utiliser de code d'échappement.

Si le nom de domaine comporte des caractères autres que a à z, 0 à 9, - (tiret) ou _ (trait de soulignement), les actions d'API Route 53 renvoient les caractères en tant que codes d'échappement. C'est le cas si vous spécifiez les caractères en tant que caractères ou en tant que codes d'échappement lorsque vous créez l'entité. La console Route 53 affiche les caractères en tant que caractères, et non en tant que codes d'échappement.

Pour obtenir la liste des caractères ASCII et des codes octaux correspondants, recherchez « table ascii » sur Internet.

Pour spécifier un nom de domaine internationalisé (IDN), convertissez le nom en Punycode. Pour de plus amples informations, veuillez consulter Mise en forme des noms de domaine internationalisés.

Utilisation d'un astérisque (*) dans les noms des zones hébergées et des enregistrements

Vous pouvez créer des zones hébergées et des enregistrements dont le nom comporte un *.

Zones hébergées

- Vous ne pouvez pas inclure un * dans l'étiquette la plus à gauche dans un nom de domaine. Par exemple, *.example.com n'est pas autorisé.

- Si vous incluez * à un autre endroit, DNS le traite comme un caractère * (ASCII 42), et non comme un caractère générique.

Enregistrements

DNS traite le caractère * comme un caractère générique ou comme le caractère * (ASCII 42), en fonction de son emplacement dans le nom. Notez les restrictions suivantes relatives à l'utilisation de * comme caractère générique dans le nom d'un enregistrement :

- Le caractère générique * doit remplacer l'étiquette la plus à gauche dans un nom de domaine, par exemple, *.example.com ou *.acme.example.com. Si vous incluez * à un autre endroit, tel que prod.*.example.com, DNS le traite comme un caractère * (ASCII 42), et non comme un caractère générique.
- Le caractère * doit remplacer l'étiquette entière. Par exemple, vous ne pouvez pas spécifier *prod.example.com ou prod*.example.com.
- Les noms de domaine spécifiques sont prioritaires. Par exemple, si vous créez des registres pour *.example.com et acme.example.com, Route 53 répond toujours aux requêtes DNS pour acme.example.com avec les valeurs du registre acme.example.com.
- Le caractère * s'applique aux requêtes DNS pour le niveau du sous-domaine qui inclut l'astérisque, et pour tous les sous-domaines de ce sous-domaine. Par exemple, si vous créez un registre nommé *.example.com, Route 53 utilise les valeurs de ce registre pour répondre aux requêtes DNS pour zenith.example.com, acme.zenith.example.com, et pinnacle.acme.zenith.example.com (s'il n'existe aucun registre de quelque type que ce soit pour cette zone hébergée).

  Si vous créez un registre appelé *.example.com et qu'il n'existe aucun registre example.com, Route 53 répond aux requêtes DNS pour example.com avec `NXDOMAIN` (domaine inexistant).
- Vous pouvez configurer Route 53 pour renvoyer la même réponse aux requêtes DNS pour tous les sous-domaines du même niveau et pour le nom de domaine. Par exemple, vous pouvez configurer Route 53 pour répondre aux requêtes DNS comme acme.example.com et zenith.example.com à l'aide du registre example.com. Procédez comme suit :

  1. Créez un enregistrement pour le domaine, par exemple example.com.
  2. Créez un enregistrement d'alias pour le sous-domaine, par exemple *.example.com. Spécifiez l'enregistrement que vous avez créé à l'étape 1 comme cible pour l'enregistrement d'alias.
- Vous ne pouvez pas utiliser * en tant que caractère générique pour les enregistrements de type NS.

Mise en forme des noms de domaine internationalisés

Lorsque vous enregistrez un nouveau nom de domaine ou créez des zones hébergées et des registres, vous pouvez spécifier des lettres autres que celles de a à z (par exemple, le ç en français), des caractères d'autres alphabets (par exemple, cyrillique ou arabe) et des caractères chinois, japonais ou coréens. Amazon Route 53 stocke ces noms de domaine internationalisés (IDNs) en Punycode, qui représente les caractères Unicode sous forme de chaînes ASCII.

Si vous enregistrez un nom de domaine, notez les informations suivantes :

- Vous pouvez utiliser des caractères autres que a-z, 0-9 et - (tiret) uniquement si le domaine de premier niveau (TLD) prend en charge IDNs et prend en charge la langue que vous souhaitez utiliser. Pour déterminer les langues prises en charge par un domaine de premier niveau, veuillez consulter Domaines que vous pouvez enregistrer avec Amazon Route 53.
- Vous pouvez spécifier un nom dans une langue non prise en charge s'il ne contient que les lettres de « a » à « z » Par exemple, si un domaine de premier niveau ne prend pas en charge le français mais que le nom que vous souhaitez utiliser inclut uniquement les lettres de « a » à « z » sans marque diacritique, vous pouvez utiliser ce nom. Dans cet exemple, un nom qui inclut un « c » est autorisé, mais un nom qui contient un « ç » ne l'est pas.
- Si un TLD ne prend pas en charge IDNs ou ne prend pas en charge la langue que vous souhaitez utiliser pour votre nom de domaine, vous ne pouvez pas non plus spécifier le nom dans Punycode, même si le Punycode inclut uniquement a-z, 0-9 et -.

L'exemple suivant montre la représentation Punycode du nom de domaine internationalisé 中国.asia :

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

Lorsque vous entrez un IDN dans la barre d'adresse d'un navigateur moderne, le navigateur le convertit en Punycode avant de soumettre une requête DNS ou une demande HTTP.

La façon de saisir un IDN dépend de ce que vous créez (noms de domaine, zones hébergées ou registres) et de la façon dont vous le créez (à l'aide d'une API, d'un kit SDK ou de la console Route 53) :

- Si vous utilisez l'API Route 53 ou l'une des API AWS SDKs, vous pouvez convertir par programmation une valeur Unicode en Punycode. Par exemple, si vous utilisez Java, vous pouvez convertir une valeur Unicode en Punycode à l'aide de la méthode toASCII de la bibliothèque java.net.IDN.

- Si vous utilisez la console Route 53 pour enregistrer un nom de domaine, vous pouvez coller le nom, y compris les caractères Unicode, dans le champ du nom, et la console convertit la valeur en Punycode avant de l'enregistrer.
- Si vous utilisez la console Route 53 pour créer des zones hébergées ou des registres, vous devez convertir le nom de domaine en Punycode avant de saisir le nom dans le champ Name (Nom) applicable. Pour plus d'informations sur les convertisseurs en ligne, recherchez « convertisseur punycode » sur Internet.

Si vous enregistrez un nom de domaine, notez que les domaines de premier niveau (TLDs) ne sont pas tous compatibles IDNs. Pour une liste des produits TLDs pris en charge par Route 53, consultezDomaines que vous pouvez enregistrer avec Amazon Route 53. TLDs qui ne sont pas pris en charge IDNs sont notés.

Enregistrement et gestion des domaines à l'aide d'Amazon Route 53

Lorsque vous souhaitez obtenir un nouveau nom de domaine, tel que la partie exemple.com de l'URL http://exemple.com, vous pouvez l'enregistrer avec Amazon Route 53. Vous pouvez également transférer l'enregistrement de domaines existants depuis d'autres bureaux d'enregistrement vers Route 53 ou transférer l'enregistrement de domaines que vous enregistrez avec Route 53 vers d'autres bureaux d'enregistrement.

Les procédures décrites dans ce chapitre expliquent comment enregistrer et transférer des domaines à l'aide de la console Route 53 et comment modifier les paramètres de domaine et afficher le statut du domaine. Si vous enregistrez et gérez seulement quelques domaines, la console est la solution la plus simple.

Si vous avez besoin d'enregistrer et de gérer un grand nombre de domaines, vous pouvez apporter des modifications par programmation. Pour de plus amples informations, veuillez consulter Configurer Amazon Route 53.

> **Note**
>
> Si vous utilisez un langage pour lequel un AWS SDK existe, utilisez le SDK plutôt que d'essayer de vous frayer un chemin dans le. APIs Ils SDKs simplifient l'authentification, s'intègrent facilement à votre environnement de développement et fournissent un accès facile aux commandes Route 53.

Les services d'enregistrement de noms de domaine sont proposés dans le cadre de notre Accord d'enregistrement de nom de domaine.

Rubriques

- Enregistrement de nouveaux domaines
- Mise à jour des paramètres d'un domaine
- Renouvellement d'un enregistrement de domaine
- Restauration d'un domaine arrivé à expiration ou supprimé
- Remplacement de la zone hébergée d'un domaine enregistré auprès de Route 53

- Transfert de domaines
- Transfert du bureau d'enregistrement vers le bureau d'enregistrement Amazon
- Renvoi des e-mails de confirmation et d'autorisation
- Configuration du protocole DNSSEC pour un domaine
- Trouver votre bureau d'enregistrement et d'autres informations concernant votre domaine
- Suppression d'un enregistrement de nom de domaine
- Contacter le AWS Support à propos de problèmes d'enregistrement de domaine
- Téléchargement d'un rapport de facturation de domaine
- Domaines que vous pouvez enregistrer avec Amazon Route 53

Enregistrement de nouveaux domaines

Cette section couvre les sujets suivants relatifs à l'enregistrement de nouveaux domaines avec Amazon Route 53 :

1. Enregistrement d'un nouveau domaine:
   - Découvrez la step-by-step procédure d'enregistrement d'un nouveau domaine à l'aide de la console Route 53.
   - Découvrez les considérations et les conditions préalables à l'enregistrement de domaines, telles que contacter le AWS Support en cas de problème, les tarifs, les domaines de premier niveau pris en charge (TLDs) et la création automatique de zones hébergées.
2. Valeurs que vous spécifiez lorsque vous enregistrez ou transférez un domaine:
   - Découvrez les valeurs que vous devez fournir lors de l'enregistrement ou du transfert d'un domaine, notamment les informations de contact, les paramètres de protection de la vie privée et les options de renouvellement automatique.
   - Comprenez les implications de la modification de certaines valeurs, telles que l'adresse e-mail du propriétaire du domaine ou du titulaire du nom de domaine.
3. Valeurs renvoyées par Amazon Route 53 lorsque vous enregistrez un domaine:
   - Découvrez les valeurs renvoyées par Route 53 après un enregistrement de domaine réussi, notamment la date d'enregistrement, la date d'expiration, les codes d'état du domaine, l'état du verrouillage des transferts et les serveurs de noms.
4. Affichage du statut de l'enregistrement d'un domaine:

- Découvrez comment consulter le statut actuel de l'enregistrement de votre domaine, y compris les codes de statut de l'ICANN et toute action requise de votre part, telle que la vérification de l'adresse e-mail du titulaire.

Enregistrement d'un nouveau domaine

Enregistrer un nouveau domaine ou mettre à jour les serveurs de noms pour un domaine existant

Vous pouvez utiliser Amazon Route 53 avec les domaines que vous enregistrez avec Route 53, et avec les domaines que vous avez enregistré avec d'autres fournisseurs DNS. En fonction de votre fournisseur DNS, choisissez l'une des procédures suivantes pour enregistrer et utiliser un nouveau domaine avec Route 53 :

- Pour l'enregistrement d'un nouveau domaine, voir Pour enregistrer un domaine avec Route 53.
- Pour un domaine existant, consultez Configuration d'Amazon Route 53 en tant que service DNS d'un domaine existant.
- Pour déplacer un domaine vers un autre bureau d'enregistrement, consultez Mise à jour des serveurs de noms lorsque vous souhaitez utiliser un autre service DNS.

Considérations concernant l'enregistrement de domaine

Avant de démarrer, notez les points suivants :

Contacter le AWS Support

Si vous rencontrez des problèmes lors de l'enregistrement d'un domaine, vous pouvez contacter le AWS Support gratuitement. Pour de plus amples informations, veuillez consulter Contacter le AWS Support à propos de problèmes d'enregistrement de domaine.

Tarification d'enregistrement de domaine

Pour plus d'informations sur le coût d'enregistrement d'un domaine, consultez Tarification Amazon Route 53 pour l'enregistrement de domaine.

Domaines pris en charge

Pour obtenir la liste des produits pris en charge TLDs, consultezDomaines que vous pouvez enregistrer avec Amazon Route 53.

Vous ne pouvez pas modifier un nom de domaine après l'avoir enregistré

Si vous enregistrez involontairement un nom de domaine incorrect, il vous est impossible de le modifier. Dans cette situation, vous devez enregistrer un nouveau nom de domaine en veillant à saisir le nom correct. En outre, si vous enregistrez involontairement un nom de domaine, vous ne pourrez pas être remboursé.

AWS crédits

Vous ne pouvez pas utiliser de AWS crédits pour payer les frais d'enregistrement d'un nouveau domaine auprès de Route 53.

Tarifs spéciaux ou premium

Les registres TLD ont attribué des tarifs spéciaux ou premium à certains noms de domaine. Vous ne pouvez pas utiliser Route 53 pour enregistrer un domaine qui dispose d'un tarif spécial ou premium.

Frais pour zones hébergées

Lorsque vous enregistrez un domaine avec Route 53, nous créons automatiquement une zone hébergée pour le domaine et appliquons un coût mensuel peu élevé pour la zone hébergée en plus des frais annuels pour l'enregistrement de domaine. Cette zone hébergée est l'endroit où vous stockez des informations sur la manière d'acheminer le trafic de votre domaine, par exemple vers une EC2 instance Amazon ou une CloudFront distribution. Si vous ne souhaitez pas utiliser votre domaine dès maintenant, vous pouvez supprimer la zone hébergée ; si vous la supprimez dans les 12 heures suivant l'enregistrement du domaine, aucun frais ne sera appliqué pour la zone hébergée sur votre facture AWS . Nous appliquons également des frais peu élevés pour les requêtes DNS que nous recevons pour votre domaine. Pour plus d'informations, consultez Tarification Amazon Route 53.

Remplacement de la zone hébergée d'un domaine

Si vous créez une nouvelle zone hébergée pour un domaine, vous devez également mettre à jour les serveurs de noms pour le domaine afin d'utiliser les mêmes serveurs de noms que la nouvelle zone hébergée. Pour plus d'informations, consultez Remplacement de la zone hébergée d'un domaine enregistré auprès de Route 53

Pour enregistrer un domaine avec Route 53

Pour enregistrer un domaine avec Route 53

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le panneau de navigation, sélectionnez Domaines puis Domaines enregistrés.
3. Sur la page Domaines enregistrés, choisissez Enregistrer des domaines.

   a. Dans la section Rechercher un domaine, entrez le nom du domaine que vous souhaitez enregistrer, puis sélectionnez Rechercher pour vérifier si le nom de domaine est disponible.

      Si le nom de domaine que vous souhaitez enregistrer contient des caractères autres que a-z, A-Z, 0-9 et – (tiret), notez ce qui suit :

      - Vous pouvez entrer le nom en utilisant les caractères applicables. Vous n'avez pas besoin de convertir le nom en Punycode.
      - Une liste de langues s'affiche. Choisissez la langue du nom spécifié. Par exemple, si vous entrez příklad (« exemple » en tchèque), choisissez tchèque (CES) ou tchèque (CZE).

      > **Note**
      >
      > Pour les langues qui ont plusieurs code, vous devrez peut-être essayer les deux. Même si CES et CZE sont synonymes, certains registres TLD ne prennent en charge que l'un ou l'autre.

      Pour plus d'informations sur la spécification d'autres caractères que a-z, 0-9 et - (trait d'union), et de noms de domaine internationaux, consultez Format de nom de domaine DNS.

      Si le domaine que vous avez saisi est disponible, il sera affiché, sinon, des domaines similaires seront affichés sous forme de suggestions.

      Vous pouvez choisir jusqu'à cinq domaines à enregistrer. Les domaines que vous sélectionnez apparaissent dans la liste des domaines sélectionnés.

   b. Pour enregistrer d'autres domaines, répétez les étapes 3a et 3b.

4. Choisissez Passer au paiement.
5. Sur la page Tarification, choisissez le nombre d'années pendant lesquelles vous souhaitez enregistrer le domaine, et indiquez si vous souhaitez que nous renouvelions automatiquement l'enregistrement de votre domaine avant la date d'expiration.

> **Note**
>
> Les enregistrements et renouvellements de noms de domaine ne sont pas remboursables. Si vous activez le renouvellement automatique et que vous décidez que vous ne voulez plus du nom de domaine une fois l'enregistrement renouvelé, vous ne pourrez pas être remboursé du coût du renouvellement.

Choisissez Suivant.

6. Sur la page Informations de contact, entrez les coordonnées du titulaire du domaine, de l'administrateur, du technicien et des contacts de facturation. Les valeurs que vous entrez ici sont appliquées à tous les domaines que vous enregistrez. Pour de plus amples informations, veuillez consulter Valeurs que vous spécifiez lorsque vous enregistrez ou transférez un domaine.

> **Important**
>
> Le contact que vous indiquez comme titulaire lors de l'enregistrement du domaine aura certains droits en tant que titulaire du nom de domaine enregistré, conformément à la politique de transfert de l'ICANN. La plupart des domaines seront supprimés lors de la fermeture de votre compte Compte AWS (pour plus d'informations, voirMon AWS compte est fermé ou définitivement, et mon domaine est enregistré auprès de Route 53), mais si un domaine reste sur un compte fermé, le contact que vous avez indiqué comme titulaire peut être en mesure de demander le transfert du nom de domaine vers un bureau d'enregistrement externe. Par conséquent, il est important que le titulaire de votre liste de contacts soit vous-même ou une autre personne en qui vous avez confiance pour agir de manière responsable.

Notez les considérations suivantes :

Prénom et nom

Pour les champs Prénom et Nom, nous vous recommandons d'indiquer le nom associé à votre identifiant officiel. Pour la modification des paramètres de domaine, certains registres de domaines vous demandent de fournir une preuve de votre identité. Le nom figurant sur votre carte d'identité doit correspondre exactement au nom du contact inscrit pour le domaine.

Contacts différents

Par défaut, nous utilisons les mêmes informations pour tous les trois contacts. Si vous souhaitez saisir des informations différentes pour un ou plusieurs contacts, désactivez la case Identique au contact inscrit.

> **Note**
>
> Pour les domaines .it, le contact inscrit et le contact administratif doivent être identiques.

> **Note**
>
> Pour les domaines .jp, les contacts techniques et administratifs doivent être les mêmes.

Plusieurs domaines

Si vous enregistrez plusieurs domaines, nous utilisons les mêmes informations de contact pour tous les domaines.

Informations supplémentaires nécessaires

Pour certains domaines de premier niveau (TLDs), nous sommes tenus de collecter des informations supplémentaires. Pour ceux-ci TLDs, entrez les valeurs applicables après le champ Code postal/ZIP.

Protection de la confidentialité

Indiquez si vous souhaitez masquer vos informations de contact pour les requêtes WHOIS.

> **Note**
>
> Vous devez définir le même paramètre de confidentialité pour les contacts administratifs, d'enregistrement, techniques et de facturation.

Pour plus d'informations, consultez les rubriques suivantes :

- Activation ou désactivation de la protection de la confidentialité pour les informations de contact pour un domaine
- Domaines que vous pouvez enregistrer avec Amazon Route 53

> **Note**
>
> Pour activer la protection de la confidentialité pour les domaines .uk, .co.uk, .me.uk, et .org.uk, vous devez ouvrir une demande de support et demander la protection de la confidentialité.

Choisissez Suivant.

7. Dans la page Vérifier, vérifiez les informations que vous avez saisies et corrigez-les éventuellement, lisez les conditions d'utilisation et cochez la case pour confirmer que vous avez lu les conditions.

   Sélectionnez Envoyer.

8. Dans le volet de navigation, choisissez Domaines, puis Requêtes.

   Sur cette page, vous pouvez voir le statut du domaine et également si vous devez répondre à l'e-mail de vérification du contact inscrit. Vous pouvez également choisir de renvoyer l'e-mail de vérification.

   Si vous avez spécifié une adresse e-mail pour le contact inscrit qui n'a jamais été utilisée pour enregistrer un domaine avec Route 53, certains registres TLD exigent que vous vérifiez la validité de cette adresse.

   Un e-mail de vérification est envoyé à partir de l'une des adresses suivantes :

- noreply@registrar.amazon — pour les personnes TLDs enregistrées auprès d'Amazon Registrar.
- noreply@domainnameverification.net — pour les TLDs inscriptions auprès de notre associé au bureau d'enregistrement, Gandi. Pour déterminer le bureau d'enregistrement pour votre domaine de premier niveau, consultez Identification de votre bureau d'enregistrement.

> **Important**
>
> Le contact inscrit doit suivre les instructions figurant dans le message afin de confirmer que l'e-mail a été reçu. En l'absence de confirmation, nous devons suspendre le domaine, comme exigé par les réglementations de l'ICANN. Lorsqu'un domaine est suspendu, il n'est pas disponible sur Internet.

a. À réception de l'e-mail de vérification, cliquez sur le lien dans le corps du message permettant de confirmer l'adresse e-mail. Si vous ne recevez pas immédiatement cet e-mail, vérifiez votre dossier de courriers indésirables.

b. Retournez à la page Requêtes. Si le statut n'est pas automatiquement mis à jour avec la valeur l'adresse e-mail est vérifiée, actualisez le navigateur.

9. Lorsque l'enregistrement de domaine est terminé, l'étape suivante dépend de si vous voulez utiliser Route 53 ou un autre service DNS en tant que service DNS pour le domaine :

   - Route 53 – Dans la zone hébergée créée par Route 53 lors de l'enregistrement du domaine, créez des enregistrements pour indiquer à Route 53 comment acheminer le trafic du domaine et des sous-domaines.

     Par exemple, lorsque quelqu'un saisit votre nom de domaine dans un navigateur et que cette requête est transmise à Route 53, souhaitez-vous que Route 53 réponde à la requête avec l'adresse IP d'un serveur web de votre centre de données ou avec le nom d'un équilibreur de charge ELB ?

     Pour de plus amples informations, veuillez consulter Utilisation des enregistrements.

> **Important**
>
> Si vous créez des enregistrements dans une zone hébergée autre que celle créée automatiquement par Route 53, vous devez mettre à jour les serveurs de noms du domaine pour utiliser les serveurs de noms de la nouvelle zone hébergée.

- Un autre service DNS – Configurez votre nouveau domaine pour acheminer les requêtes DNS vers l'autre service DNS. Exécutez la procédure Mise à jour des serveurs de noms pour utiliser un autre bureau d'enregistrement.

Valeurs que vous spécifiez lorsque vous enregistrez ou transférez un domaine

> **Note**
>
> Nous avons mis à jour la console des domaines pour Route 53. Pendant la période de transition, vous pouvez continuer à utiliser l'ancienne console ou vous pouvez utiliser la nouvelle. La plupart des informations renvoyées par Route 53 sont les mêmes pour les deux consoles. Les différences sont indiquées dans la liste suivante.

Lorsque vous enregistrez un domaine ou transférez l'enregistrement d'un domaine vers Amazon Route 53, vous spécifiez les valeurs décrites dans cette rubrique.

> **Note**
>
> Si vous enregistrez plusieurs domaines, Route 53 utilise les valeurs spécifiées pour tous les domaines du panier.

Vous pouvez aussi modifier les valeurs pour un domaine actuellement enregistré avec Route 53. Remarques :

- Si vous modifiez les informations de contact pour le domaine, nous envoyons une notification par e-mail au contact inscrit afin de l'informer de la modification. Cet e-mail provient de

noreply@registrar.amazon. Pour la plupart des modifications, le contact inscrit n'est pas tenu de répondre.

- Pour les modifications d'informations de contact qui constituent également une modification de la propriété, nous envoyons au contact inscrit un e-mail supplémentaire. L'ICANN exige que le contact inscrit confirme la réception de l'e-mail. Pour plus d'informations, consultez les rubriques First Name, Last Name et Organization ultérieurement dans cette section.

Pour plus d'informations sur la modification des paramètres pour un domaine existant, consultez Mise à jour des paramètres d'un domaine .

Valeurs que vous spécifiez

- 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

Identique au contact du titulaire

Indique si vous voulez utiliser les mêmes informations de contact pour l'inscrit du domaine, le contact administratif et le contact technique.

Type de contact

Catégorie pour ce contact. Remarques :

- Si vous sélectionnez une option autre que Person, vous devez entrer un nom d'organisation.
- Pour certains TLDs, la protection de la vie privée disponible dépend de la valeur que vous choisissez pour le type de contact. Pour consulter les paramètres de protection de la confidentialité pour votre domaine de premier niveau, consultez Domaines que vous pouvez enregistrer avec Amazon Route 53.
- Pour les domaines .es, la valeur Type de contact doit être Personne pour les trois contacts.

Prénom, nom

Le prénom et le nom du contact.

> **Important**
>
> Pour les champs Prénom et Nom, nous vous recommandons d'indiquer le nom associé à votre identifiant officiel. Pour certaines modifications apportées aux paramètres de domaine, vous devez fournir une preuve de votre identité. Le nom de votre carte d'identité doit correspondre au nom du contact inscrit pour le domaine.

Si vous transférez un domaine vers Route 53 et que les conditions suivantes sont réunies, alors vous modifiez le propriétaire du domaine :

- Le type de contact est Person (Personne).
- Vous modifiez les champs Prénom et and/or Nom de famille du contact inscrit à partir des paramètres actuels.

Dans ce cas, l'ICANN exige l'envoi d'un e-mail au contact inscrit afin d'obtenir l'approbation. Un e-mail est envoyé à partir de l'une des adresses suivantes :

TLDs	Adresse e-mail qui envoie l'e-mail d'approbation
TLDs enregistré par Amazon Registrar	noreply@registrar.amazon
.fr	nic@nic.fr (l'e-mail est envoyé au contact inscrit actuel et au nouveau contact inscrit.)

TLDs	Adresse e-mail qui envoie l'e-mail d'approbation
Tous les autres	noreply@domainnameverification.net

Pour déterminer le bureau d'enregistrement pour votre domaine de premier niveau, consultez Domaines que vous pouvez enregistrer avec Amazon Route 53.

> **Important**
>
> Le contact inscrit doit suivre les instructions reçues dans l'e-mail afin de confirmer que l'e-mail a été reçu. En l'absence de confirmation, nous devons suspendre le domaine, comme exigé par les réglementations de l'ICANN. Lorsqu'un domaine est suspendu, il n'est pas disponible sur Internet.

Si vous modifiez l'adresse e-mail du contact inscrit, cet e-mail est envoyé à l'ancienne et à la nouvelle adresse e-mail pour le contact inscrit.

Certains bureaux d'enregistrement de domaines de premier niveau appliquent des frais à la modification du propriétaire du domaine. Lorsque vous modifiez l'une de ces valeurs, la console Route 53 affiche un message qui vous indique si des frais seront appliqués.

Organisation

Organisation associée au contact, le cas échéant. Pour les contacts inscrit et administratif, il s'agit généralement de l'organisation qui enregistre le domaine. Pour le contact technique, cela peut être l'organisation qui gère le domaine.

Lorsque le type de contact est une valeur autre que Person et que vous modifiez le champ Organization pour le contact inscrit, vous modifiez le propriétaire du domaine. L'ICANN exige l'envoi d'un e-mail au contact inscrit afin d'obtenir l'approbation. Un e-mail est envoyé à partir de l'une des adresses suivantes :

TLDs	Adresse e-mail qui envoie l'e-mail d'approbation
TLDs enregistré par Amazon Registrar	noreply@registrar.amazon

TLDs	Adresse e-mail qui envoie l'e-mail d'approbation
.fr	nic@nic.fr (l'e-mail est envoyé au contact inscrit actuel et au nouveau contact inscrit.)
Tous les autres	noreply@domainnameverification.net

Pour déterminer le bureau d'enregistrement pour votre domaine de premier niveau, consultez Domaines que vous pouvez enregistrer avec Amazon Route 53.

Si vous modifiez l'adresse e-mail du contact inscrit, cet e-mail est envoyé à l'ancienne et à la nouvelle adresse e-mail pour le contact inscrit.

Certains bureaux d'enregistrement de domaines de premier niveau appliquent des frais à la modification du propriétaire du domaine. Lorsque vous modifiez la valeur du champ Organization (Organisation), la console Route 53 affiche un message qui vous indique si des frais seront appliqués.

E-mail

Adresse e-mail du contact.

Si vous modifiez l'adresse e-mail du contact inscrit, nous envoyons un e-mail de notification à l'ancienne et à la nouvelle adresse e-mail. Cet e-mail provient de noreply@registrar.amazon.

Téléphone

Numéro de téléphone du contact :

- Si vous saisissez un numéro de téléphone pour des sites aux États-Unis ou au Canada, entrez 1 dans le premier champ et le numéro de téléphone, indicatif compris, à 10 chiffres dans le deuxième champ.
- Si vous saisissez un numéro de téléphone pour n'importe quel autre pays, entrez le code du pays dans le premier champ et le reste du numéro de téléphone dans le deuxième champ. Pour obtenir la liste des indicatifs pays, consultez l'article de Wikipedia suivant : Liste des indicatifs téléphoniques internationaux par pays.

Adresse 1

Adresse du contact.

Adresse 2

Informations d'adresse supplémentaires du contact, par exemple le numéro d'appartement ou la boîte postale.

Pays

Pays du contact.

État

État ou province du contact, le cas échéant.

Ville

Ville du contact.

Code postal

Code postal du contact.

Champs pour des domaines de premier niveau sélectionnés

Les domaines de premier niveau (TLDs) suivants nécessitent que vous spécifiiez des valeurs supplémentaires :

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

En outre, bon nombre d'entre TLDs eux ont besoin d'un numéro d'identification TVA.

Pour plus d'informations sur les valeurs valides, consultez ExtraParamle manuel Amazon Route 53 API Reference.

Protection de la confidentialité

Si vous souhaitez masquer vos informations de contact pour les requêtes WHOIS. Si vous sélectionnez Activer la protection de la confidentialité (nouvelle console) ou Masquer les informations de contact (ancienne console), les requêtes WHOIS (« qui est ») retourneront des informations de contact pour le bureau d'enregistrement ou la valeur « Protégé par la stratégie ».

> **Note**
>
> Vous devez définir le même paramètre de confidentialité pour les contacts administratifs, d'enregistrement, techniques et de facturation.

Si vous sélectionnez Don't hide contact information, vous recevrez plus de courriers indésirables à l'adresse e-mail que vous avez spécifiée.

N'importe qui peut envoyer une requête WHOIS pour un domaine et récupérer toutes les informations de contact pour ce domaine. La commande WHOIS est disponible dans de nombreux systèmes d'exploitation. Elle est également disponible en tant qu'application web sur de nombreux sites web.

> **Important**
>
> Bien que les informations de contact associées à votre domaine puissent être utilisées par des personnes légitimes, ce sont les expéditeurs de courrier indésirable qui les utilisent le plus souvent pour adresser aux contacts du domaine des courriers indésirables et de fausses offres. En général, nous recommandons de sélectionner Hide contact information pour Privacy Protection.

Pour activer ou désactiver la protection de la confidentialité pour certains domaines, vous devez ouvrir une demande de support et demander la protection de la confidentialité.

Pour plus d'informations sur la protection de la confidentialité, consultez les rubriques suivantes :

- Activation ou désactivation de la protection de la confidentialité pour les informations de contact pour un domaine
- Domaines que vous pouvez enregistrer avec Amazon Route 53

Renouvellement automatique (uniquement disponible lors de la modification des paramètres de domaine)

Permet d'indiquer si vous souhaitez que Route 53 renouvelle automatiquement le domaine avant son expiration. Les frais d'inscription sont débités de votre AWS compte. Sur l'ancienne console, ce paramètre n'est disponible que lors de la modification des paramètres du domaine. Pour de plus amples informations, veuillez consulter Renouvellement d'un enregistrement de domaine.

> **Important**
>
> Si vous désactivez le renouvellement automatique, l'enregistrement du domaine ne sera pas renouvelé à la date d'expiration, ce qui peut entraîner la perdre de contrôle du nom de domaine.

La période pendant laquelle vous pouvez renouveler un nom de domaine varie selon le domaine de premier niveau (TLD). Pour obtenir une vue d'ensemble du renouvellement des domaines, consultez Renouvellement d'un enregistrement de domaine. Pour plus d'informations sur l'extension de l'enregistrement de domaine pour un nombre d'années spécifié, consultez Extension de la période d'enregistrement pour un domaine.

Valeurs renvoyées par Amazon Route 53 lorsque vous enregistrez un domaine

Lorsque vous enregistrez votre domaine avec Amazon Route 53, Route 53 retourne les valeurs suivantes, en plus de celles que vous avez spécifiées.

Registered on

Date à laquelle le domaine a été initialement enregistré avec Route 53.

Expires on

Date et heure auxquelles la période d'enregistrement actuelle expire, à l'heure de Greenwich (GMT).

La période d'enregistrement est généralement d'un an, bien que les registres de certains domaines de premier niveau (TLDs) aient des périodes d'enregistrement plus longues. Pour consulter la période d'enregistrement et de renouvellement pour votre domaine de premier niveau, consultez Domaines que vous pouvez enregistrer avec Amazon Route 53.

Dans la plupart des cas TLDs, vous pouvez prolonger la période d'enregistrement jusqu'à dix ans. Pour de plus amples informations, veuillez consulter Extension de la période d'enregistrement pour un domaine.

Domain name status code

Le statut actuel du domaine.

L'ICANN, l'organisme qui gère une base de données centrale de noms de domaine, a développé un ensemble de codes de statuts pour les noms de domaines (aussi appelés codes EPP) qui vous indiquent le statut de différentes opérations effectuées sur un nom de domaine. Par exemple, l'enregistrement d'un nom de domaine, le transfert d'un nom de domaine vers un autre, le renouvellement de l'enregistrement d'un nom de domaine, etc. Tous les bureaux d'enregistrement utilisent ce même ensemble de codes de statuts.

Pour obtenir une liste des codes de statuts de noms de domaines et la signification de chaque code, accédez au site web de l'ICANN et recherchez codes EPP. (Effectuez une recherche sur le site web de l'ICANN. Les recherches sur Internet renvoient parfois une ancienne version du document.)

Verrouillage du transfert

Indique si le domaine est verrouillé afin de limiter la possibilité qu'une personne transfère votre domaine vers un autre bureau d'enregistrement sans votre permission. Si le domaine est verrouillé, la valeur de Verrouillage du transfert est sur Activé. Si le domaine n'est pas verrouillé, la valeur est sur Désactivé.

Renouvellement automatique

Indique si Route 53 renouvelle automatiquement l'enregistrement pour ce domaine peu de temps avant la date d'expiration.

Authorization code

Code requis si vous souhaitez transférer l'enregistrement de ce domaine vers un autre bureau d'enregistrement. Un code d'autorisation est généré uniquement à votre demande. Pour plus d'informations sur le transfert d'un domaine vers un autre bureau d'enregistrement, consultez Transfert d'un domaine depuis Amazon Route 53 vers un autre bureau d'enregistrement.

Serveurs de noms

Serveurs Route 53 qui répondent aux requêtes DNS pour ce domaine. Nous vous recommandons de ne pas supprimer les serveurs de noms Route 53.

Pour plus d'informations sur l'ajout, la modification ou la suppression de serveurs de noms, consultez Ajout ou modification de serveurs de noms et d'enregistrements de type glue pour un domaine.

Affichage du statut de l'enregistrement d'un domaine

L'ICANN, l'organisme qui gère une base de données centrale de noms de domaine, a développé un ensemble de codes de statuts pour les noms de domaines (aussi appelés codes EPP) qui vous indiquent le statut de différentes opérations, par exemple l'enregistrement d'un nom de domaine, le transfert d'un nom de domaine vers un autre bureau d'enregistrement, le renouvellement de l'enregistrement d'un nom de domaine, etc. Tous les bureaux d'enregistrement utilisent ce même ensemble de codes de statuts.

Pour afficher le code de statut pour vos domaines, exécutez la procédure suivante.

Pour afficher le code de statut ICANN d'un domaine

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le panneau de navigation, développez Domaines, puis choisissez Domaines enregistrés.
3. Sélectionnez le nom lié de votre domaine.
4. Si vous devez effectuer une action, telle que renvoyer l'e-mail de vérification au contact inscrit, une bannière en haut de la page indiquera l'action à effectuer.
5. Le statut actuel de votre domaine s'affiche dans le champ Code de statut du nom de domaine.

   Pour obtenir une liste des codes de statuts de noms de domaines et la signification de chaque code, accédez au site web de l'ICANN et recherchez codes EPP. (Effectuez une recherche sur le site web de l'ICANN. Les recherches sur Internet renvoient parfois une ancienne version du document.)

Vous pouvez également consulter le statut de l'enregistrement sur la page Requêtes.

Pour consulter le statut de l'enregistrement

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation, développez Domaines, puis choisissez Requêtes.

3. Sur la page Demandes, vous pouvez consulter le statut de l'enregistrement, ainsi que le statut de toutes les autres actions, telles que la suppression de domaines, le verrouillage des transferts de domaines, l'ajout ou la suppression de clés DNSSEC, que vous avez effectuées sur des domaines,

   Toute action que vous pourriez avoir à effectuer pour terminer un processus, telle que la vérification de votre adresse e-mail, est également répertoriée.

   - Pour répondre à une demande d'action, sélectionnez le bouton radio à côté du nom de domaine, puis sélectionnez l'action dans le menu déroulant Action.

Mise à jour des paramètres d'un domaine

Cette section fournit des informations sur les sujets suivants relatifs à la gestion des paramètres de domaine dans Route 53 :

1. Mise à jour des informations de contact et de la propriété pour un domaine:
   - Découvrez comment mettre à jour les informations de contact d'un domaine, y compris les contacts administratifs, techniques, de titulaire et de facturation.
   - Comprenez le processus de changement de propriétaire d'un domaine lorsque le registre exige un formulaire de changement de propriétaire de domaine.
2. Activation ou désactivation de la protection de la confidentialité pour les informations de contact pour un domaine:
   - Découvrez comment activer ou désactiver la protection de la confidentialité des informations de contact, qui masque ou révèle vos informations personnelles lors des requêtes WHOIS.
3. Activation ou désactivation du renouvellement automatique pour un domaine:
   - Découvrez comment activer ou désactiver le renouvellement automatique d'un domaine, qui détermine si Route 53 renouvelle automatiquement l'enregistrement avant son expiration.
4. Verrouillage d'un domaine pour empêcher son transfert non autorisé vers un autre bureau d'enregistrement:
   - Découvrez comment verrouiller un domaine pour empêcher tout transfert non autorisé vers un autre bureau d'enregistrement, et comment désactiver le verrouillage en cas de besoin.
5. Extension de la période d'enregistrement pour un domaine:
   - Découvrez le processus de prolongation de la période d'enregistrement d'un domaine, généralement jusqu'à dix ans par tranches d'un an.

6. Mise à jour des serveurs de noms pour utiliser un autre bureau d'enregistrementet Ajout ou modification de serveurs de noms et d'enregistrements de type glue pour un domaine :
   - Découvrez comment mettre à jour les serveurs de noms afin qu'ils utilisent un autre service DNS ou comment configurer des serveurs de noms en marque blanche (personnalisés).
   - Découvrez les considérations et les meilleures pratiques à prendre en compte lors de la modification des serveurs de noms et des enregistrements collés.

Mise à jour des informations de contact et de la propriété pour un domaine

Pour les contacts administratif et technique d'un domaine, vous pouvez modifier toutes les informations de contact sans devoir autoriser les modifications. Pour de plus amples informations, veuillez consulter Mise à jour des informations de contact pour un domaine.

Pour le contact inscrit d'un domaine, vous pouvez modifier la plupart des valeurs sans devoir autoriser les modifications. Cependant, pour certains TLDs, le changement de propriétaire d'un domaine nécessite une autorisation. Pour plus d'informations, consultez la rubrique applicable.

Rubriques

- Qui est le propriétaire d'un domaine ?
- TLDs qui nécessitent un traitement spécial pour changer de propriétaire
- Mise à jour des informations de contact pour un domaine
- Modification du propriétaire d'un domaine lorsque le registre requiert un formulaire de modification de la propriété du domaine

Qui est le propriétaire d'un domaine ?

> **Important**
>
> Le contact que vous indiquez en tant que titulaire aura certains droits en tant que titulaire du nom de domaine enregistré, conformément à la politique de transfert de l'ICANN. La plupart des domaines seront supprimés lors de la fermeture de votre compte Compte AWS (pour plus d'informations, voirMon AWS compte est fermé ou définitivement, et mon domaine est enregistré auprès de Route 53), mais si un domaine reste sur un compte fermé, le contact que vous avez indiqué comme titulaire peut être en mesure de demander le transfert du nom de domaine vers un bureau d'enregistrement externe. Par conséquent, il est important que

le titulaire de votre liste de contacts soit vous-même ou une autre personne en qui vous avez confiance pour agir de manière responsable.

Lorsque le type de contact est Person (Personne) et que vous modifiez les champs First Name (Prénom) ou Last Name (Nom) pour le contact inscrit, vous modifiez le propriétaire du domaine.

Lorsque le type de contact est une valeur autre que Person et que vous modifiez le champ Organization (Organisation), vous modifiez le propriétaire du domaine.

Tenez compte des éléments suivants pour la modification du propriétaire d'un domaine :

- Pour certains TLDs, le changement de propriétaire d'un domaine entraîne des frais. Pour déterminer si des frais sont appliqués pour le TLD de votre domaine, consultez la colonne « Tarification du changement de propriété » dans Tarification Amazon Route 53 pour enregistrement de domaine.

  > **Note**
  >
  > Vous ne pouvez pas utiliser de AWS crédits pour payer les frais éventuels de changement de propriétaire d'un domaine.

- Dans certains cas TLDs, lorsque vous changez de propriétaire d'un domaine, nous envoyons un e-mail d'autorisation à l'adresse e-mail du contact du titulaire. Le contact inscrit doit suivre les instructions de l'e-mail pour autoriser la modification.
- Pour certains TLDs, vous devez remplir un formulaire de changement de propriétaire de domaine et fournir une preuve d'identité afin qu'un ingénieur du support Amazon Route 53 puisse mettre à jour les valeurs pour vous. Si le TLD de votre domaine requiert un formulaire de modification de la propriété du domaine, la console affiche un message contenant un lien vers un formulaire permettant de soumettre une demande de support. Pour de plus amples informations, veuillez consulter Modification du propriétaire d'un domaine lorsque le registre requiert un formulaire de modification de la propriété du domaine.

TLDs qui nécessitent un traitement spécial pour changer de propriétaire

Lorsque vous modifiez le propriétaire d'un domaine, les registres de certains domaines TLDs nécessitent un traitement spécial. Si vous modifiez le propriétaire de l'un des domaines suivants, effectuez la procédure applicable. Si vous modifiez le propriétaire d'un autre domaine, vous pouvez

le modifier vous-même, par programmation ou à l'aide de la console Route 53. Consultez Mise à jour des informations de contact pour un domaine.

Les éléments suivants TLDs nécessitent un traitement spécial pour modifier le propriétaire du domaine :

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

.be

Vous devez obtenir un code de transfert dans le registre pour les domaines .be, puis ouvrir un dossier auprès du AWS Support.

- Pour obtenir le code de transfert, rendez-vous sur https://www.dnsbelgium. be/en/manage-your-domain-name/change-holder #transfer, et suivez les instructions.
- Pour envoyer une demande, consultez Contacter le AWS Support à propos de problèmes d'enregistrement de domaine.

.cl

Vous devez remplir et envoyer un formulaire au AWS Support. Consultez Modification du propriétaire d'un domaine lorsque le registre requiert un formulaire de modification de la propriété du domaine.

.com.ar

Vous devez remplir et envoyer un formulaire au AWS Support. Consultez Modification du propriétaire d'un domaine lorsque le registre requiert un formulaire de modification de la propriété du domaine.

.com.br

Vous devez remplir et envoyer un formulaire au AWS Support. Consultez Modification du propriétaire d'un domaine lorsque le registre requiert un formulaire de modification de la propriété du domaine.

.es

Vous devez remplir et envoyer un formulaire au AWS Support. Consultez Modification du propriétaire d'un domaine lorsque le registre requiert un formulaire de modification de la propriété du domaine.

.fi

Initier le changement de propriétaire sur la console Route 53. Une fois que vous aurez initié le changement, vous recevrez une clé de transfert du titulaire de l'adresse e-mail fi-domain-tech@traficom .fi. Après avoir reçu la clé, ouvrez un dossier d' AWS assistance auprès du Support et partagez le code clé avec nous. Consultez Contacter le AWS Support à propos de problèmes d'enregistrement de domaine.

.qa

Vous devez remplir et envoyer un formulaire au AWS Support. Consultez Modification du propriétaire d'un domaine lorsque le registre requiert un formulaire de modification de la propriété du domaine.

.ru

Vous devez remplir et envoyer un formulaire au AWS Support. Consultez Modification du propriétaire d'un domaine lorsque le registre requiert un formulaire de modification de la propriété du domaine.

.se

Vous devez remplir et envoyer un formulaire au AWS Support. Consultez Modification du propriétaire d'un domaine lorsque le registre requiert un formulaire de modification de la propriété du domaine.

.sh

Vous devez remplir et envoyer un formulaire au AWS Support. Consultez Modification du propriétaire d'un domaine lorsque le registre requiert un formulaire de modification de la propriété du domaine.

Mise à jour des informations de contact pour un domaine

Pour mettre à jour les informations de contact pour un domaine, exécutez la procédure suivante.

Pour mettre à jour les informations de contact pour un domaine

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le panneau de navigation, choisissez Registered domains (Domaines membres).

3. Choisissez le nom du domaine dont vous souhaitez mettre à jour les informations de contact.
4. Dans l'onglet Coordonnées, choisissez Modifier.
5. Si vous n'avez pas accès à l'adresse e-mail du contact du titulaire, effectuez les étapes suivantes. Si vous avez accès à l'adresse e-mail du contact du titulaire, passez à l'étape 6.

   a. Modifiez uniquement l'adresse e-mail du contact inscrit. Ne modifiez aucune autre valeur des contacts pour le domaine. Si vous souhaitez également modifier d'autres valeurs, vous aurez l'occasion de le faire ultérieurement.

      Sélectionnez Enregistrer les modifications.

      Pour vérifier la nouvelle adresse e-mail, nous envoyons un e-mail de vérification à la nouvelle adresse (si nécessaire pour le TLD). Sélectionnez le lien présent dans l'e-mail afin de pouvoir vérifier la nouvelle adresse e-mail. Si une vérification est nécessaire et vous ne vérifiez pas la nouvelle adresse e-mail, Route 53 suspend le domaine comme l'exige la réglementation ICANN.

      Si vous devez renvoyer l'e-mail de vérification, accédez à la page Domaines enregistrés, cliquez sur le bouton radio à côté du nom de domaine que vous avez mis à jour, puis choisissez le nom du domaine que vous mettez à jour. Dans l'alerte Vérifiez votre adresse e-mail pour éviter la suspension du domaine, choisissez Renvoyer un e-mail.

   b. Si vous souhaitez modifier d'autres valeurs pour le titulaire, l'administrateur, le technicien ou les contacts de facturation du domaine, revenez à l'étape 1 et répétez la procédure.
6. Mettez à jour les valeurs applicables. Vous pouvez également choisir Contact inscrit copié pour remplir automatiquement les mêmes informations que celles que vous avez saisies pour le contact inscrit. Pour de plus amples informations, veuillez consulter Valeurs que vous spécifiez lorsque vous enregistrez ou transférez un domaine.

   En fonction du TLD de votre domaine et des valeurs que vous modifiez, la console peut afficher le message suivant :

   « Pour modifier le nom de l'inscrit ou l'organisation, ouvrez un incident. »

   Si ce message s'affiche, ignorez la suite des instructions de cette procédure et consultez Modification du propriétaire d'un domaine lorsque le registre requiert un formulaire de modification de la propriété du domaine pour plus d'informations.
7. Choisissez Enregistrer.

8. Si vous modifiez le propriétaire du domaine, comme décrit dans Qui est le propriétaire d'un domaine ?, nous envoyons un e-mail au contact inscrit pour le domaine. L'e-mail vous demande l'autorisation de modifier le propriétaire.

   Si nous ne recevons pas d'autorisation pour la modification demandée dans un délai de 3 à 15 jours, selon le domaine de premier niveau, nous devons annuler la demande, comme requis par l'ICANN.

   L'e-mail est envoyé à partir de l'une des adresses suivantes.

TLDs	Adresse e-mail qui envoie l'e-mail d'autorisation
.fr	nic@nic.fr
.com.au .net.au	noreply@emailverification.info
Tous les autres	Une des adresses e-mail suivantes : • noreply@registrar.amazon • noreply@domainnameverification.net

9. Si vous rencontrez des problèmes lors de la mise à jour des informations de contact, vous pouvez contacter le AWS Support gratuitement. Pour de plus amples informations, veuillez consulter Contacter le AWS Support à propos de problèmes d'enregistrement de domaine.

Pour plus d'informations sur l'API que vous pouvez utiliser pour mettre à jour les informations de contact, consultez UpdateDomainContact.

Modification du propriétaire d'un domaine lorsque le registre requiert un formulaire de modification de la propriété du domaine

Si le registre de votre domaine exige que vous effectuiez un changement de propriétaire de domaine et que vous soumettiez le formulaire au AWS Support, effectuez la procédure suivante. Pour déterminer si vous devez effectuer cette procédure, consultez les rubriques suivantes :

- Pour déterminer si la valeur que vous modifiez est considérée comme une modification de propriétaire, consultez Qui est le propriétaire d'un domaine ?.
- Pour déterminer si un formulaire de modification de la propriété du domaine est requis pour votre domaine, consultez TLDs qui nécessitent un traitement spécial pour changer de propriétaire.

Pour modifier la propriété d'un domaine lorsque le registre requiert un formulaire de modification de la propriété du domaine

1. Consultez l'introduction de cette rubrique pour déterminer si le registre de votre domaine requiert un traitement particulier pour modifier le propriétaire du domaine. Si tel est le cas, et s'il est nécessaire de remplir un formulaire de modification de la propriété du domaine, suivez cette procédure.

   Si aucun formulaire de modification de la propriété du domaine n'est nécessaire, suivez la procédure décrite dans la rubrique appropriée.
2. Téléchargez le formulaire de modification de la propriété du domaine. Le fichier est compressé dans un fichier .zip.
3. Remplissez le formulaire.
4. Pour le contact inscrit pour le propriétaire du domaine et pour le nouveau propriétaire, obtenez une copie de la preuve d'identité signée (carte d'identité, permis de conduire, passeport ou autre preuve d'identité).

   En outre, si une entité juridique est répertoriée comme l'organisation, collectez les informations suivantes pour le propriétaire du domaine et pour le nouveau propriétaire :

   - Preuve que l'organisation dans laquelle le domaine est enregistré existe.
   - Preuve que les représentants pour le propriétaire et le nouveau propriétaire sont autorisés à agir pour le compte de l'organisation. Ce document doit être un document juridique certifié qui contient le nom de l'organisation et les noms des représentants en tant que responsables signataires (par exemple, PDG, président ou directeur exécutif).

5. Numérisez le formulaire de modification de la propriété du domaine et la preuve requise. Enregistrez les documents numérisés dans un format courant, par exemple un fichier .pdf ou .png.
6. À l'aide du AWS compte sur lequel le domaine est actuellement enregistré, connectez-vous au AWS Support Center.

> **Important**
>
> Vous devez vous connecter à l'aide du compte racine ou d'un utilisateur qui a reçu les autorisations IAM de l'une ou plusieurs des manières suivantes :
>
> - La politique AdministratorAccessgérée est attribuée à l'utilisateur.
> - La politique DomainsFullAccess gérée AmazonRoute53 est attribuée à l'utilisateur.
> - La politique FullAccess gérée AmazonRoute53 est attribuée à l'utilisateur.
>
> Si vous ne vous connectez pas à l'aide du compte racine ou d'un utilisateur qui dispose des autorisations requises, nous ne pouvons pas mettre à jour le propriétaire du domaine. Cette obligation empêche les utilisateurs non autorisés de modifier le propriétaire d'un domaine.

7. Indiquez l’une des valeurs suivantes :

   Regarding

   Acceptez la valeur par défaut du champ Compte et facturation.

   Service

   Acceptez la valeur par défaut de Domains.

   Catégorie

   Acceptez la valeur par défaut du changement de propriétaire.

   Sévérité

   Acceptez la valeur par défaut de Question générale.

   Choisissez Next step: Additional information (Étape suivante : informations supplémentaires)

Sujet

Spécifiez Change the owner of a domain (Modifier le propriétaire d'un domaine).

Description

Saisissez les informations suivantes :

- Domaine dont vous souhaitez modifier le propriétaire
- ID de compte à 12 chiffres du AWS compte sur lequel le domaine est enregistré

Ajouter un attachement

Chargez les documents que vous avez numérisés à l'étape 5.

Contact method

Indiquez une méthode de contact et entrez les valeurs applicables.

8. Sélectionnez Envoyer.

   Un ingénieur du AWS Support passe en revue les informations que vous avez fournies et met à jour les paramètres. L'ingénieur vous contactera une fois la mise à jour finie ou pour obtenir d'autres informations.

Activation ou désactivation de la protection de la confidentialité pour les informations de contact pour un domaine

Lorsque vous enregistrez un domaine auprès d'Amazon Route 53 ou que vous transférez un domaine vers Route 53, nous activons la protection de la confidentialité par défaut pour tous les contacts du domaine. Cela masque généralement la plupart de vos informations de contact pour les requêtes WHOIS et limite le nombre de courriers indésirables que vous recevez. Lorsque vous activez la protection de la confidentialité, vos informations de contact sont remplacées par les informations du bureau d'enregistrement ou par l'expression « REDACTED FOR PRIVACY » (Censuré pour raison de confidentialité) ou « On behalf of <domain name> owner » (Au nom du propriétaire de <nom de domaine>).

Si vous choisissez de désactiver la protection de la vie privée, vous devez la désactiver pour tous les contacts d'un domaine. Si vous désactivez la protection de la vie privée, n'importe qui peut envoyer une requête WHOIS pour le domaine et, pour la plupart des domaines de premier niveau (TLDs), pourra peut-être obtenir toutes les informations de contact que vous avez fournies lors de l'enregistrement ou du transfert du domaine, notamment le nom, l'adresse, le numéro de téléphone et

l'adresse e-mail. La commande WHOIS est largement disponible. Elle est incluse dans de nombreux systèmes d'exploitation et est également disponible en tant qu'application web sur de nombreux sites web.

Si vous transférez un domaine vers un autre bureau d'enregistrement et que la protection de la confidentialité est activée pour les contacts du domaine, l'e-mail de vérification du transfert sera envoyé à partir des adresses identity-protect.org pour les personnes enregistrées TLDs auprès d'Amazon Registrar. Pour déterminer le bureau d'enregistrement pour votre domaine de premier niveau, consultez Identification de votre bureau d'enregistrement.

Les informations que vous pouvez masquer pour les requêtes WHOIS dépendent de deux facteurs principaux :

Du registre du domaine de premier niveau

La plupart des registres TLD masquent automatiquement toutes les informations de contact, d'autres vous permettent de choisir de masquer toutes les informations de contact, de masquer seulement certaines informations ou ne vous autorisent à masquer aucune information.

Lorsque la protection de confidentialité sur un domaine est activée, vos informations de contact sont remplacées par les informations du service de confidentialité ou par l'expression « REDACTED FOR PRIVACY » (Censuré pour raison de confidentialité). Le service de protection de la vie privée applique des fonctionnalités de prévention du spam (rotation et SPF/DKIM/spam analyse des adresses) et, dans la plupart des cas, redirige automatiquement les e-mails passant par ces filtres. Toutefois, il n'est pas conseillé d'envoyer des e-mails critiques à des adresses e-mail protégées, car le mécanisme d'antispam pourrait empêcher leur transfert.

De plus, le choix du mécanisme de protection de la confidentialité à utiliser pour un domaine n'est pas configurable et est sélectionné automatiquement par le système. Les coordonnées de notre service de protection de la confidentialité ne peuvent pas être mises à jour manuellement.

> **Note**
>
> Pour activer ou désactiver la protection de la confidentialité pour certains domaines, vous devez ouvrir une demande de support et demander la protection de la confidentialité. Pour plus d'informations, consultez la section pertinente sous Domaines que vous pouvez enregistrer avec Amazon Route 53 :
>
> - .co.uk (Royaume-Uni)
> - .me.uk (Royaume-Uni)

- .org.uk (Royaume-Uni)
- .link

Du bureau d'enregistrement

Lorsque vous enregistrez un domaine avec Route 53 ou transférez un domaine vers Route 53, le bureau d'enregistrement pour le domaine est Amazon Registrar ou notre partenaire, Gandi. Par défaut, le bureau d'enregistrement Amazon et Gandi masquent des informations différentes :

- Amazon Registrar – Par défaut, toutes vos informations de contact sont masquées. Toutefois, les réglementations pour le registre TLD sont prioritaires.
- Gandi – Par défaut, toutes vos informations de contact sont masquées, à l'exception du nom de l'organisation, s'il en existe un. Toutefois, les réglementations pour le registre TLD sont prioritaires.

  Pour les zones géographiques TLDs qui n'autorisent pas la protection de la vie privée, vos informations personnelles seront marquées comme « expurgées » sur la page de recherche du répertoire Whois du site Web de Gandi. Toutefois, il est possible que vos informations personnelles soient disponibles au niveau du registre des domaines ou sur des sites web WHOIS tiers.

Pour savoir quelle information est masquée pour le TLD de votre domaine, consultez Domaines que vous pouvez enregistrer avec Amazon Route 53.

Lorsque vous souhaitez activer ou désactiver la protection de la confidentialité pour un domaine que vous avez enregistré à l'aide de Route 53, exécutez la procédure suivante.

Pour activer ou désactiver la protection de la confidentialité pour les informations de contact pour un domaine

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le panneau de navigation, choisissez Registered domains (Domaines membres).
3. Choisissez le nom du domaine dont vous souhaitez activer ou désactiver la protection de la confidentialité.
4. Dans la section Coordonnées, choisissez Modifier.

5. Dans la section Protection de la confidentialité, spécifiez si vous souhaitez masquer vos coordonnées. Vous devez définir le même paramètre de confidentialité pour les quatre contacts : administrateur, inscrit, technique et de facturation.

> **Note**
>
> Si la protection de la confidentialité n'est pas prise en charge pour votre TLD, la section Protection de la confidentialité ne s'affiche pas.

6. Sélectionnez Enregistrer les modifications.
7. Si vous rencontrez des problèmes lors de l'activation ou de la désactivation de la protection de la vie privée, vous pouvez contacter le AWS Support gratuitement. Pour de plus amples informations, veuillez consulter Contacter le AWS Support à propos de problèmes d'enregistrement de domaine.

Activation ou désactivation du renouvellement automatique pour un domaine

Lorsque vous souhaitez modifier le paramètre Amazon Route 53 de renouvellement automatique de l'enregistrement pour un domaine peu de temps avant la date d'expiration, ou lorsque vous souhaitez afficher le paramètre actuel de renouvellement automatique, exécutez la procédure suivante.

Notez que vous ne pouvez pas utiliser de AWS crédits pour payer les frais de renouvellement de l'enregistrement d'un domaine.

> **Note**
>
> Assurez-vous de désactiver le renouvellement automatique si vous avez l'intention d'annuler votre AWS compte. Dans le cas contraire, vous continuerez de recevoir des notifications de renouvellement de la part de AWS. Votre domaine ne sera toutefois pas renouvelé, sauf si vous réactivez votre compte.

Pour activer ou désactiver le renouvellement automatique pour un domaine

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.

2. Dans le panneau de navigation, choisissez Registered domains (Domaines membres).
3. Choisissez le nom du domaine que vous souhaitez mettre à jour.
4. Dans la section Détails, dans le menu déroulant Actions, choisissez Activer le renouvellement automatique

   Dans le champ Activer le renouvellement automatique pour <nom domaine> ?, acceptez de payer le tarif annuel, puis choisissez Activer.

   > **Note**
   >
   > Le prix indiqué correspond à la période d'inscription en cours et peut changer. Pour plus d'informations, consultez Tarification Amazon Route 53 pour l'enregistrement de domaine.

5. Pour désactiver le renouvellement automatique, sélectionnez Désactiver le renouvellement automatique dans le menu déroulant Actions.
6. Si vous rencontrez des problèmes lors de l'activation ou de la désactivation du renouvellement automatique, vous pouvez contacter le AWS Support gratuitement. Pour de plus amples informations, veuillez consulter Contacter le AWS Support à propos de problèmes d'enregistrement de domaine.

Verrouillage d'un domaine pour empêcher son transfert non autorisé vers un autre bureau d'enregistrement

Les registres de domaines génériques TLDs et de nombreux registres géographiques vous TLDs permettent de verrouiller un domaine pour empêcher quelqu'un de le transférer vers un autre bureau d'enregistrement sans votre autorisation. Pour déterminer si le registre pour votre domaine vous permet de verrouiller le domaine, consultez Domaines que vous pouvez enregistrer avec Amazon Route 53. Si le verrouillage est pris en charge et que vous souhaitez verrouiller votre domaine, procédez comme suit. Vous pouvez également utiliser la procédure pour désactiver le verrouillage si vous souhaitez transférer un domaine vers un autre bureau d'enregistrement.

Pour verrouiller un domaine afin d'empêcher son transfert non autorisé vers un autre bureau d'enregistrement

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.

2. Dans le panneau de navigation, sélectionnez Registered Domains (Domaines enregistrés).
3. Choisissez le nom du domaine que vous souhaitez mettre à jour.
4. Dans la section Détails, dans le menu déroulant Actions, choisissez Activer le verrouillage du transfert ou Désactiver le verrouillage du transfert, selon que vous souhaitez activer ou désactiver le verrouillage du transfert.

   Vous pouvez accéder à la page Requêtes pour voir l'état d'avancement de votre demande.
5. Si vous rencontrez des problèmes lors du verrouillage d'un domaine, vous pouvez contacter le AWS Support gratuitement. Pour de plus amples informations, veuillez consulter Contacter le AWS Support à propos de problèmes d'enregistrement de domaine.

Dans la recherche WHOIS, ce statut apparaît comme : `clientTransferProhibited`. Certains TLDs peuvent également avoir les statuts suivants :

- `clientUpdateProhibited`
- `clientDeleteProhibited`

Extension de la période d'enregistrement pour un domaine

Lorsque vous enregistrez un domaine avec Amazon Route 53 ou que vous transférez l'enregistrement d'un domaine vers Route 53, nous configurons ce domaine de façon à ce qu'il soit automatiquement renouvelé. La période de renouvellement automatique est généralement d'un an, bien que les registres de certains domaines de premier niveau (TLDs) aient des périodes de renouvellement plus longues.

Remarques :

Période de renouvellement maximale

Tous les codes génériques TLDs et de nombreux codes de pays vous TLDs permettent de prolonger l'enregistrement d'un domaine pour de plus longues périodes, généralement jusqu'à dix ans par tranches d'un an. Pour déterminer si vous pouvez étendre la période d'enregistrement pour votre domaine, consultez Domaines que vous pouvez enregistrer avec Amazon Route 53. Si de plus longues périodes d'enregistrement sont autorisées, exécutez la procédure suivante.

Restrictions relatives au moment où vous pouvez renouveler ou prolonger l'enregistrement d'un domaine

Certains registres TLD imposent des restrictions concernant le moment où vous pouvez renouveler ou étendre l'enregistrement d'un domaine, par exemple, les deux derniers mois avant l'expiration du domaine. Même si le registre permet d'étendre la période d'enregistrement pour un domaine, il peut ne pas permettre l'extension dans un délai défini avant l'expiration du domaine.

> **Note**
>
> Par exemple, si la période de renouvellement maximale autorisée est de 5 ans pour le domaine TLDs que vous utilisez, vous pouvez ajouter des renouvellements annuels à tout moment jusqu'à ce que vous atteigniez la limite de 5 ans. Plus précisément, si vous possédez un domaine dont la validité est actuellement de 2,5 ans, vous ne pouvez le renouveler que pour 2 ans supplémentaires.

AWS crédits

Vous ne pouvez pas utiliser de AWS crédits pour payer les frais de prolongation de la période d'enregistrement d'un domaine.

Pour étendre la période d'enregistrement pour votre domaine

1. Ouvrez la console Route 53 à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le panneau de navigation, sélectionnez Registered Domains (Domaines enregistrés).
3. Choisissez le nom du domaine pour lequel vous voulez étendre la période d'enregistrement.
4. Dans la section Détails, dans le menu déroulant Actions, choisissez Renouveler l'enregistrement de domaine.
5. Dans la boîte de dialogue Renouveler l'enregistrement de domaine, dans le menu déroulant Période de renouvellement, choisissez le nombre d'années pendant lesquelles vous souhaitez prolonger l'enregistrement.

   La liste affiche toutes les options actuelles basées sur la date d'expiration actuelle et la période d'enregistrement maximale autorisée par le registre pour ce domaine. La date d'expiration avec ce nombre d'années est indiquée sous la durée.
6. Choisissez Renouveler l'enregistrement de domaine.

Lorsque nous recevons confirmation du registre que la date d'expiration a été mise à jour, nous vous envoyons un e-mail afin de confirmer que nous avons modifié la date d'expiration.

7. Si vous rencontrez des problèmes lors de la prolongation de la période d'enregistrement d'un domaine, vous pouvez contacter le AWS Support gratuitement. Pour de plus amples informations, veuillez consulter Contacter le AWS Support à propos de problèmes d'enregistrement de domaine.

Mise à jour des serveurs de noms pour utiliser un autre bureau d'enregistrement

Si vous souhaitez transférer la gestion DNS vers un autre bureau d'enregistrement, vous devez mettre à jour les serveurs de noms vers lesquels pointer

Pour mettre à jour les serveurs de noms de votre domaine lorsque vous souhaitez utiliser un autre service DNS

1. Utilisez la procédure fournie par votre service DNS pour obtenir les serveurs de noms pour le domaine.
2. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
3. Dans le panneau de navigation, choisissez Registered domains (Domaines membres).
4. Choisissez le nom du domaine que vous souhaitez configurer pour qu'il utilise un autre service DNS.
5. Dans la section Détails, sous le menu déroulant Actions, sélectionnez Modifier des serveurs de noms.
6. Supprimez les serveurs de noms existants, puis ajoutez les noms des serveurs de noms à ceux que vous avez obtenus de votre service DNS à l'étape 1.
7. Sélectionnez Enregistrer les modifications.
8. (Facultatif) Supprimez la zone hébergée créée automatiquement par Route 53 lorsque vous avez enregistré votre domaine. Cela évite que des frais soient appliqués pour une zone hébergée que vous n'utilisez pas.

   a. Dans le volet de navigation, choisissez Hosted Zones (Zones hébergées).

b. Sélectionnez la case d'option pour la zone hébergée portant le même nom que votre domaine.
c. Choisissez Delete Hosted Zone.
d. Choisissez Confirm pour confirmer que vous souhaitez supprimer la zone hébergée.

Ajout ou modification de serveurs de noms et d'enregistrements de type glue pour un domaine

Lorsque vous enregistrez un domaine avec Route 53, nous créons automatiquement une zone hébergée pour le domaine, attribuons quatre serveurs de noms à la zone hébergée, puis mettons à jour l'enregistrement de domaine pour utiliser les serveurs de noms. En général, vous n'avez pas besoin de changer ces paramètres, sauf si vous souhaitez utiliser un autre service DNS ou si vous souhaitez utiliser des serveurs de noms en marque blanche.

Le nombre maximal de serveurs de noms par domaine dans Route 53 s'élève à 6.

> **Warning**
>
> Si vous indiquez des valeurs incorrectes pour les serveurs de noms, des adresses IP incorrectes dans les enregistrements de type glue ou supprimez un ou plusieurs serveurs de noms sans en spécifier de nouveaux, votre site web ou votre application peut devenir indisponible sur Internet pendant un maximum de deux jours.

Rubriques

- Éléments à prendre en compte pour modifier les serveurs de noms et les enregistrements de type glue
- Ajout ou modification de serveurs de noms ou d'enregistrements de type glue

Éléments à prendre en compte pour modifier les serveurs de noms et les enregistrements de type glue

Prenez en compte les problèmes suivants avant de modifier votre configuration.

Rubriques

- 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

Vous souhaitez faire de Route 53 le service DNS pour votre domaine

Si vous utilisez actuellement un autre service DNS et que vous souhaitez faire de Route 53 le service DNS pour votre domaine, consultez Configuration d'Amazon Route 53 en tant que service DNS d'un domaine existant pour obtenir des instructions détaillées sur la façon de procéder à la migration du service DNS vers Route 53.

> **Important**
>
> Si vous ne suivez pas rigoureusement le processus de migration, votre domaine peut devenir indisponible sur Internet pendant un maximum de deux jours.

Vous souhaitez utiliser un autre service DNS

Si vous souhaitez utiliser un service DNS autre que Route 53 pour votre domaine, utilisez la procédure suivante pour modifier les serveurs de noms pour l'enregistrement de domaine vers les serveurs de noms qui sont fournis par l'autre service DNS.

> **Note**
>
> Si vous modifiez les serveurs de noms et que Route 53 renvoie le message d'erreur suivant, le registre de domaine de premier niveau (TLD) ne reconnaît pas les serveurs de noms que vous avez spécifié en tant que serveurs de noms valides :
> `"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."`
> Les registres TLD prennent généralement en charge les serveurs de noms fournis par les services DNS publics, mais pas les serveurs DNS privés, tels que les serveurs DNS que vous avez configurés sur des EC2 instances Amazon, sauf si le registre possède des adresses IP pour ces serveurs de noms. Route 53 ne prend pas en charge l'utilisation de serveurs de noms qui ne sont pas reconnus par le registre de domaine de premier niveau

(TLD). Si vous rencontrez cette erreur, vous devez modifier les serveurs de noms pour Route 53 ou un autre service DNS public.

Vous souhaitez utiliser des serveurs de noms en marque blanche

Si vous voulez que les noms de vos serveurs de noms soient des sous-domaines de votre nom de domaine, vous pouvez créer des serveurs de noms en marque blanche. (Les serveurs de noms en marque blanche sont aussi appelés serveurs de noms personnels ou serveurs de noms privés.) Par exemple, vous pouvez créer des serveurs de noms ns1.example.com via ns4.example.com pour le domaine example.com. Pour utiliser des serveurs de noms en marque blanche, utilisez la procédure suivante pour spécifier les adresses IP de vos serveurs de noms au lieu des noms. Ces adresses IP sont appelées enregistrements de type glue.

Pour plus d'informations sur la configuration des serveurs de noms en marque blanche, consultez Configuration de serveurs de noms en marque blanche.

Vous modifiez les serveurs de noms pour un domaine .it

IName les serveurs de votre domaine informatique doivent passer une vérification DNS. Nous vous suggérons de vérifier les serveurs de noms sur https://dns-check.nic.it/ avant de soumettre la demande de modification. Le registre continue de répondre aux requêtes DNS en utilisant les serveurs de noms antérieurs à la modification. Si les serveurs de noms antérieurs ne sont plus disponibles, votre domaine devient indisponible sur Internet.

> **Important**
>
> À chaque modification des serveurs de noms pour un domaine, vérifiez que DNS répond bien aux requêtes avec les nouveaux serveurs de noms avant d'annuler l'ancien service DNS ou de supprimer la zone hébergée Route 53 qui utilise les anciens serveurs de noms.

Pour savoir comment obtenir de l'aide AWS pour corriger les noms de vos serveurs de noms dans le registre des domaines .it, consultezContacter le AWS Support à propos de problèmes d'enregistrement de domaine.

Ajout ou modification de serveurs de noms ou d'enregistrements de type glue

Pour ajouter ou de modifier des serveurs de noms ou des enregistrements de type glue, exécutez la procédure suivante :

> **Note**
>
> Par défaut, les résolveurs DNS mettent généralement en cache les noms des serveurs de noms pendant deux jours. Par conséquent, vos modifications peuvent prendre deux jours pour entrer en vigueur. Pour de plus amples informations, veuillez consulter Comment Amazon Route 53 achemine le trafic de votre domaine.

Pour ajouter ou modifier des serveurs de noms ou des enregistrements de type glue pour un domaine

1. Vérifiez Éléments à prendre en compte pour modifier les serveurs de noms et les enregistrements de type glue et résolvez les problèmes applicables, le cas échéant.
2. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
3. Dans le panneau de navigation, choisissez Registered domains (Domaines membres).
4. Choisissez le nom du domaine dont vous souhaitez modifier les paramètres.
5. Dans la section Détails, dans le menu déroulant Actions, sélectionnez Modifier des serveurs de noms.
6. Dans la boîte de dialogue Modifier des serveurs de noms, vous pouvez procéder comme suit :

   - Modifiez le service DNS pour le domaine en effectuant l'une des opérations suivantes :
     - Remplacez les serveurs de noms d'un autre service DNS par les serveurs de noms d'une zone hébergée Route 53
     - Remplacez les serveurs de noms d'une zone hébergée Route 53 par les serveurs de noms d'un autre service DNS
     - Remplacez les serveurs de noms d'une zone hébergée Route 53 par les serveurs de noms d'une zone hébergée Route 53 différente

   Pour plus d'informations sur la modification du service DNS pour un domaine, consultez Configuration d'Amazon Route 53 en tant que service DNS d'un domaine existant. Pour plus d'informations sur la façon d'obtenir des serveurs de noms pour la zone hébergée Route 53

que vous souhaitez utiliser pour le service DNS pour le domaine, consultez Obtention de la liste des serveurs de noms d'une zone hébergée publique.

- Ajoutez un ou plusieurs serveurs de noms.
- Remplacez le nom d'un serveur de noms existant.
- Si vous spécifiez des serveurs de noms en marque blanche, ajoutez ou modifiez les adresses IP dans les enregistrements de type glue. Vous pouvez saisir les adresses au IPv6 format IPv4 or. Si un serveur de noms a plusieurs adresses IP, entrez chaque adresse sur une ligne distincte.

  Un serveur de noms en marque blanche inclut votre nom de domaine, comme example.com, dans le nom du serveur de noms, comme ns1.example.com. Lorsque vous spécifiez un serveur de noms en marque blanche, Route 53 vous invite à spécifier une ou plusieurs adresses IP pour le serveur de noms. L'adresse IP est qualifiée de glue record. Pour de plus amples informations, veuillez consulter Configuration de serveurs de noms en marque blanche.
- Supprimez un serveur de noms. Choisissez l'icône x à droite du champ de ce serveur de noms.

> **Warning**
>
> Si vous indiquez des valeurs incorrectes pour les serveurs de noms, des adresses IP incorrectes dans les enregistrements de type glue ou supprimez un ou plusieurs serveurs de noms sans en spécifier de nouveaux, votre site web ou votre application peut devenir indisponible sur Internet pendant un maximum de deux jours.

7. Choisissez Mettre à jour.
8. Si vous rencontrez des problèmes lors de l'ajout ou de la modification de serveurs de noms ou d'enregistrements collés, vous pouvez contacter le AWS Support gratuitement. Pour de plus amples informations, veuillez consulter Contacter le AWS Support à propos de problèmes d'enregistrement de domaine.

Renouvellement d'un enregistrement de domaine

Lorsque vous enregistrez un domaine avec Amazon Route 53 ou que vous transférez l'enregistrement d'un domaine vers Route 53, nous configurons ce domaine de façon à ce qu'il soit

automatiquement renouvelé. La période de renouvellement automatique est généralement d'un an, bien que les registres de certains domaines de premier niveau (TLDs) aient des périodes de renouvellement plus longues. Pour consulter la période d'enregistrement et de renouvellement pour votre domaine de premier niveau, consultez Domaines que vous pouvez enregistrer avec Amazon Route 53.

> **Note**
>
> Vous ne pouvez pas utiliser de AWS crédits pour payer les frais de renouvellement de l'enregistrement d'un domaine.

Pour la plupart des domaines de premier niveau (TLDs), vous pouvez modifier la date d'expiration d'un domaine. Pour de plus amples informations, veuillez consulter Extension de la période d'enregistrement pour un domaine.

> **Important**
>
> Si vous désactivez le renouvellement automatique, vous devez être informé des effets suivants sur votre domaine :
>
> - Certains registres TLD suppriment les domaines avant la date d'expiration si vous ne renouvelez pas les domaines assez tôt. Nous vous recommandons vivement de laisser le renouvellement automatique activé si vous souhaitez conserver un nom de domaine.
> - Nous vous recommandons également vivement de ne pas prévoir de réenregistrer un domaine après expiration. Certains bureaux d'enregistrement autorisent des tiers à enregistrer des domaines immédiatement après l'expiration d'un domaine. Vous ne pourrez ainsi peut-être pas réenregistrer le domaine avant qu'il ne soit pris par une autre personne.
> - Certains registres appliquent des frais importants pour restaurer des domaines ayant expiré.
> - A la date d'expiration, ou à une date proche de ce jour, le domaine devient non disponible sur Internet.

Pour déterminer si le renouvellement automatique est activé pour votre domaine, consultez Activation ou désactivation du renouvellement automatique pour un domaine.

Si le renouvellement automatique est activé, voici ce qui se produit :

45 jours avant l'expiration

Nous envoyons un e-mail au contact inscrit pour indiquer que le renouvellement automatique est actuellement activé et donner des instructions pour le désactiver. Veillez à mettre à jour l'adresse e-mail de votre contact inscrit afin de ne pas manquer cet e-mail.

35 ou 30 jours avant l'expiration

Pour tous les domaines à l'exception des domaines .com.ar,. com.br et .jp, nous renouvelons l'enregistrement de domaine 35 jours avant la date d'expiration, ce qui nous laisse le temps de résoudre les éventuels problèmes relatifs à votre renouvellement avant l'expiration du nom de domaine.

Les registres pour les domaines .com.ar, .com.br et .jp nécessitent de renouveler les domaines au maximum 30 jours avant l'expiration. Vous recevez un e-mail de renouvellement de Gandi, notre partenaire, 30 jours avant l'expiration. C'est également ce jour-là que nous renouvelons votre domaine si vous avez activé le renouvellement automatique.

> **Note**
>
> Lorsque nous renouvelons votre domaine, nous vous envoyons un e-mail pour vous en informer. Si le renouvellement a échoué, nous vous envoyons un e-mail pour en expliquer la raison.

Si le renouvellement automatique est désactivé, voici ce qui se passe à l'approche de la date d'expiration d'un nom de domaine :

45 jours avant l'expiration

Nous envoyons un e-mail au contact inscrit pour le domaine pour indiquer que le renouvellement automatique est actuellement désactivé et donner les instructions pour l'activer. Veillez à mettre à jour l'adresse e-mail de votre contact inscrit afin de ne pas manquer cet e-mail.

30 jours et 7 jours avant l'expiration

Si le renouvellement automatique est désactivé pour le domaine, l'ICANN, l'organisme de réglementation pour l'enregistrement de domaine, exige l'envoi d'e-mail par le bureau d'enregistrement. L'e-mail est envoyé à partir de l'une des adresses suivantes :

- noreply@registrar.amazon — Pour les domaines pour lesquels le bureau d'enregistrement est Amazon Registrar.

- noreply@domainnameverification.net – Pour les domaines dont le bureau d'enregistrement est notre partenaire Gandi.

Pour déterminer le bureau d'enregistrement pour votre domaine de premier niveau, consultez Domaines que vous pouvez enregistrer avec Amazon Route 53.

Si vous activez le renouvellement automatique moins de 30 jours avant l'expiration et si la période de renouvellement n'est pas terminée, nous renouvelons le domaine dans les 24 heures.

> **Important**
>
> Certains registres TLD imposent des restrictions quant au moment où vous pouvez renouveler un domaine. Pour obtenir des informations spécifiques à votre domaine, consultezDomaines que vous pouvez enregistrer avec Amazon Route 53. Une journée peut être nécessaire pour le traitement d'un renouvellement. Si vous n'activez pas le renouvellement automatique à temps, le domaine peut expirer avant que le renouvellement puisse être traité et vous risquez de perdre le domaine. Si la date d'expiration approche, nous vous recommandons d'étendre manuellement la date d'expiration pour le domaine. Pour de plus amples informations, veuillez consulter Extension de la période d'enregistrement pour un domaine.

Pour plus d'informations sur les périodes de renouvellement, consultez la section Délais pour le renouvellement et la restauration de domaines pour votre TLD dans Domaines que vous pouvez enregistrer avec Amazon Route 53.

Après la date d'expiration

La plupart des domaines sont conservés par le bureau d'enregistrement après expiration pendant une durée très courte. Il est donc possible de renouveler un domaine après la date d'expiration, mais si vous souhaitez conserver un domaine, nous vous recommandons vivement d'activer le renouvellement automatique. Pour plus d'informations sur le renouvellement d'un domaine après la date d'expiration, consultez Restauration d'un domaine arrivé à expiration ou supprimé.

Si votre domaine expire, mais que le renouvellement tardif est autorisé pour le domaine, vous pouvez renouveler le domaine au prix de renouvellement standard. Pour déterminer si la période de renouvellement tardif est en cours pour le domaine, effectuez la procédure décrite dans la section Extension de la période d'enregistrement pour un domaine. Si le domaine est toujours répertorié, sa période de renouvellement tardif est en cours.

Pour plus d'informations sur les périodes de renouvellement, consultez la section Délais pour le renouvellement et la restauration de domaines pour votre TLD dans Domaines que vous pouvez enregistrer avec Amazon Route 53.

Restauration d'un domaine arrivé à expiration ou supprimé

Si vous ne renouvelez pas un domaine avant la fin de la période de renouvellement tardif ou si vous le supprimez accidentellement, pour certains registres de domaines de premier niveau (TLDs), vous pouvez restaurer le domaine avant qu'il ne soit disponible pour que d'autres puissent l'enregistrer.

Lorsqu'un domaine est supprimé ou qu'il dépasse la fin de la période de renouvellement tardif, il n'apparaît plus dans la console Amazon Route 53.

> **Important**
>
> Le tarif de restauration d'un domaine est généralement supérieur et parfois beaucoup plus élevé que le tarif d'enregistrement ou de renouvellement d'un domaine. Pour connaître le prix actuel de restauration d'un domaine, consultez la colonne Tarification de restauration dans Tarification Amazon Route 53 pour l'enregistrement de domaine.

Vous ne pouvez pas utiliser de AWS crédits pour payer les frais de restauration d'un domaine expiré.

Pour tenter de restaurer l'enregistrement de domaine lorsqu'un domaine est supprimé ou que la période de renouvellement tardif a expiré

1. Déterminez si le registre TLD pour le domaine prend en charge la restauration des domaines et, si c'est le cas, la période pendant laquelle la restauration est autorisée.

   a. Accédez à Domaines que vous pouvez enregistrer avec Amazon Route 53.

   > **Important**
   >
   > Pour les domaines TLD génériques supprimés dans les 5 premiers jours suivant l'enregistrement, la période de remboursement standard de 30 jours (pour vérifier le nombre de jours réel de la période de remboursement, voirDomaines que vous pouvez enregistrer avec Amazon Route 53) ne s'applique pas. Au lieu de cela, ces domaines sont immédiatement disponibles pour un nouvel enregistrement.

b. Recherchez le TLD pour votre domaine et vérifiez les valeurs dans la section Délais pour le renouvellement et la restauration de domaines.

> **Important**
>
> Nous transmettons les demandes de restauration à notre partenaire Gandi, qui traite les demandes du lundi au vendredi, pendant les heures ouvrables. Gandi est basé à Paris, où le temps est de UTC/GMT +1 heure. Par conséquent, en fonction du moment où vous soumettez votre demande, le traitement de la demande peut nécessiter un délai d'une semaine ou plus.

2. Vérifiez le prix pour la restauration d'un domaine, qui est généralement supérieur voire très supérieur au tarif d'enregistrement ou de renouvellement d'un domaine. Dans Tarification d'Amazon Route 53 pour l'enregistrement de domaine, recherchez le TLD de votre domaine (tel que .com) et vérifiez le prix dans la colonne Tarification de restauration. Si vous souhaitez toujours restaurer le domaine, notez le prix ; vous en aurez besoin dans une étape ultérieure.
3. À l'aide du AWS compte sur lequel le domaine a été enregistré, connectez-vous au AWS Support Center.
4. Indiquez l'une des valeurs suivantes :

   Regarding

   Acceptez la valeur par défaut du champ Compte et facturation.

   Service

   Acceptez la valeur par défaut de Domains.

   Catégorie

   Acceptez la valeur par défaut de Restoration.

   Sévérité

   Acceptez la valeur par défaut de Question générale.

   Choisissez Next step: Additional information (Étape suivante : informations supplémentaires)

Sujet

Entrez Restore an expired domain (Restaurer un domaine expiré) ou Restore a deleted domain (Restaurer un domaine supprimé).

Description

Saisissez les informations suivantes :

- Domaine que vous voulez restaurer
- L'identifiant de compte à 12 chiffres du AWS compte sur lequel le domaine a été enregistré
- Confirmation que vous acceptez le prix pour restaurer le domaine. Utilisez le texte suivant :

  "J'accepte le prix de ____ $ pour la restauration de mon domaine."

  Dans la zone laissée vide, indiquez le prix que vous avez trouvé à l'étape 2.

Contact method

Indiquez une méthode de contact et entrez les valeurs applicables.

5. Sélectionnez Envoyer.
6. Lorsque nous saurons si nous avons pu restaurer votre domaine, un représentant du AWS Support vous contactera. En outre, si nous avons réussi à restaurer votre domaine, celui-ci s'affiche de nouveau dans la console. La date d'expiration varie selon que le domaine a expiré ou qu'il a été accidentellement supprimé :

   Le domaine a expiré

   La nouvelle date d'expiration se situe généralement un ou deux ans (selon le TLD) après l'ancienne date d'expiration.

   > **Note**
   >
   > La nouvelle date d'expiration n'est pas calculée à partir de la date à laquelle le domaine a été restauré.

   Le domaine a été accidentellement supprimé

   La date d'expiration ne change généralement pas.

Remplacement de la zone hébergée d'un domaine enregistré auprès de Route 53

Si vous supprimez la zone hébergée d'un domaine, vous devez en créer une autre dès que vous êtes prêt à rendre le domaine disponible sur Internet. Utilisez la procédure suivante.

Pour remplacer la zone hébergée d'un domaine

1. Créez une zone hébergée publique. Pour de plus amples informations, veuillez consulter Création d'une zone hébergée publique.
2. Créez des enregistrements dans la zone hébergée. Les enregistrements définissent la façon dont vous voulez acheminer le trafic pour le domaine (example.com) et les sous-domaines (apex.example.com, zenith.example.com). Pour de plus amples informations, veuillez consulter Utilisation des enregistrements.
3. Mettez à jour la configuration du domaine pour utiliser les serveurs de noms de la nouvelle zone hébergée. Pour de plus amples informations, veuillez consulter Ajout ou modification de serveurs de noms et d'enregistrements de type glue pour un domaine.

   > **Important**
   >
   > Lorsque vous créez une zone hébergée, Route 53 attribue un jeu de quatre serveurs de noms à la zone hébergée. Si vous supprimez une zone hébergée et en créez une, Route 53 attribue un autre jeu de quatre serveurs de noms. En règle générale, aucun des serveurs de noms de la nouvelle zone hébergée ne correspond à l'un des serveurs de noms de la zone hébergée précédente. Si vous ne mettez pas à jour la configuration du domaine pour utiliser les serveurs de noms de la nouvelle zone hébergée, le domaine reste indisponible sur Internet.

4. Si vous rencontrez des problèmes lors du remplacement de la zone hébergée d'un domaine, vous pouvez contacter le AWS Support gratuitement. Pour de plus amples informations, veuillez consulter Contacter le AWS Support à propos de problèmes d'enregistrement de domaine.

Transfert de domaines

Vous pouvez transférer un enregistrement de domaine d'un autre serveur d'inscriptions (registrar) vers Amazon Route 53, d'un compte AWS à un autre ou de Route 53 à un autre serveur d'inscriptions. Le transfert de domaines d'un AWS compte à un autre est gratuit.

Les rubriques de cette section couvrent les sujets suivants relatifs au transfert de domaines :

1. Transfert d'un enregistrement de domaine vers Amazon Route 53
   - Découvrez la step-by-step procédure de transfert d'un domaine d'un autre bureau d'enregistrement vers Route 53, notamment les conditions requises, les codes d'autorisation et la mise à jour des paramètres DNS.
   - Découvrez comment le transfert d'un domaine affecte la date d'expiration et les considérations relatives aux différents domaines de premier niveau (TLDs).
2. Affichage du statut du transfert d'un domaine
   - Découvrez comment consulter le statut d'une demande de transfert de domaine et la signification des différents codes de statut au cours du processus de transfert.
3. Incidence du transfert d'un domaine vers Amazon Route 53 sur la date d'expiration de l'enregistrement de votre domaine
   - Découvrez comment le transfert d'un domaine vers Route 53 peut affecter la date d'expiration du domaine.
4. Transférer un domaine vers un autre AWS compte
   - Découvrez comment transférer un domaine d'un AWS compte à un autre, y compris les rôles et les autorisations requis pour initier et accepter le transfert.
   - Découvrez l'étape facultative de migration de la zone hébergée vers le nouveau compte après le transfert de domaine.
5. Transfert d'un domaine depuis Amazon Route 53 vers un autre bureau d'enregistrement
   - Découvrez le processus de transfert d'un domaine de Route 53 vers un autre bureau d'enregistrement, notamment l'obtention du code d'autorisation, la mise à jour des paramètres DNS et la réponse aux e-mails de confirmation.
   - Tenez compte des facteurs à prendre en compte lors du transfert du service DNS vers un autre fournisseur et de l'impact potentiel sur les fonctionnalités spécifiques de Route 53, telles que les enregistrements d'alias et les politiques de routage.

En suivant les informations fournies dans les rubriques répertoriées ci-dessus, vous pouvez transférer efficacement des domaines vers et depuis Route 53, gérer le processus de transfert et assurer une transition fluide tout en conservant une configuration et un routage DNS appropriés.

Transfert d'un enregistrement de domaine vers Amazon Route 53

> **Important**
>
> Lors du transfert de tout domaine de premier niveau (ccTLDs) de code de pays vers Route 53, à l'exception des domaines .cc et .tv, les mises à jour du contact du propriétaire sont ignorées et les coordonnées du propriétaire figurant dans le registre sont utilisées. Une fois le transfert terminé, vous pouvez mettre à jour les coordonnées du propriétaire. Pour de plus amples informations, veuillez consulter Mise à jour des informations de contact et de la propriété pour un domaine.

Pour transférer l'enregistrement d'un domaine vers Amazon Route 53, suivez les procédures décrites dans cette rubrique.

> **Important**
>
> Si vous sautez une étape, votre nom de domaine risque d'être indisponible sur Internet.

Remarques :

Contacter le AWS Support

Si vous rencontrez des problèmes lors du transfert d'un domaine, vous pouvez contacter le AWS Support gratuitement. Pour de plus amples informations, veuillez consulter Contacter le AWS Support à propos de problèmes d'enregistrement de domaine.

Date d’expiration

Pour plus d'informations sur l'impact du transfert de votre domaine sur la date d'expiration actuelle, consultez Incidence du transfert d'un domaine vers Amazon Route 53 sur la date d'expiration de l'enregistrement de votre domaine.

Frais de transfert

Lorsque vous transférez un domaine vers Route 53, les frais de transfert que nous appliquons à votre AWS compte dépendent du domaine de premier niveau, tel que .com ou .org. Pour en savoir plus, consultez Tarification Route 53.

Vous ne pouvez pas utiliser de AWS crédits pour payer les frais éventuels de transfert d'un domaine vers Route 53.

> **Note**
>
> Route 53 facture les frais de transfert de votre domaine avant le début du processus de transfert. Si un transfert échoue pour une raison quelconque, nous créditerons immédiatement sur votre compte le coût du transfert.

Noms de domaine spéciaux et premium

Les registres TLD ont attribué des tarifs spéciaux ou premium à certains noms de domaine. Vous ne pouvez pas transférer vers Route 53 un domaine qui dispose d'un tarif spécial ou premium.

Quotas de domaines

Le nombre maximum de domaines par AWS compte par défaut est de 20. Vous pouvez demander un quota plus élevé. Pour de plus amples informations, veuillez consulter Quotas applicables aux domaines.

Limite des serveurs de noms

Le nombre maximal de serveurs de noms par domaine dans Route 53 s'élève à 6.

Rubriques

- Exigences liées au transfert de domaines de premier niveau
- Étape 1 : confirmer qu'Amazon Route 53 prend en charge le domaine de premier niveau
- Étape 2 (facultative) : transférer votre service DNS vers Amazon Route 53 ou vers un autre fournisseur de services DNS
- Étape 3 : Modifier les paramètres avec le bureau d'enregistrement actuel
- Étape 4 : Obtenir les noms de vos serveurs de noms

- Étape 5 : Demander le transfert
- Étape 6 : cliquez sur le lien dans les e-mails de confirmation et d'autorisation
- Étape 7 : mise à jour de la configuration du domaine

Exigences liées au transfert de domaines de premier niveau

La plupart des bureaux d'enregistrement de domaine imposent des exigences pour le transfert d'un domaine vers un autre bureau d'enregistrement. Ces exigences servent principalement à empêcher les propriétaires de domaines frauduleux de transférer de façon répétée les domaines vers différents bureaux d'enregistrement. Ces exigences varient, à l'exception des exigences classiques suivantes :

- Vous devez avoir enregistré le domaine avec le bureau d'enregistrement actuel ou transféré l'enregistrement pour le domaine vers le bureau d'enregistrement actuel au moins 60 jours auparavant.
- Si l'enregistrement d'un nom de domaine a expiré et a dû être restauré, la restauration a dû avoir lieu au moins 60 jours auparavant.
- Le code de statut du domaine ne peut pas être l'un des codes suivants :
  - clientTransferProhibited
  - pendingDelete
  - pendingTransfer
  - redemptionPeriod
  - serverTransferProhibited
- Les registres de certains domaines de premier niveau n'autorisent pas les transferts tant que les modifications ne sont pas terminées, comme les modifications de propriétaire de domaine.

Pour obtenir une liste actuelle des codes de statut de noms de domaines et une explication de chaque code, accédez au site web de l'ICANN, puis recherchez codes de statut EPP. (Effectuez une recherche sur le site web de l'ICANN. Les recherches sur Internet renvoient parfois une ancienne version du document.)

> **Note**
>
> L'ICANN est l'organisation qui établit des stratégies régissant l'enregistrement et le transfert de noms de domaine.

Vous pouvez également rechercher votre nom de domaine sur le site web Whois, afin d'afficher les codes d'état et d'autres informations pour votre domaine.

Étape 1 : confirmer qu'Amazon Route 53 prend en charge le domaine de premier niveau

Consultez Domaines que vous pouvez enregistrer avec Amazon Route 53. Si le domaine de premier niveau du domaine que vous souhaitez transférer figure sur la liste, vous pouvez transférer le domaine vers Amazon Route 53.

Si un TLD ne figure pas sur la liste, vous ne pouvez pas actuellement transférer l'enregistrement de domaine vers Route 53. Nous ajoutons parfois d'autres éléments TLDs à la liste, alors revenez voir si nous avons ajouté la prise en charge de votre domaine.

Étape 2 (facultative) : transférer votre service DNS vers Amazon Route 53 ou vers un autre fournisseur de services DNS

Pourquoi transférer le service DNS en premier ?

Certains bureaux d'enregistrement fournissent un service DNS gratuit qui peut être désactivé dès qu'ils reçoivent une demande de Route 53 destinée à transférer l'enregistrement du domaine. Si vous souhaitez que Route 53 fournisse un service DNS pour votre domaine, consultez Configuration d'Amazon Route 53 en tant que service DNS d'un domaine existant.

Étape 3 : Modifier les paramètres avec le bureau d'enregistrement actuel

À l'aide de la méthode fournie par votre bureau d'enregistrement actuel, exécutez les tâches suivantes pour chaque domaine que vous souhaitez transférer.

- 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)

Vérifiez que l'e-mail du contact inscrit de votre domaine est à jour

Nous allons envoyer un e-mail à cette adresse e-mail pour demander l'autorisation de transfert. Vous devez cliquer sur un lien figurant dans l'e-mail afin d'autoriser le transfert. Si vous ne cliquez pas sur le lien, nous devons annuler le transfert.

> **Important**
>
> Le contact que vous indiquez en tant que titulaire aura certains droits en tant que titulaire du nom de domaine enregistré, conformément à la politique de transfert de l'ICANN. La plupart des domaines seront supprimés lors de la fermeture de votre compte Compte AWS (pour plus d'informations, voirMon AWS compte est fermé ou définitivement, et mon domaine est enregistré auprès de Route 53), mais si un domaine reste sur un compte fermé, le contact que vous avez indiqué comme titulaire peut être en mesure de demander le transfert du nom de domaine vers un bureau d'enregistrement externe. Par conséquent, il est important que le titulaire de votre liste de contacts soit vous-même ou une autre personne en qui vous avez confiance pour agir de manière responsable.

Déverrouillez le domaine afin qu'il puisse être transféré

ICANN, l'organisme de réglementation pour les enregistrements de domaine, nécessite que votre domaine soit déverrouillé avant d'être transféré.

Vérifiez que le statut du domaine vous permet de transférer le domaine

Pour de plus amples informations, veuillez consulter Exigences liées au transfert de domaines de premier niveau.

Désactiver le protocole DNSSEC pour le domaine

Si vous utilisez le protocole DNSSEC avec un domaine et que vous transférez l'enregistrement de domaine vers Route 53, vous devez d'abord désactiver le protocole DNSSEC dans l'ancien bureau d'enregistrement. Ensuite, après avoir transféré l'enregistrement de domaine, suivez les étapes afin de configurer le protocole DNSSEC pour le domaine dans Route 53. Route 53 prend en charge le protocole DNSSEC pour l'enregistrement de domaine et pour la signature DNSSEC. Pour de plus amples informations, veuillez consulter Configuration de la signature DNSSEC dans Amazon Route 53.

> **Important**
>
> Si vous transférez un enregistrement de domaine vers Route 53 alors que le protocole DNSSEC est configuré, les clés publiques DNSSEC sont également transférées. Si vous transférez un service DNS vers un autre fournisseur qui ne prend pas en charge le protocole DNSSEC, la résolution DNS échoue par intermittence jusqu'à ce que vous supprimiez les clés DNSSEC du domaine. Pour de plus amples informations, veuillez consulter Suppression de clés publiques pour un domaine.

Obtenir un code d'autorisation

Un code d'autorisation, provenant du bureau d'enregistrement actuel, nous autorise à demander le transfert de l'enregistrement du domaine vers Route 53. Ce code sera saisi ultérieurement dans la console Route 53.

Certains domaines de premier niveau ont des obligations supplémentaires :

Domaines .co.za

Vous n'avez pas besoin de code d'autorisation pour transférer un domaine .co.za domaine vers Route 53.

Domaines .uk, .co.uk, .me.uk et .org.uk

Si vous transférez un domaine .uk, .co.uk, .me.uk ou .org.uk vers Route 53, vous n'avez pas besoin de code d'autorisation. Au lieu de cela, utilisez la méthode fournie par votre bureau d'enregistrement de domaine actuel pour remplacer la valeur de la balise IPS pour le domaine par GANDI, écrit en majuscules. (Nominet, le registre des noms de domaine .uk, requiert une balise IPS). Si votre bureau d'enregistrement ne permet pas de modifier la valeur de la balise IPS, contactez Nominet.

Notez ce qui suit à propos de la modification de la balise IPS :

Vous devez demander le transfert dans les cinq jours

Si vous ne demandez pas le transfert dans les cinq jours suivant la modification de la balise IPS, la balise reprend sa valeur précédente. Vous devez modifier à nouveau la valeur de la balise IPS, sinon la demande de transfert échouera.

Affichage de la balise IPS dans les requêtes WHOIS

La modification apportée à la balise IPS n'apparaît pas dans les requêtes WHOIS tant que le transfert vers Route 53 n'est pas terminé.

E-mail de Gandi

Vous pouvez recevoir un e-mail de notre bureau d'enregistrement partenaire, Gandi, concernant le processus de transfert. Si vous recevez un e-mail de Gandi (transfer-auth@gandi.net) concernant le transfert de votre domaine, ignorez les instructions contenues dans l'e-mail car elles ne concernent pas les domaines .uk, .co.uk, .me.uk ou .org.uk. Suivez plutôt les instructions de cette rubrique.

Renouvelez l'enregistrement de votre domaine avant de le transférer (zone géographique sélectionnée TLDs)

Dans la plupart des cas TLDs, lorsque vous transférez un domaine, l'enregistrement est automatiquement prolongé d'un an. Toutefois, pour certaines zones géographiques TLDs, l'enregistrement n'est pas prolongé lorsque vous transférez le domaine. Si vous transférez un domaine vers Route 53 doté de l'une de ces TLDs options, nous vous recommandons de renouveler l'enregistrement du domaine avant de le transférer, en particulier si la date d'expiration approche.

> **Important**
>
> Si vous ne renouvelez pas le domaine avant de le transférer, l'enregistrement pourrait expirer avant que le transfert ne soit terminé. Dans cette situation, le domaine devient indisponible sur Internet, et le nom de domaine peut alors être acheté par d'autres personnes.

L'enregistrement n'est pas prolongé automatiquement lorsque vous transférez les domaines suivants vers un autre bureau d'enregistrement :

- .ch (Suisse)
- .cl (Chili)
- .co.uk (Royaume-Uni)
- .co.za (Afrique du Sud)
- .com.au (Australie)

- .cz (République tchèque)
- .es (Espagne)
- .fi (Finlande)
- .im (Ile de Man)
- .jp (Japon)
- .me.uk (Royaume-Uni)
- .net.au (Australie)
- .org.uk (Royaume-Uni)
- .se (Suède)
- .uk (Royaume-Uni)

Étape 4 : Obtenir les noms de vos serveurs de noms

Si vous utilisez déjà Amazon Route 53 comme service DNS ou si vous continuez à utiliser le service DNS existant, nous obtiendrons les noms des serveurs de noms automatiquement pour vous ultérieurement lors du processus. Passez à Étape 5 : Demander le transfert.

Si vous souhaitez changer le service DNS pour un fournisseur autre que Route 53 tout en transférant le domaine vers Route 53, utilisez la procédure fournie par le fournisseur de services DNS pour obtenir les noms des serveurs de noms pour chaque domaine que vous souhaitez transférer.

> **Important**
>
> Si le bureau d'enregistrement de votre nom de domaine est également le fournisseur de services DNS du domaine, transférez votre service DNS vers Route 53 ou vers un autre fournisseur de services DNS avant de poursuivre le processus de transfert de l'enregistrement de domaine.
> Si vous transférez le service DNS en même temps que vous transférez l'enregistrement de domaine, le site web, la messagerie et les applications web associés au domaine peuvent devenir indisponibles. Pour de plus amples informations, veuillez consulter Étape 2 (facultative) : transférer votre service DNS vers Amazon Route 53 ou vers un autre fournisseur de services DNS.

Étape 5 : Demander le transfert

Pour transférer un enregistrement de domaine du serveur d'inscriptions (registrar) actuel vers Amazon Route 53, utilisez la console Route 53 pour demander le transfert. Route 53 gère la communication avec le bureau d'enregistrement actuel pour le domaine.

Vous pouvez utiliser la console pour transférer jusqu'à cinq domaines.

La procédure varie selon que vous souhaitez transférer un seul domaine ou de deux à cinq domaines :

- Pour transférer l'enregistrement d'un seul domaine vers Route 53
- Pour transférer un enregistrement de domaine vers Route 53 pour cinq domaines maximum

Utilisez le processus Transférer le domaine vers votre compte pour transférer un seul domaine vers votre compte.

Pour transférer l'enregistrement d'un seul domaine vers Route 53

1. Ouvrez la console Route 53 à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le panneau de navigation, choisissez Registered domains (Domaines membres).
3. Sur la page Domaines enregistrés, choisissez Domaine unique dans le menu déroulant Transférer en.
4. Sur la page Transférer le domaine vers votre compte, dans la section Vérifier la transférabilité du domaine, entrez le nom du domaine pour lequel vous souhaitez transférer l'enregistrement vers Route 53, puis choisissez Vérifier.
5. Si l'enregistrement du domaine est disponible pour le transfert, vérifiez que vous avez rempli les conditions de transfert pour les domaines de premier niveau, puis choisissez Suivant.

   Si l'enregistrement de domaine n'est pas disponible pour le transfert, la console Route 53 en indique les raisons. Pour plus d'informations sur la résolution des problèmes qui vous empêchent de transférer votre enregistrement, contactez votre bureau d'enregistrement.
6. Sur la page du service DNS, passez en revue les informations relatives aux serveurs de noms, puis choisissez Suivant.
7. Si vous y êtes invité, entrez le code d'autorisation ou la balise IPS que vous avez obtenu à partir de votre bureau d'enregistrement actuel dans Étape 3 : Modifier les paramètres avec le bureau d'enregistrement actuel.

> **Note**
>
> Vous n'avez pas besoin de saisir de code d'autorisation pour transférer un domaine .co.za, .uk, .co.uk, .me.uk ou .org.uk vers Route 53.

Choisissez Suivant.

8. Sur la page Options de tarification de domaine, choisissez le nombre d'années pendant lesquelles vous souhaitez enregistrer le domaine pour lequel vous effectuez le transfert et indiquez si vous souhaitez que nous renouvelions automatiquement l'enregistrement de votre domaine avant la date d'expiration.

> **Note**
>
> Les enregistrements et renouvellements de noms de domaine ne sont pas remboursables. Si vous activez le renouvellement automatique et que vous décidez que vous ne voulez plus du nom de domaine une fois l'enregistrement renouvelé, vous ne pourrez pas être remboursé du coût du renouvellement.

Choisissez Suivant.

9. Sur la page Informations de contact, entrez les coordonnées du titulaire du domaine, de l'administrateur, des contacts techniques et des contacts de facturation. Les valeurs que vous entrez ici sont appliquées à tous les domaines que vous enregistrez. Pour de plus amples informations, veuillez consulter Valeurs que vous spécifiez lorsque vous enregistrez ou transférez un domaine.

   Notez les considérations suivantes :

   Prénom et nom

   Pour les champs Prénom et Nom, nous vous recommandons d'indiquer le nom associé à votre identifiant officiel. Pour la modification des paramètres de domaine, certains registres de domaines vous demandent de fournir une preuve de votre identité. Le nom figurant sur votre carte d'identité doit correspondre exactement au nom du contact inscrit pour le domaine.

Contacts différents

Par défaut, nous utilisons les mêmes informations pour tous les trois contacts. Si vous souhaitez saisir des informations différentes pour un ou plusieurs contacts, désactivez la case Identique au contact inscrit.

> **Note**
>
> Pour les domaines .it, le contact inscrit et le contact administratif doivent être identiques.

Informations supplémentaires nécessaires

Pour certains domaines de premier niveau (TLDs), nous sommes tenus de collecter des informations supplémentaires. Pour ceux-ci TLDs, entrez les valeurs applicables après le champ Code postal/ZIP.

Protection de la confidentialité

Indiquez si vous souhaitez masquer vos informations de contact pour les requêtes WHOIS.

> **Note**
>
> Vous devez spécifier le même paramètre de confidentialité pour les contacts administratif, inscrit et technique.

Pour plus d'informations, consultez les rubriques suivantes :

- Activation ou désactivation de la protection de la confidentialité pour les informations de contact pour un domaine
- Domaines que vous pouvez enregistrer avec Amazon Route 53

> **Note**
>
> Pour activer la protection de la confidentialité pour les domaines .uk, .co.uk, .me.uk, et .org.uk, vous devez ouvrir une demande de support et demander la protection de la confidentialité.

Choisissez Suivant.

10. Sur la page Vérifier, passez en revue les informations que vous avez entrées et corrigez-les éventuellement. Lisez les conditions d'utilisation et cochez la case pour confirmer que vous les avez lues.

    Choisissez Submit request (Soumettre une demande).

11. Dans le volet de navigation, choisissez Domaines, puis Requêtes.

    Sur cette page, vous pouvez voir le statut du domaine et également si vous devez répondre à l'e-mail de vérification du contact inscrit. Vous pouvez également choisir de renvoyer l'e-mail de vérification.

    Si vous avez spécifié une adresse e-mail pour le contact inscrit qui n'a jamais été utilisée pour enregistrer un domaine avec Route 53, certains registres TLD exigent que vous vérifiez la validité de cette adresse.

    Un e-mail de vérification est envoyé à partir de l'une des adresses suivantes :

    - noreply@registrar.amazon — pour les personnes TLDs enregistrées auprès d'Amazon Registrar.
    - noreply@domainnameverification.net — pour les TLDs inscriptions auprès de notre associé au bureau d'enregistrement, Gandi. Pour déterminer le bureau d'enregistrement pour votre domaine de premier niveau, consultez Identification de votre bureau d'enregistrement.

    > **Important**
    >
    > Le contact inscrit doit suivre les instructions figurant dans le message afin de confirmer que l'e-mail a été reçu. En l'absence de confirmation, nous devons suspendre le domaine, comme exigé par les réglementations de l'ICANN. Lorsqu'un domaine est suspendu, il n'est pas disponible sur Internet.

    a. À réception de l'e-mail de vérification, cliquez sur le lien dans le corps du message permettant de confirmer l'adresse e-mail. Si vous ne recevez pas immédiatement cet e-mail, vérifiez votre dossier de courriers indésirables.

b. Retournez à la page Requêtes. Si le statut n'est pas automatiquement mis à jour avec la valeur l'adresse e-mail est vérifiée, choisissez Actualiser le statut.

12. Lorsque l'enregistrement de domaine est terminé, l'étape suivante dépend de si vous voulez utiliser Route 53 ou un autre service DNS en tant que service DNS pour le domaine :

    - Route 53 – Dans la zone hébergée créée par Route 53 lors de l'enregistrement du domaine, créez des enregistrements pour indiquer à Route 53 comment acheminer le trafic du domaine et des sous-domaines.

      Par exemple, lorsque quelqu'un saisit votre nom de domaine dans un navigateur et que la requête est transmise à Route 53, souhaitez-vous que Route 53 réponde à la requête avec l'adresse IP d'un serveur web de votre centre de données ou avec le nom d'un équilibreur de charge Elastic Load Balancing ?

      Pour de plus amples informations, veuillez consulter Utilisation des enregistrements.

      > **Important**
      >
      > Si vous créez des enregistrements dans une zone hébergée autre que celle créée automatiquement par Route 53, vous devez mettre à jour les serveurs de noms du domaine pour utiliser les serveurs de noms de la nouvelle zone hébergée.

    - Un autre service DNS – Configurez votre nouveau domaine pour acheminer les requêtes DNS vers l'autre service DNS. Exécutez la procédure Mise à jour des serveurs de noms pour utiliser un autre bureau d'enregistrement.

Suivez la procédure ci-dessous pour transférer jusqu'à cinq domaines vers votre compte.

Pour transférer un enregistrement de domaine vers Route 53 pour cinq domaines maximum

1. Ouvrez la console Route 53 à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le panneau de navigation, choisissez Registered domains (Domaines membres).
3. Sur la page Domaines enregistrés, choisissez Domaines multiples dans le menu déroulant Transférer dans.
4. Sur la page Transférer plusieurs domaines sur votre compte, saisissez jusqu'à cinq domaines que vous souhaitez transférer, ainsi que leur code d'autorisation, le cas échéant, par ligne, puis choisissez Vérifier.

5. Si l'enregistrement du domaine est disponible pour le transfert, il est répertorié dans la liste de disponibilité des domaines dès qu'il est disponible. Cochez la case en regard de chaque domaine pour lequel vous souhaitez transférer l'enregistrement, vérifiez que vous avez rempli les conditions de transfert pour les domaines de premier niveau, puis choisissez Suivant.

   Si l'enregistrement de domaine n'est pas disponible pour le transfert, la console Route 53 en indique les raisons. Pour plus d'informations sur la résolution des problèmes qui vous empêchent de transférer votre enregistrement, contactez votre bureau d'enregistrement.
6. Sur la page du service DNS, passez en revue les informations relatives aux serveurs de noms, puis choisissez Suivant.

   > **Note**
   >
   > Les enregistrements et renouvellements de noms de domaine ne sont pas remboursables. Si vous activez le renouvellement automatique et que vous décidez que vous ne voulez plus du nom de domaine une fois l'enregistrement renouvelé, vous ne pourrez pas être remboursé du coût du renouvellement.
7. Sur la page Coordonnées, saisissez les informations de contact des contacts inscrit, administratif et technique du domaine. Les valeurs que vous entrez ici sont appliquées à tous les domaines que vous transférez.

   > **Important**
   >
   > Nous vous recommandons de spécifier les valeurs suivantes pour le contact du titulaire (le propriétaire du domaine) :
   >
   > - First and last name (Nom et prénom) : nous vous conseillons d'indiquer le nom associé à votre identifiant officiel. Pour la modification des paramètres de domaine, certains registres de domaines vous demandent de fournir une preuve de votre identité. Le nom figurant sur votre carte d'identité doit correspondre exactement au nom du contact inscrit pour le domaine.
   > - Contact details (Coordonnées) : lors du transfert de domaine, nous vous recommandons de spécifier les mêmes valeurs que celles spécifiées avec le bureau d'enregistrement actuel. Lorsque vous modifiez les coordonnées du contact du titulaire, vous modifiez le propriétaire du domaine, mais certains registres TLD ne permettent pas de modifier le propriétaire du domaine lors d'un transfert de domaine. Si vous modifiez les coordonnées du contact du titulaire, le transfert peut échouer.

Vous pouvez modifier les coordonnées du contact du titulaire après le transfert du domaine.

Par défaut, nous utilisons les mêmes informations pour tous les trois contacts. Si vous souhaitez saisir des informations différentes pour un ou plusieurs contacts, désactivez la valeur de la case Identique au contact inscrit.

> **Note**
>
> Pour les domaines .it, le contact inscrit et le contact administratif doivent être identiques.

Pour de plus amples informations, veuillez consulter Valeurs que vous spécifiez lorsque vous enregistrez ou transférez un domaine.

8. Pour certains TLDs, nous sommes tenus de collecter des informations supplémentaires. Pour ceux-ci TLDs, entrez les valeurs applicables après le champ Code postal/ZIP.
9. Si la valeur de Contact Type est Person, choisissez si vous souhaitez masquer vos informations de contact pour les requêtes WHOIS. Pour de plus amples informations, veuillez consulter Activation ou désactivation de la protection de la confidentialité pour les informations de contact pour un domaine.
10. Sélectionnez Envoyer.
11. Vérifiez les informations que vous avez saisies, lisez les conditions d'utilisation et cochez la case pour confirmer que vous avez lu les conditions.
12. Choisissez Submit request (Soumettre une demande).

    Nous confirmons que les domaines peuvent être transférés et nous envoyons un e-mail aux contacts inscrits du domaine pour demander l'autorisation de transférer le domaine.
13. Dans le volet de navigation, choisissez Domaines, puis Requêtes.

    Sur cette page, vous pouvez voir le statut du domaine et également si vous devez répondre à l'e-mail de vérification du contact inscrit. Vous pouvez également choisir de renvoyer l'e-mail de vérification.

    Si vous avez spécifié une adresse e-mail pour le contact inscrit qui n'a jamais été utilisée pour enregistrer un domaine avec Route 53, certains registres TLD exigent que vous vérifiez la validité de cette adresse.

Un e-mail de vérification est envoyé à partir de l'une des adresses suivantes :

- noreply@registrar.amazon — pour les personnes TLDs enregistrées auprès d'Amazon Registrar.
- noreply@domainnameverification.net — pour les TLDs inscriptions auprès de notre associé au bureau d'enregistrement, Gandi. Pour déterminer le bureau d'enregistrement pour votre domaine de premier niveau, consultez Identification de votre bureau d'enregistrement.

> **Important**
>
> Le contact inscrit doit suivre les instructions figurant dans le message afin de confirmer que l'e-mail a été reçu. En l'absence de confirmation, nous devons suspendre le domaine, comme exigé par les réglementations de l'ICANN. Lorsqu'un domaine est suspendu, il n'est pas disponible sur Internet.

a. À réception de l'e-mail de vérification, cliquez sur le lien dans le corps du message permettant de confirmer l'adresse e-mail. Si vous ne recevez pas immédiatement cet e-mail, vérifiez votre dossier de courriers indésirables.

b. Retournez à la page Requêtes. Si le statut n'est pas automatiquement mis à jour avec la valeur l'adresse e-mail est vérifiée, choisissez Actualiser le statut.

14. Lorsque l'enregistrement de domaine est terminé, l'étape suivante dépend de si vous voulez utiliser Route 53 ou un autre service DNS en tant que service DNS pour le domaine :

    - Route 53 – Dans la zone hébergée créée par Route 53 lors de l'enregistrement du domaine, créez des enregistrements pour indiquer à Route 53 comment acheminer le trafic du domaine et des sous-domaines.

      Par exemple, lorsque quelqu'un saisit votre nom de domaine dans un navigateur et que cette requête est transmise à Route 53, souhaitez-vous que Route 53 réponde à la requête avec l'adresse IP d'un serveur web de votre centre de données ou avec le nom d'un équilibreur de charge ELB ?

      Pour de plus amples informations, veuillez consulter Utilisation des enregistrements.

> **Important**
>
> Si vous créez des enregistrements dans une zone hébergée autre que celle créée automatiquement par Route 53, vous devez mettre à jour les serveurs de noms du domaine pour utiliser les serveurs de noms de la nouvelle zone hébergée.

- Un autre service DNS – Configurez votre nouveau domaine pour acheminer les requêtes DNS vers l'autre service DNS. Exécutez la procédure Mise à jour des serveurs de noms pour utiliser un autre bureau d'enregistrement.

Étape 6 : cliquez sur le lien dans les e-mails de confirmation et d'autorisation

Peu de temps après votre demande de transfert, nous pouvons envoyer un ou plusieurs e-mails au contact inscrit pour le domaine :

E-mail pour confirmer que le contact inscrit est joignable

Si vous n'avez jamais enregistré un domaine auprès de Route 53 ni transféré un domaine vers Route 53, nous vous envoyons un e-mail pour vous demander de confirmer que l'adresse e-mail est valide. Nous conservons ces informations pour éviter d'avoir à vous renvoyer cet e-mail de confirmation.

E-mail pour obtenir l'autorisation de transférer le domaine

Dans certains TLDs cas, vous devez répondre à un e-mail pour autoriser le transfert du domaine.

TLDs Génériques tels que .com, .net et .org

L'autorisation n'est pas obligatoire pour les domaines qui présentent un domaine de premier niveau (TLD) générique, par exemple .com, .net ou .org.

Géographique TLDs , par exemple .co.uk et .jp

Pour les domaines ayant un domaine de premier niveau (TLD) géographique, nous sommes tenus d'obtenir votre autorisation de transférer le domaine. Si vous transférez 10 domaines, nous devons vous envoyer autant d'e-mails, et vous devez cliquer sur le lien d'autorisation figurant dans chacun d'eux.

Les e-mails sont tous adressés au contact inscrit pour le domaine :

- Si vous êtes le contact inscrit pour le domaine, suivez les instructions dans l'e-mail afin d'autoriser le transfert.
- Si une autre personne est le contact inscrit, demandez à cette personne de suivre les instructions figurant de l'e-mail pour autoriser le transfert.

> **Important**
>
> Si vous transférez un domaine ayant un domaine de premier niveau (TLD) géographique, nous attendons un maximum de cinq jours pour que le contact inscrit autorise le transfert. Si le contact inscrit ne répond pas au terme ce délai, nous annulons l'opération de transfert et nous en informons le contact inscrit par e-mail.

Rubriques

- E-mail d'autorisation pour un nouveau propriétaire ou une nouvelle adresse e-mail
- Adresses e-mail qui envoient les e-mails d'autorisation
- Approbation du bureau d'enregistrement actuel
- Quelle est l'étape suivante ?

E-mail d'autorisation pour un nouveau propriétaire ou une nouvelle adresse e-mail

Si vous avez modifié les valeurs suivantes, nous vous envoyons un e-mail distinct pour demander votre autorisation :

Propriétaire du domaine

Si vous modifiez le propriétaire du domaine, tel que décrit dans Qui est le propriétaire d'un domaine ?, nous envoyons un e-mail au contact inscrit pour le domaine.

Adresse e-mail du contact du titulaire (uniquement pour certains TLDs)

Dans certains cas TLDs, si vous modifiez l'adresse e-mail du contact du titulaire, nous envoyons un e-mail à l'ancienne et à la nouvelle adresse e-mail du contact du titulaire. La modification doit être autorisée par les deux destinataires qui doivent suivre les instructions reçues dans les e-mails.

Concernant les modifications apportées au propriétaire du domaine ou à l'adresse électronique du contact inscrit, si nous ne recevons pas d'autorisation pour la modification demandée dans un délai de 3 à 15 jours, selon le domaine de premier niveau, nous devons annuler la demande, comme requis par l'ICANN.

Adresses e-mail qui envoient les e-mails d'autorisation

Tous les e-mails sont envoyés à partir de l'une des adresses suivantes.

TLDs	Adresse e-mail qui envoie l'e-mail d'autorisation
.com.au et .net.au	no-reply@ispapi.net L'e-mail contient un lien vers http://transfers.ispapi.net.
.fr	nic@nic.fr, si vous modifiez le contact inscrit pour un nom de domaine .fr lorsque vous transférez le domaine. (L'e-mail est envoyé au contact inscrit actuel et au nouveau contact inscrit.)
Tous les autres	Une des adresses e-mail suivantes : • noreply@registrar.amazon • noreply@domainnameverification.net

Pour déterminer le bureau d'enregistrement pour votre domaine de premier niveau, consultez Domaines que vous pouvez enregistrer avec Amazon Route 53.

Approbation du bureau d'enregistrement actuel

Si le contact inscrit autorise le transfert, nous commençons à collaborer avec votre bureau d'enregistrement actuel pour transférer votre domaine. Cette étape peut prendre jusqu'à dix jours, en fonction du TLD pour votre domaine :

- Domaines de premier niveau génériques – Prend jusqu'à sept jours

- Domaines géographiques de premier niveau (également appelés domaines de premier niveau nationaux) – Prend jusqu'à dix jours

S'il ne répond pas à notre demande de transfert, ce qui est fréquent, le transfert se fait automatiquement. Si votre bureau d'enregistrement actuel rejette la demande de transfert, nous en envoyons par courriel une notification au contact inscrit actuel. L'inscrit doit contacter le bureau d'enregistrement actuel et résoudre les problèmes relatifs au transfert.

Quelle est l'étape suivante ?

Lorsque le transfert de votre domaine a été approuvé, nous adressons un nouvel e-mail au contact inscrit. Pour plus d'informations sur le processus, consultez Affichage du statut du transfert d'un domaine.

Nous facturons le transfert de domaine sur votre AWS compte dès que le transfert est terminé. Pour obtenir la liste des frais par domaine de premier niveau (TLD), consultez Tarification Amazon Route 53 pour l'enregistrement de domaine.

> **Note**
>
> Il s'agit d'un prélèvement unique, il n'apparaît donc pas dans vos statistiques CloudWatch de facturation. Pour plus d'informations sur CloudWatch les métriques, consultez la section Utilisation CloudWatch des métriques Amazon dans le guide de CloudWatch l'utilisateur Amazon.

Étape 7 : mise à jour de la configuration du domaine

Une fois que le transfert est terminé, vous pouvez éventuellement modifier les paramètres suivants :

Verrouillage du transfert

Pour transférer le domaine vers Route 53, vous devez désactiver le verrouillage du transfert. Si vous souhaitez réactiver le verrouillage pour empêcher les transferts non autorisés, consultez Verrouillage d'un domaine pour empêcher son transfert non autorisé vers un autre bureau d'enregistrement.

Renouvellement automatique

Nous configurons le renouvellement automatique du domaine transféré, à l'approche de la date d'expiration. Pour plus d'informations sur la façon de modifier ce paramètre, consultez Activation ou désactivation du renouvellement automatique pour un domaine.

Période d'enregistrement étendue

Par défaut, Route 53 renouvelle le domaine une fois par an. Si vous souhaitez enregistrer le domaine pour une période plus longue, consultez Extension de la période d'enregistrement pour un domaine.

DNSSEC

Pour plus d'informations sur la configuration DNSSEC pour le domaine, consultez Configuration du protocole DNSSEC pour un domaine.

Affichage du statut du transfert d'un domaine

Une fois que vous lancez le transfert d'un domaine depuis un autre bureau d'enregistrement de domaine vers Amazon Route 53, vous pouvez suivre le statut sur la page Requêtes (nouvelle console) ou la page (Demandes en attente (ancienne console) de la console Route 53. La colonne Status comprend une brève description de l'étape en cours. La liste suivante présente le texte qui s'affiche dans la console et une description plus détaillée de chaque étape.

> **Note**
>
> Lorsque vous envoyez une demande de transfert, le statut initial est Domain transfer request submitted, ce qui signifie que nous avons reçu votre demande.

Déterminer si le domaine répond aux exigences de transfert (étape 1 sur 14)

Nous confirmons que votre domaine est éligible pour le transfert. Vous devez déverrouiller votre domaine. Par ailleurs, le code de statut du domaine ne peut pas être l'un des codes suivants lorsque vous envoyez la demande de transfert :

- clientTransferProhibited
- pendingDelete
- pendingTransfer

- redemptionPeriod

Géographique TLDs uniquement — vérification des informations WHOIS (étape 2 de 14)

Si vous transférez un domaine ayant un domaine de premier niveau (TLD) géographique, nous envoyons une requête WHOIS pour votre domaine afin de déterminer si vous avez désactivé la protection de confidentialité pour ce domaine. Si la protection de la confidentialité est toujours activée avec votre bureau d'enregistrement actuel, nous ne serons pas en mesure d'accéder aux informations dont nous avons besoin pour transférer le domaine.

> **Note**
>
> L'autorisation n'est pas obligatoire pour les domaines qui présentent un domaine de premier niveau (TLD) générique, par exemple .com, .net ou .org.

Géographique TLDs uniquement — Envoi d'un e-mail au contact du titulaire pour obtenir l'autorisation de transfert (étape 3 de 14)

Si vous transférez un domaine ayant un domaine de premier niveau (TLD) géographique, nous avons envoyé un e-mail au contact inscrit pour le domaine. L'objectif de l'e-mail est de confirmer que le transfert a été demandé par un contact autorisé pour le domaine.

> **Note**
>
> L'autorisation n'est pas obligatoire pour les domaines qui présentent un domaine de premier niveau (TLD) générique, par exemple .com, .net ou .org.

Vérification du transfert avec le bureau d'enregistrement actuel (étape 4 sur 14)

Nous avons envoyé une demande au bureau d'enregistrement actuel pour le domaine afin d'initier le transfert.

Géographique TLDs uniquement — En attente de l'autorisation du contact du titulaire (étape 5 sur 14)

Nous avons envoyé un e-mail au contact inscrit du domaine (voir étape 3 de 14) et nous attendons que celui-ci clique sur un lien dans l'e-mail pour autoriser le transfert. Si vous transférez un domaine ayant un domaine de premier niveau (TLD) géographique et vous n'avez pas reçu l'e-mail pour une raison quelconque, consultez Renvoi des e-mails de confirmation et d'autorisation.

On a contacté le bureau d'enregistrement actuel pour demander le transfert (étape 6 sur 14)

Nous travaillons en collaboration avec le bureau d'enregistrement actuel pour le domaine afin de finaliser le transfert.

Attendre que le bureau d'enregistrement actuel termine le transfert (étape 7 sur 14)

Votre bureau d'enregistrement actuel confirme que votre domaine répond aux exigences de transfert. Cette étape peut prendre jusqu'à dix jours, en fonction du TLD pour votre domaine :

- Domaines de premier niveau génériques – Prend jusqu'à sept jours
- Domaines géographiques de premier niveau (également appelés domaines de premier niveau nationaux) – Prend jusqu'à dix jours

> **Note**
>
> Si vous avez approuvé l'e-mail de confirmation envoyé depuis Route 53 lors du transfert d'un domaine .JP, mais qu'il s'est arrêté pendant plusieurs jours à l'ÉTAPE 7, veuillez prendre contact avec le Centre de support AWS pour obtenir de l'aide.

Pour la plupart des bureaux d'enregistrement, le processus est entièrement automatisé et ne peut pas être accéléré. Certains bureaux d'enregistrement vous envoient un e-mail vous demandant d'approuver le transfert. Si c'est le cas de votre bureau d'enregistrement, le transfert sera peut-être beaucoup plus rapide que la durée habituelle de sept à dix jours.

Pour plus d'informations sur les raisons pour lesquelles un bureau d'enregistrement peut rejeter le transfert, consultez Exigences liées au transfert de domaines de premier niveau.

Confirmer avec le contact propriétaire que le contact a initié le transfert (étape 8 sur 14)

Certains registres TLD envoient au contact inscrit un autre e-mail afin de confirmer que le transfert de domaine a été demandé par un utilisateur autorisé.

Synchronisation des serveurs de noms avec le registre (étape 9 sur 14)

Cette étape a lieu uniquement si les serveurs de noms que vous avez fournis dans le cadre de la demande de transfert sont différents des serveurs de noms indiqués au bureau d'enregistrement actuel. Nous allons essayer de mettre à jour vos serveurs de noms avec les nouveaux serveurs de noms que vous avez fournis.

Synchronisation des paramètres avec le registre (étape 10 sur 14)

Nous vérifions que le transfert s'est correctement déroulé. Nous synchronisons les données relatives à votre domaine avec le partenaire auquel nous faisons appel pour l'enregistrement.

Envoi des informations de contact mises à jour au registre (étape 11 sur 14)

Si vous avez modifié la propriété du domaine lorsque vous avez demandé le transfert, nous essayons de valider cette modification. Toutefois, la plupart des registres ne permettent pas le transfert de la propriété dans le cadre du processus de transfert du domaine.

Finalizing the transfer to Route 53 (step 12 of 14)

Nous confirmons que le processus de transfert s'est déroulé correctement.

Finalisation du transfert (étape 13 sur 14)

Nous configurons votre domaine dans Route 53.

Transfert terminé (étape 14 sur 14)

Votre transfert est terminé.

Incidence du transfert d'un domaine vers Amazon Route 53 sur la date d'expiration de l'enregistrement de votre domaine

Lorsque vous transférez un domaine entre des bureaux d'enregistrement, certains registres TLD vous permettent de conserver la même date d'expiration pour votre domaine, d'autres registres ajoutent une année à la date d'expiration et certains registres ajoutent une année à la date de transfert.

> **Note**
>
> Dans la plupart des cas TLDs, vous pouvez prolonger la période d'enregistrement d'un domaine jusqu'à dix ans après son transfert vers Amazon Route 53. Pour de plus amples informations, veuillez consulter Extension de la période d'enregistrement pour un domaine.

Générique TLDs

Lorsque vous transférez un domaine de premier niveau générique (par exemple, .com) vers Route 53, la nouvelle date d'expiration pour le domaine est la date d'expiration définie avec votre bureau d'enregistrement précédent, plus un an.

Géographique TLDs

Lorsque vous transférez un domaine de premier niveau géographique (par exemple, .co.uk) vers Route 53, la nouvelle date d'expiration pour le domaine varie selon le domaine de premier niveau. Identifiez votre domaine de premier niveau dans le tableau suivant pour déterminer l'incidence du transfert de votre domaine sur la date d'expiration.

Continent	Géographie TLDs et effet du transfert d'un domaine sur la date d'expiration
Afrique	.co.za – La date d'expiration ne change pas.
Amériques	.cl, .com.ar, .com.br – La date d'expiration ne change pas. .ca, .co, .mx, .us – Une année est ajoutée à l'ancienne date d'expiration.
Asie/Océanie	.com.au, .com.sg, .jp, .net.au, .sg — La date d'expiration reste la même. .co.nz, .in, .net.nz, .org.nz — Un an est ajouté à l'ancienne date d'expiration.
Europe	.ch, .co.uk, .es, .fi, .me.uk, .org.uk, .se – La date d'expiration ne change pas. .berlin, .eu, .io, .me, .ruhr, .wien – Une année est ajoutée à l'ancienne date d'expiration. .be, .de, .fr, .it, .nl – La date d'expiration équivaut à une année après la date du transfert.

Transférer un domaine vers un autre AWS compte

Si vous avez enregistré un domaine à l'aide d'un AWS compte et que vous souhaitez le transférer vers un autre AWS compte, vous pouvez facilement le transférer en utilisant la nouvelle console ou en utilisant la AWS CLI ou d'autres méthodes de programmation.

Rubriques

- Étape 1 : transférer un domaine vers un autre AWS compte
- Étape 2 (facultatif) : migrer une zone hébergée vers un autre AWS compte

Étape 1 : transférer un domaine vers un autre AWS compte

Les domaines ne peuvent pas être transférés dans les 14 premiers jours suivant l'enregistrement.

Lorsque vous lancez le transfert de domaine, vous devez vous connecter à l'aide du compte racine ou d'un utilisateur qui a reçu les autorisations IAM de l'une ou plusieurs des manières suivantes :

- La politique AdministratorAccessgérée est attribuée à l'utilisateur.
- La politique DomainsFullAccess gérée AmazonRoute53 est attribuée à l'utilisateur.
- La politique FullAccess gérée AmazonRoute53 est attribuée à l'utilisateur.
- La politique PowerUserAccessgérée est attribuée à l'utilisateur.
- L'utilisateur a l'autorisation d'effectuer toutes les actions suivantes : `TransferDomains`, `DisableDomainTransferLock` et `RetrieveDomainAuthCode`.

Si vous ne vous connectez pas à l'aide du compte racine ou d'un utilisateur qui dispose des autorisations requises, nous ne pouvons pas effectuer le transfert. Cette exigence empêche les utilisateurs non autorisés de transférer des domaines vers d'autres Comptes AWS.

Le processus de transfert comporte deux étapes. Le titulaire du compte d'origine commence d'abord le transfert : dans la procédure initier un transfert vers un autre Compte AWS, puis le titulaire du compte de destination accepte le transfert dans le cadre de la procédure accepter un transfert depuis une autre Compte AWS.

Pour transférer un domaine vers un autre AWS compte

1. Connectez-vous à en AWS utilisant le nom de domaine sur Compte AWS lequel le domaine est actuellement enregistré.
2. Ouvrez la console Route 53 à l'adresse https://console.aws.amazon.com/route53/.
3. Dans le panneau de navigation, choisissez Registered domains (Domaines membres).
4. Choisissez le nom du domaine que vous souhaitez transférer vers un autre Compte AWS.
5. Au-dessus de la section Détails, dans le menu déroulant Transfert sortant, choisissez Transférer vers un autre Compte AWS.

6. Dans la boîte de dialogue Transférer vers un autre Compte AWS, entrez l'ID du compte de destination. Vous pouvez obtenir cet identifiant auprès du propriétaire du Compte AWS de destination.
7. Choisissez Confirmer.
8. Dans la boîte de dialogue Générer un mot de passe, copiez le mot de passe et transmettez-le au Compte AWS propriétaire destinataire.

   Sur la page Requêtes, le statut du domaine s'affiche En cours et le type indique Transfert interne hors du domaine.

Pour accepter un transfert de domaine depuis un autre AWS compte

1. Connectez-vous en AWS utilisant celui Compte AWS qui reçoit le domaine.
2. Ouvrez la console Route 53 à l'adresse https://console.aws.amazon.com/route53/.
3. Dans le panneau de navigation, sélectionnez Requêtes.
4. Sur la page Demandes, sélectionnez le bouton radio à côté du nom de domaine que vous transférez d'un autre nom de domaine Compte AWS. Si le domaine est prêt à être transféré, le statut est Action requise et le type est Transfert interne de domaine entrant.

   Vous avez trois jours pour accepter la demande. Si le transfert n'est pas accepté dans les trois jours, la demande de transfert est annulée.
5. Dans le menu déroulant Action, choisissez Accepter.

   Vous pouvez également choisir Refuser pour annuler le processus de transfert.
6. Si vous avez accepté, sur la page Transférer le domaine vers votre compte, dans la section Mot de passe, entrez le mot de passe que vous avez reçu du titulaire du compte d'origine.

   Acceptez ces conditions générales et choisissez Suivant.
7. Accédez à la page Requêtes pour suivre l'état du transfert et les autres étapes à effectuer.
8. Une fois le transfert terminé, vous pouvez mettre à jour les informations de contact. Pour de plus amples informations, veuillez consulter Mise à jour des informations de contact et de la propriété pour un domaine.

Transférer le domaine par programmation

Vous pouvez également transférer le domaine par programmation en utilisant l'API Route 53 AWS CLI, l'une des ou l'API Route 53. AWS SDKs Pour plus d'informations, consultez la documentation de suivante :

- Pour un aperçu du processus de transfert et de la documentation sur les actions d'API que vous utilisez pour transférer un domaine à l'aide de l'API d'enregistrement de domaine Route 53, consultez TransferDomainToAnotherAwsAccountle manuel Amazon Route 53 API Reference.
- Pour obtenir de la documentation sur les autres options de transfert de domaines par programmation, consultez « SDKs & Toolkits » dans la section Guides et références d'API de la page « AWS documentation ».
- Le compte destinataire dispose de trois jours pour accepter le transfert depuis le compte d'origine, en utilisant l'API transfer-domain-to-another-aws-account. Si le transfert n'est pas accepté dans les trois jours, la demande de transfert est annulée.

> **Important**
>
> Lorsque vous transférez un domaine vers un autre AWS compte, la zone hébergée du domaine n'est pas transférée. Si vous souhaitez également transférer la zone hébergée, patientez jusqu'à ce que le domaine ait été transféré, puis consultez Étape 2 (facultatif) : migrer une zone hébergée vers un autre AWS compte.

Étape 2 (facultatif) : migrer une zone hébergée vers un autre AWS compte

Si vous utilisez Route 53 comme service DNS pour le domaine, Route 53 ne transfère pas la zone hébergée lorsque vous transférez un domaine vers un autre compte AWS . Si l'enregistrement de domaine est associé à un compte et si la zone hébergée correspondante est associée à un autre compte, cela n'a aucune incidence sur l'enregistrement de domaine, ni sur les fonctionnalités DNS. Le seule différence est que vous devrez vous connecter à la console Route 53 à l'aide d'un compte pour voir le domaine et vous connecter à l'aide de l'autre compte pour voir la zone hébergée.

Si vous possédez le compte depuis lequel vous transférez le domaine et le compte vers lequel vous transférez le domaine, vous pouvez éventuellement procéder à la migration de la zone hébergée du domaine vers un autre compte, mais ce n'est pas obligatoire. Route 53 continuera d'utiliser les enregistrements de la zone hébergée existante pour acheminer le trafic pour le domaine.

> **Important**
>
> Si vous ne possédez pas à la fois le compte à partir duquel vous transférez le domaine et le compte vers lequel vous transférez le domaine, vous devez soit migrer la zone hébergée existante vers le AWS compte vers lequel vous transférez le domaine, soit créer une nouvelle zone hébergée dans un AWS compte que vous possédez. Si vous ne possédez pas le compte qui a créé la zone hébergée qui achemine le trafic pour le domaine, vous ne pouvez pas contrôler la façon dont le trafic est acheminé.

Pour migrer la zone hébergée existante vers le nouveau compte, consultez Migration d'une zone hébergée vers un autre compte AWS.

Pour créer une nouvelle zone hébergée, consultez Configuration d'Amazon Route 53 en tant que service DNS d'un domaine existant. Cette rubrique est généralement utilisée lorsque vous transférez des domaines d'un autre bureau d'enregistrement vers Route 53, mais le processus est le même lorsque vous transférez des domaines d'un AWS compte à un autre.

Transfert d'un domaine depuis Amazon Route 53 vers un autre bureau d'enregistrement

Lorsque vous transférez un domaine depuis Amazon Route 53 vers un autre bureau d'enregistrement, vous obtenez des informations de Route 53 et les fournissez au nouveau bureau d'enregistrement. Le nouveau bureau d'enregistrement se charge du reste.

> **Important**
>
> Si vous utilisez actuellement Route 53 en tant que fournisseur de services DNS et si vous souhaitez également transférer le service DNS vers un autre fournisseur, sachez que certains fournisseurs de services DNS ne proposent pas de fonctions strictement équivalentes aux fonctions de Route 53 suivantes. Vous devrez déterminer avec le nouveau fournisseur de services DNS la façon d'obtenir des fonctionnalités comparables :
>
> - Enregistrements d'alias. Pour de plus amples informations, veuillez consulter Choix entre des enregistrements avec ou sans alias.
> - Les stratégies de routage autres que la stratégie de routage simple. Pour de plus amples informations, veuillez consulter Sélection d'une stratégie de routage.

- Les surveillances de l'état associées à des enregistrements. Pour de plus amples informations, veuillez consulter Configuration du basculement DNS.

La plupart des bureaux d'enregistrement de domaine imposent des exigences pour le transfert d'un domaine vers un autre bureau d'enregistrement. Ces exigences servent principalement à empêcher les propriétaires de domaines frauduleux de transférer de façon répétée les domaines vers différents bureaux d'enregistrement. Ces exigences varient, à l'exception des exigences classiques suivantes :

- Vous devez avoir enregistré le domaine auprès du bureau d'enregistrement actuel ou transféré l'enregistrement du domaine au bureau d'enregistrement actuel il y a au moins 14 jours.
- Le code de statut du domaine ne peut pas être l'un des codes suivants :
  - pendingDelete
  - pendingTransfer
  - redemptionPeriod
  - clientTransferProhibited
  - serverTransferProhibited

Pour obtenir une liste des codes de statuts de noms de domaines et la signification de chaque code, accédez au site web de l'ICANN et recherchez codes EPP. (Effectuez une recherche sur le site web de l'ICANN. Les recherches sur Internet renvoient parfois une ancienne version du document.)

> **Note**
>
> Si vous souhaitez transférer votre domaine vers un autre bureau d'enregistrement de domaines mais que le AWS compte sous lequel le domaine est enregistré est fermé, suspendu ou résilié, vous pouvez contacter le AWS Support pour obtenir de l'aide. Les domaines ne peuvent pas être transférés dans les 14 premiers jours suivant l'enregistrement. Pour de plus amples informations, veuillez consulter Contacter le AWS Support à propos de problèmes d'enregistrement de domaine.

> **Note**
>
> Si le nouveau bureau d'enregistrement a besoin d'un code REG-ID, vous pouvez contacter le AWS Support pour obtenir de l'aide. Pour de plus amples informations, veuillez consulter Contacter le AWS Support à propos de problèmes d'enregistrement de domaine.

Pour transférer un domaine depuis Route 53 vers un autre bureau d'enregistrement

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le panneau de navigation, choisissez Registered domains (Domaines membres).
3. Choisissez le nom du domaine que vous souhaitez transférer vers un autre bureau d'enregistrement.
4. Sur la page Nom de domaine, vérifiez la valeur du code de statut du nom de domaine. S'il s'agit de l'une des valeurs suivantes, vous ne pouvez pas transférer le domaine actuellement :

   - pendingDelete
   - pendingTransfer
   - redemptionPeriod
   - clientTransferProhibited
   - serverTransferProhibited

   Pour obtenir une liste des codes de statuts de noms de domaines et la signification de chaque code, accédez au site web de l'ICANN et recherchez codes EPP. (Effectuez une recherche sur le site web de l'ICANN. Les recherches sur Internet renvoient parfois une ancienne version du document.)

   Si la valeur du code de statut du nom de domaine est serverTransferProhibited, vous pouvez contacter le AWS Support gratuitement pour savoir ce que vous devez faire pour transférer le domaine. Pour de plus amples informations, veuillez consulter Contacter le AWS Support à propos de problèmes d'enregistrement de domaine.
5. Si la valeur du verrouillage du transfert est activée, choisissez Désactiver le verrouillage du transfert dans le menu déroulant Actions.

> **Note**
>
> Contactez le AWS Support pour débloquer le transfert des domaines .jp vers le bureau d'enregistrement. Pour de plus amples informations, veuillez consulter Contacter le AWS Support à propos de problèmes d'enregistrement de domaine.

6. Tous les domaines sauf les domaines .be, .co.za, .ru, .uk, .co.uk, .me.uk et .org.uk — Sur la page du nom de domaine, choisissez Transférer vers un autre bureau d'enregistrement dans le menu déroulant Transférer vers un autre bureau d'enregistrement.

   Dans la boîte de dialogue Transférer vers un autre bureau d'enregistrement, choisissez Copier pour copier le code d'autorisation pour le transfert de domaine. Vous fournirez cette valeur à votre bureau d'enregistrement ultérieurement dans cette procédure.

   > **Note**
   >
   > Pour les domaines .eu, vous pouvez également générer le code d'authentification en utilisant le panneau « My.EU » du registre : https://my.eurid.eu/.

   Domaines .be, .co.za, .es, .ru, .uk, .co.uk, .me.uk et .org.uk — Procédez comme suit :

   domaines .be

   Obtenez le code d'autorisation dans le registre des domaines .be sur le site Web de DNS Belgium.

   Domaines .co.za

   Vous n'avez pas besoin de code d'autorisation pour transférer un domaine .co.za vers un autre bureau d'enregistrement.

   Domaines .ru

   Obtenez le code d'autorisation dans le registre des domaines .ru à l'adresse https://www.nic.ru/en/auth/recovery/:

   a. Choisissez l'option pour récupérer les informations d'identification par nom de domaine.
   b. Entrez votre nom de domaine, puis choisissez Continuer.
   c. Suivez les invites à l'écran pour obtenir l'accès à la page d'administration RU-CENTER.

d. Dans la section Manage your account (Gérer votre compte), choisissez Domain transfer (Transfert de domaine).

e. Confirmez le transfert avec REGRU-RU.

Domaines .uk, .co.uk, .me.uk et .org.uk

Modifier la balise IPS pour la valeur pour le nouveau bureau d'enregistrement :

a. Accédez à la page Find a Registrar sur le site web de Nominet pour connaître la balise IPS pour le nouveau bureau d'enregistrement. (Nominet est le registre pour les domaines .uk, .co.uk, .me.uk et .org.uk.)

b. Sur la page Domaines enregistrés > nom de domaine, sélectionnez le menu déroulant Transférer, puis Mettre à jour le tag IPS, et spécifiez la valeur que vous avez obtenue à l'étape 6a.

c. Choisissez Mettre à jour.

> **Note**
>
> Vous pouvez également mettre à jour le tag IPS sur la console Nominet. Pour obtenir des instructions, voir Changer de bureau d'enregistrement.

7. Si vous n'utilisez pas Route 53 en tant que fournisseur de services DNS pour votre domaine actuellement, passez à l'étape 10.

   Si vous utilisez Route 53 en tant que fournisseur de services DNS du domaine actuellement, effectuez les opérations suivantes :

   a. Choisissez Hosted Zones (Zones hébergées).

   b. Sélectionnez le nom de la zone hébergée pour votre domaine. Le domaine et la zone hébergée portent le même nom.

   c. Si vous souhaitez continuer à utiliser Route 53 en tant que fournisseur de services DNS pour le domaine : obtenez les noms des quatre serveurs de noms affectés par Route 53 à votre zone hébergée. Pour de plus amples informations, veuillez consulter Obtention de la liste des serveurs de noms d'une zone hébergée publique.

      Si vous ne souhaitez pas continuer à utiliser Route 53 en tant que fournisseur de services DNS du domaine : prenez note des paramètres de tous vos enregistrements, sauf pour les enregistrements NS et SOA. Pour les fonctions spécifiques à Route 53, telles que les

enregistrements d'alias, vous devrez déterminer avec le nouveau fournisseur de services DNS la façon d'obtenir des fonctionnalités comparables.

8. Si vous transférez un service DNS vers un autre fournisseur, utilisez les méthodes fournies par le nouveau service DNS pour effectuer les tâches suivantes :

   - Créer une zone hébergée
   - Création d'enregistrements qui reproduisent les fonctionnalités de vos enregistrements Route 53
   - Obtenir les serveurs de noms affectés par le nouveau service DNS à votre zone hébergée

9. Suivre le processus fourni par le nouveau bureau d'enregistrement pour demander le transfert du domaine.

   Tous les domaines sauf les domaines .co.za, .uk, .co.uk, .me.uk et .org.uk : vous serez invité à saisir le code d'autorisation que vous avez reçu de la console Route 53 à l'étape 6 de cette procédure.

10. Si vous souhaitez toujours utiliser Route 53 comme fournisseur de services DNS, utilisez le processus fourni par le nouveau bureau d'enregistrement pour spécifier les noms des serveurs de noms Route 53 que vous avez obtenus à l'étape 7. Si vous souhaitez utiliser un autre fournisseur de services DNS, spécifiez les noms des serveurs de noms que le nouveau fournisseur vous a fournis lorsque vous avez créé une nouvelle zone hébergée à l'étape 8.

11. Répondez à l'e-mail de confirmation :

    Tous les domaines sauf les domaines .jp

    Route 53 envoie un e-mail de confirmation à l'adresse email du contact inscrit pour le domaine :

    - Si vous ne répondez pas à l'e-mail, le transfert se fait automatiquement à la date spécifiée.
    - Si vous souhaitez effectuer le transfert rapidement si vous voulez annuler le transfert, cliquez sur le lien contenu dans l'e-mail pour accéder au site Web de Route 53 et sélectionnez l'option de votre choix.
    - Selon le TLD, l'e-mail de confirmation peut contenir un lien vers https://approvemove.com lequel vous pouvez approuver ou refuser le transfert. Lorsque la protection de la confidentialité est activée pour les contacts du domaine, l'e-mail est envoyé à partir des adresses identity-protect.org enregistrées TLDs auprès d'Amazon Registrar. Pour déterminer le bureau d'enregistrement pour votre domaine de premier niveau, consultez Identification de votre bureau d'enregistrement.

Domaines .jp

Route 53 envoie un e-mail de confirmation à l'adresse email du contact inscrit pour le domaine depuis l'adresse noreply@domainnameverification.net avec un lien pour confirmer le transfert :

- Si vous ne répondez pas à l'e-mail, le transfert est annulé à la date spécifiée.
- Si vous souhaitez effectuer le transfert rapidement si vous voulez annuler le transfert, cliquez sur le lien contenu dans l'e-mail pour accéder au site Web de Route 53 et sélectionnez l'option de votre choix. Vous devrez fournir le code d'autorisation de domaine que vous avez obtenu à l'étape 7.

En outre, vous pouvez recevoir un e-mail de WIXI.jp. Vous pouvez ignorer cet e-mail.

12. Si le bureau d'enregistrement sur lequel vous transférez le domaine rapporte que le transfert a échoué, contactez le bureau d'enregistrement pour plus d'informations. Lorsque vous transférez un domaine vers un autre bureau d'enregistrement, toutes les mises à jour de statut vont vers le nouveau bureau d'enregistrement ; c'est pourquoi Route 53 n'a aucune information sur l'échec d'un transfert.

    Si le nouveau bureau d'enregistrement indique que le transfert a échoué parce que le code d'autorisation que vous avez reçu de Route 53 n'est pas valide, ouvrez un dossier auprès du AWS Support. (Vous n'avez pas besoin de contrat de support, et il n'y a pas de frais.) Pour de plus amples informations, veuillez consulter Contacter le AWS Support à propos de problèmes d'enregistrement de domaine.

    > **Note**
    >
    > Les codes d'autorisation générés par Gandi sont valides pendant environ 5 jours. Si votre tentative de transfert a lieu après cette période, il est possible qu'elle échoue en raison d'un code expiré.

13. Si vous avez transféré le service DNS à un autre fournisseur de services DNS, vous pouvez supprimer les enregistrements dans la zone hébergée et supprimer la zone hébergée une fois que les résolveurs DNS ont cessé de répondre aux requêtes DNS en renvoyant les noms des serveurs de noms Route 53. Cette procédure dure généralement deux jours, le temps que les résolveurs DNS mettent en cache les noms des serveurs de noms pour un domaine.

> **Important**
>
> Si vous supprimez la zone hébergée alors que les résolveurs DNS continuent de répondre aux requêtes DNS en renvoyant les noms des serveurs de noms Route 53, votre domaine devient indisponible sur Internet.

Une fois la zone hébergée supprimée, Route 53 cesse de vous facturer les frais mensuels associés à une zone hébergée. Pour plus d'informations, consultez la documentation suivante :

- Suppression d'enregistrements
- Suppression d'une zone hébergée publique
- Tarification Route 53

Transfert du bureau d'enregistrement vers le bureau d'enregistrement Amazon

Amazon Route 53 Domains utilise deux bureaux d'enregistrement pour enregistrer les domaines des clients : Amazon Registrar, un bureau d'enregistrement détenu et géré par AWS, et Gandi, un bureau d'enregistrement associé avec lequel nous travaillons. Au départ, la plupart des domaines Route 53 étaient enregistrés via Gandi, car Amazon Registrar n'était pas directement accrédité pour de nombreux domaines de premier niveau (TLDs), tels que .com ou .club. Maintenant qu'Amazon Registrar est directement accrédité auprès de centaines TLDs (et ce nombre ne cesse de croître), nous allons commencer à transférer les domaines enregistrés via Gandi vers Amazon Registrar en votre nom.

Cela ne changera pas la façon dont vous gérez le domaine dans Route 53, cela mettra simplement à jour le bureau d'enregistrement de votre domaine de Gandi à Amazon Registrar. Le transfert aura lieu pendant le processus de renouvellement du domaine et seuls les frais de renouvellement standard s'appliqueront. Une fois le transfert terminé, les nouvelles demandes de transfert de votre domaine vers un nouveau bureau d'enregistrement extérieur AWS peuvent être retardées. Route 53 informera les titulaires de domaines concernés 15 jours avant le transfert lors du renouvellement. Ce processus est décrit dans notre accord d'enregistrement de nom de domaine (voir section 3.11.5).

Ce transfert est obligatoire si vous souhaitez continuer à utiliser le service Route 53 pour gérer vos domaines. Si vous ne souhaitez pas utiliser Amazon Registrar pour gérer votre domaine, vous devez

le transférer vers un autre bureau d'enregistrement dans les 15 jours suivant la réception de l'avis de transfert lors du renouvellement de AWS.

Renvoi des e-mails de confirmation et d'autorisation

Pour plusieurs opérations liées à l'enregistrement de domaine, l'ICANN exige d'avoir l'autorisation du contact inscrit pour le domaine ou une confirmation que l'adresse e-mail du contact inscrit est valide. Afin d'obtenir l'autorisation ou la confirmation, nous envoyons un e-mail qui contient un lien. Vous avez entre 3 et 15 jours pour cliquer sur le lien, selon l'opération et le domaine de premier niveau. Au-delà de ce délai, le lien ne fonctionne plus.

Si vous ne cliquez pas sur le lien figurant dans l'e-mail dans le temps imparti, l'ICANN exige généralement la suspension ou l'annulation de l'opération en cours, selon le cas :

Enregistrement d'un domaine

Nous suspendons le domaine, il n'est alors plus accessible sur Internet. Pour renvoyer l'e-mail de confirmation, consultez Pour renvoyer l'e-mail de confirmation pour un enregistrement de domaine.

Géographique TLDs uniquement — Transférez un domaine vers Amazon Route 53

Si vous transférez un domaine ayant un domaine de premier niveau (TLD) géographique, nous annulons le transfert. Pour renvoyer l'e-mail d'autorisation, consultez Pour renvoyer l'e-mail d'autorisation concernant un transfert de domaine.

> **Note**
>
> L'autorisation n'est pas obligatoire pour les domaines qui présentent un domaine de premier niveau (TLD) générique, par exemple .com, .net ou .org.

Modification du nom ou de l'adresse e-mail du contact inscrit pour le domaine (le propriétaire)

Nous annulons la modification. Pour renvoyer l'e-mail d'autorisation, consultez Pour renvoyer l'e-mail d'autorisation pour mettre à jour le contact inscrit ou supprimer un domaine.

Supprimer un domaine

Nous annulons la demande de suppression. Pour renvoyer l'e-mail d'autorisation, consultez Pour renvoyer l'e-mail d'autorisation pour mettre à jour le contact inscrit ou supprimer un domaine.

Géographique TLDs uniquement — Transférez un domaine de Route 53 vers un autre bureau d'enregistrement

Si vous transférez un domaine ayant un domaine de premier niveau (TLD) géographique, le nouveau bureau d'enregistrement annule le transfert.

> **Note**
>
> L'autorisation n'est pas obligatoire pour les domaines qui présentent un domaine de premier niveau (TLD) générique, par exemple .com, .net ou .org.

Rubriques

- Mise à jour de votre adresse électronique
- Renvoi d'e-mails

Mise à jour de votre adresse électronique

Nous envoyons toujours des e-mails de confirmation et d'autorisation à l'adresse électronique du contact inscrit pour un domaine. Dans certains cas TLDs, nous sommes tenus d'envoyer un e-mail à l'ancienne et à la nouvelle adresse e-mail du contact du titulaire dans les cas suivants :

- Vous modifiez l'adresse e-mail d'un domaine déjà enregistré auprès d'Amazon Route 53
- Vous modifiez l'adresse e-mail d'un domaine que vous transférez vers Route 53

Renvoi d'e-mails

Utilisez la procédure applicable pour renvoyer des e-mails de confirmation ou d'autorisation.

- Pour renvoyer l'e-mail de confirmation pour un enregistrement de domaine
- Pour renvoyer l'e-mail d'autorisation concernant un transfert de domaine
- Pour renvoyer l'e-mail d'autorisation pour mettre à jour le contact inscrit ou supprimer un domaine

Pour renvoyer l'e-mail de confirmation pour un enregistrement de domaine

1. Vérifiez que l'adresse e-mail du contact inscrit et, si nécessaire, mettez-la à jour. Pour de plus amples informations, veuillez consulter Mise à jour des informations de contact et de la propriété pour un domaine.
2. Recherchez dans le dossier de courrier indésirable de votre application de messagerie, un e-mail provenant de l'une des adresses e-mail suivantes.

   Si trop de temps s'est écoulé, le lien ne fonctionne plus, mais vous saurez à quel endroit rechercher l'e-mail de confirmation que nous vous renverrons.

TLDs	Adresse électronique émettrice de l'e-mail d'approbation ou de confirmation
.fr	nic@nic.fr
Tous les autres	Une des adresses e-mail suivantes : • noreply@registrar.amazon • noreply@domainnameverification.net

> **Note**
>
> Les e-mails peuvent contenir un lien vers www.verify-whois.com. Ce lien peut être utilisé en toute sécurité.

3. Utilisez la console Amazon Route 53 pour renvoyer l'e-mail de confirmation :
   a. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
   b. Dans le panneau de navigation, choisissez Registered domains (Domaines membres).
   c. Choisissez le nom du domaine pour lequel vous souhaitez renvoyer un e-mail.
   d. Dans la zone d'avertissement indiquant « votre domaine est peut-être suspendu », choisissez Envoyer un e-mail.

> **Note**
>
> Si aucune zone d'avertissement ne s'affiche, cela signifie que vous avez déjà confirmé que l'adresse e-mail du contact inscrit était valide.

4. Si vous rencontrez des problèmes lors du renvoi de l'e-mail de confirmation, vous pouvez contacter le AWS Support gratuitement. Pour de plus amples informations, veuillez consulter Contacter le AWS Support à propos de problèmes d'enregistrement de domaine.

Pour renvoyer l'e-mail d'autorisation concernant un transfert de domaine

Cette méthode ne fonctionne pas pour les demandes de transfert de domaine .jp.

1. Utilisez la méthode fournie par le bureau d'enregistrement de votre domaine actuel pour confirmer que la protection de la confidentialité du domaine est désactivée. Si ce n'est pas le cas, désactivez-la.

   Nous envoyons l'e-mail d'autorisation à l'adresse e-mail enregistrée dans la base de données WHOIS, par le bureau d'enregistrement actuel. Lorsque la protection de la confidentialité est activée, cette adresse e-mail est généralement cryptée. Le bureau d'enregistrement réel ne peut pas transférer, vers votre adresse e-mail réelle, l'e-mail qu'Amazon Route 53 envoie à l'adresse e-mail figurant dans la base de données WHOIS.

   > **Note**
   >
   > Si le bureau d'enregistrement actuel du domaine ne vous permet pas de désactiver la protection de la confidentialité, nous pouvons quand même transférer le domaine si vous avez spécifié un code d'autorisation valide à l'Étape 5 : Demander le transfert.

2. Vérifiez que l'adresse e-mail du contact inscrit et, si nécessaire, mettez-la à jour. Utilisez la méthode fournie par le bureau d'enregistrement actuel pour le domaine.
3. Recherchez dans le dossier de courrier indésirable de votre application de messagerie, un e-mail provenant de l'une des adresses e-mail suivantes.

   Si trop de temps s'est écoulé, le lien ne fonctionne plus, mais vous saurez à quel endroit rechercher l'e-mail d'autorisation que nous vous renverrons.

TLDs	Adresse électronique émettrice de l'e-mail d'approbation ou de confirmation
.com.au et .net.au	no-reply@ispapi.net L'e-mail contient un lien vers https://approve.domainadmin.com.
.fr	nic@nic.fr
Tous les autres	Une des adresses e-mail suivantes : • noreply@registrar.amazon • noreply@domainnameverification.net

> **Note**
>
> Les e-mails peuvent contenir un lien vers www.verify-whois.com. Ce lien peut être utilisé en toute sécurité.

4. Si le transfert est interrompu (si nous l'avons annulé, car un laps de temps trop important s'est écoulé), redemandez le transfert et nous enverrons un autre e-mail d'autorisation.

> **Note**
>
> Dans les 15 premiers jours suivant la demande de transfert, vous pouvez déterminer le statut du transfert en vérifiant le tableau Notifications dans la page Dashboard Tableau de bord de la console Route 53. Après 15 jours, utilisez le AWS CLI pour obtenir le statut. Pour de plus amples informations, consultez route53domains dans la Référence de commande AWS CLI .

Si le transfert est en cours d'exécution, effectuez les opérations suivantes pour renvoyer l'e-mail d'autorisation.

a. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.

b. Dans le tableau Notifications, recherchez le domaine que vous souhaitez transférer.

c. Dans la colonne Status (État) pour ce domaine, choisissez Resend email (Renvoyer un e-mail).

5. Si vous rencontrez des problèmes lors du renvoi de l'e-mail d'autorisation pour un transfert de domaine, vous pouvez contacter le AWS Support gratuitement. Pour de plus amples informations, veuillez consulter Contacter le AWS Support à propos de problèmes d'enregistrement de domaine.

Pour renvoyer l'e-mail d'autorisation pour mettre à jour le contact inscrit ou supprimer un domaine

1. Vérifiez que l'adresse e-mail du contact inscrit et, si nécessaire, mettez-la à jour. Pour de plus amples informations, veuillez consulter Mise à jour des informations de contact et de la propriété pour un domaine.
2. Recherchez dans le dossier de courrier indésirable de votre application de messagerie, un e-mail provenant de l'une des adresses e-mail suivantes.

   Si trop de temps s'est écoulé, le lien ne fonctionne plus, mais vous saurez à quel endroit rechercher l'e-mail d'autorisation que nous vous renverrons.

TLDs	Adresse électronique qui envoie l'e-mail d'autorisation
.fr	nic@nic.fr
Tous les autres	Une des adresses e-mail suivantes : • noreply@registrar.amazon • noreply@domainnameverification.net

> **Note**
>
> Les e-mails peuvent contenir un lien vers www.verify-whois.com. Ce lien peut être utilisé en toute sécurité.

3. Annulez la modification ou la suppression. Vous avez deux options :
   - Vous pouvez attendre la fin de la période de 3 à 15 jours, au-delà de laquelle nous annulons automatiquement l'opération demandée.
   - Vous pouvez également contacter le AWS Support et lui demander d'annuler l'opération.
4. Une fois que la modification ou la suppression est annulée, vous pouvez modifier les informations sur le contact ou supprimer le domaine à nouveau, et nous vous enverrons un autre e-mail d'autorisation.
5. Si vous rencontrez des problèmes lors du renvoi de l'e-mail d'autorisation, vous pouvez contacter le AWS Support gratuitement. Pour de plus amples informations, veuillez consulter Contacter le AWS Support à propos de problèmes d'enregistrement de domaine.

Configuration du protocole DNSSEC pour un domaine

Les pirates informatiques détournent parfois le trafic vers des points de terminaison Internet, par exemple des serveurs web. Ils interceptent des requêtes DNS et renvoient leurs propres adresses IP aux résolveurs DNS à la place des adresses IP réelles de ces points de terminaison. Les utilisateurs sont ensuite dirigés vers les adresses IP fournies par les pirates dans la réponse usurpée, par exemple, vers de faux sites web.

Vous pouvez protéger votre domaine contre ce type d'attaque, connu sous le nom d'usurpation du DNS ou d' man-in-the-middleattaque, en configurant les extensions de sécurité du système de noms de domaine (DNSSEC), un protocole destiné à sécuriser le trafic DNS.

> **Important**
>
> Amazon Route 53 prend en charge la signature DNSSEC et DNSSEC pour l'enregistrement de domaine. Si vous souhaitez configurer la signature DNSSEC pour un domaine enregistré avec Route 53, consultez Configuration de la signature DNSSEC dans Amazon Route 53.

Rubriques

- Vue d'ensemble de la protection de votre domaine grâce au protocole DNSSEC
- Prérequis et limites maximales de la configuration du protocole DNSSEC pour un domaine
- Ajout de clés publiques pour un domaine
- Suppression de clés publiques pour un domaine

Vue d'ensemble de la protection de votre domaine grâce au protocole DNSSEC

Lorsque vous configurez le protocole DNSSEC pour votre domaine, un résolveur DNS établit une chaîne de confiance pour les réponses des résolveurs intermédiaires. La chaîne de confiance commence par le registre TLD pour le domaine (la zone parent de votre domaine) et se termine par les serveurs de noms faisant autorité de votre fournisseur de services DNS. Tous les résolveurs DNS ne prennent pas en charge le protocole DNSSEC. Seuls les résolveurs qui prennent en charge DNSSEC peuvent signer ou effectuer la validation de l'authenticité.

Voici la procédure simplifiée pour configurer le protocole DNSSEC pour les domaines enregistrés avec Amazon Route 53 afin de protéger vos hôtes Internet de l'usurpation DNS :

1. Utilisez la méthode fournie par votre fournisseur de services DNS pour signer les enregistrements de votre zone hébergée avec la clé privée d'une paire de clés asymétrique.

   > **Important**
   >
   > Route 53 prend en charge la signature DNSSEC et DNSSEC pour l'enregistrement de domaine. Pour en savoir plus, veuillez consulter la section Configuration de la signature DNSSEC dans Amazon Route 53.

2. Fournissez la clé publique de la paire de clés de votre bureau d'enregistrement de domaine et spécifiez l'algorithme utilisé pour générer la paire de clés. Le registre de domaine transmet la clé publique et l'algorithme au registre pour le domaine de premier niveau (TLD).

   Pour plus d'informations sur la façon d'effectuer cette étape pour des domaines que vous avez enregistrés avec Route 53, consultez Ajout de clés publiques pour un domaine.

Une fois que vous avez configuré le protocole DNSSEC, voici comment le protocole protège votre domaine de l'usurpation DNS :

1. Envoyez une requête DNS, par exemple en accédant à un site web ou en envoyant un message électronique.
2. La demande est acheminée vers un résolveur DNS. Les résolveurs sont chargés de renvoyer la valeur appropriée vers les clients en fonction de la demande, par exemple, l'adresse IP de l'hôte qui exécute un serveur web ou un serveur de messagerie.
3. Si l'adresse IP est mise en cache sur le résolveur DNS car la même requête DNS a déjà été envoyée et que le résolveur a déjà obtenu la valeur, le résolveur renvoie l'adresse IP au client qui a envoyé la demande. Le client utilise ensuite l'adresse IP pour accéder à l'hôte.

   Si l'adresse IP n'est pas mise en cache sur le résolveur DNS, le résolveur envoie une demande à la zone parent de votre domaine, au registre TLD, qui renvoie deux valeurs :

   - L'enregistrement Delegation Signer (DS), clé publique qui correspond à la clé privée qui a été utilisée pour signer l'enregistrement.
   - Les adresses IP des serveurs de noms faisant autorité pour votre domaine.
4. Le résolveur DNS envoie la demande d'origine à un autre résolveur DNS. Si ce résolveur n'a pas d'adresse IP, il répète le processus jusqu'à ce qu'un résolveur envoie la demande vers un serveur de noms de votre fournisseur de services DNS. Le serveur de noms renvoie deux valeurs :

   - L'enregistrement pour le domaine, par exemple example.com. Généralement, ce jeu contient l'adresse IP d'un hôte.
   - La signature pour l'enregistrement, que vous avez créée lorsque vous avez configuré le protocole DNSSEC.
5. Le résolveur DNS utilise la clé publique, que vous avez fournie au bureau d'enregistrement de domaine et que celui-ci a transmis au registre TLD, pour effectuer deux actions :

   - Etablir une chaîne de confiance
   - Vérifier que la réponse signée à partir du fournisseur de services DNS est légitime et qu'elle n'a pas été remplacée par une mauvaise réponse par un pirate informatique
6. Si la réponse est authentique, le résolveur renvoie la valeur au client qui a envoyé la demande.

   Si la réponse ne peut pas être vérifiée, le résolveur renvoie une erreur à l'utilisateur.

   Si le registre TLD pour le domaine n'a pas la clé publique du domaine, le résolveur répond à la requête DNS à l'aide de la réponse renvoyée par le fournisseur de services DNS.

Prérequis et limites maximales de la configuration du protocole DNSSEC pour un domaine

Pour configurer le protocole DNSSEC pour un domaine, votre fournisseur de domaine et votre fournisseur de services DNS doivent répondre aux exigences suivantes :

- Le registre pour le TLD doit prendre en charge le protocole DNSSEC. Pour déterminer si le registre pour votre domaine de premier niveau prend en charge le protocole DNSSEC, consultez Domaines que vous pouvez enregistrer avec Amazon Route 53.
- Le fournisseur de services DNS du domaine doit prendre en charge le protocole DNSSEC.

> **Important**
>
> Route 53 prend en charge la signature DNSSEC et DNSSEC pour l'enregistrement de domaine. Pour en savoir plus, veuillez consulter la section Configuration de la signature DNSSEC dans Amazon Route 53.

- Vous devez configurer le protocole DNSSEC avec le fournisseur de services DNS pour votre domaine avant d'ajouter des clés publiques pour le domaine à Route 53.
- Le nombre de clés publiques que vous pouvez ajouter à un domaine varie selon le domaine de premier niveau pour le domaine :
  - Domaines .com et .net – Jusqu'à treize clés
  - Tous les autres domaines – Jusqu'à quatre clés

Ajout de clés publiques pour un domaine

Lorsque vous effectuez une rotation des clés ou que vous activez le protocole DNSSEC pour un domaine, exécutez la procédure suivante après avoir configuré le protocole DNSSEC avec le fournisseur de services DNS du domaine.

Pour ajouter des clés publiques à un domaine

1. Si vous n'avez pas déjà configuré le protocole DNSSEC avec votre fournisseur de services DNS, utilisez la méthode fournie par ce dernier pour le configurer.
2. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.

3. Dans le panneau de navigation, choisissez Registered domains (Domaines membres).
4. Choisissez le nom du domaine pour lequel vous souhaitez ajouter des clés.
5. Choisissez l'onglet Clés DNSSEC, puis Ajouter une clé.
6. Indiquez l'une des valeurs suivantes :

   Type de clé

   Indiquez si vous souhaitez charger une clé KSK ou une clé ZSK.

   Algorithm

   Sélectionnez l'algorithme que vous avez utilisé pour valider les enregistrements pour la zone hébergée.

   Clé publique

   Spécifiez la clé publique de la paire de clés asymétrique que vous avez utilisée pour configurer le protocole DNSSEC avec votre fournisseur de services DNS.

   Remarques :

   - Spécifiez la clé publique, pas le hachage.
   - Vous devez spécifier la clé au format base64.
7. Choisissez Ajouter.

   > **Note**
   >
   > Vous pouvez seulement ajouter une clé publique à la fois. Si vous avez besoin d'ajouter plusieurs clés, patientez jusqu'à réception d'un e-mail de confirmation de la part de Route 53.

8. Lorsque Route 53 reçoit une réponse du registre, nous envoyons un e-mail au contact inscrit. L'e-mail confirme que la clé publique a été ajoutée au domaine au niveau du registre ou explique pourquoi la clé n'a pas pu être ajoutée.

Suppression de clés publiques pour un domaine

Lorsque vous effectuez une rotation des clés ou que vous désactivez le protocole DNSSEC pour le domaine, supprimez les clés publiques à l'aide de la procédure suivante avant de désactiver le protocole DNSSEC avec votre fournisseur de services DNS. Remarques :

- Si vous effectuez une rotation des clés publiques, nous vous recommandons d'attendre jusqu'à trois jours après l'ajout de nouvelles clés publiques avant de supprimer les anciennes clés publiques.
- Si vous désactivez le protocole DNSSEC, commencez par supprimer les clés publiques pour le domaine. Nous vous recommandons d'attendre jusqu'à trois jours avant de désactiver le protocole DNSSEC avec le service DNS pour le domaine.

> **Important**
>
> Si le protocole DNSSEC est activé pour le domaine et si vous le désactivez avec le service DNS, les résolveurs DNS qui le prennent en charge renverront une erreur `SERVFAIL` aux clients. Ces derniers ne seront pas en mesure d'accéder aux points de terminaison qui sont associés au domaine.

Pour supprimer des clés publiques d'un domaine

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le panneau de navigation, choisissez Registered domains (Domaines membres).
3. Choisissez le nom du domaine pour lequel vous souhaitez supprimer des clés.
4. Dans l'onglet Clés DNSSEC, choisissez la case d'option en regard de la clé à supprimer, puis choisissez Supprimer la clé.
5. Dans la boîte de dialogue Supprimer la clé DNSSEC, entrez supprimer dans la zone de texte pour confirmer que vous souhaitez supprimer la clé, puis choisissez Supprimer.

   > **Note**
   >
   > Vous pouvez seulement supprimer une clé publique à la fois. Si vous avez besoin de supprimer plusieurs clés, patientez jusqu'à réception d'un e-mail de confirmation de la part d'Amazon Route 53.

6. Lorsque Route 53 reçoit une réponse du registre, nous envoyons un e-mail au contact inscrit. L'e-mail confirme que la clé publique a été supprimée du domaine au niveau du registre ou explique pourquoi la clé n'a pas pu être supprimée.

Trouver votre bureau d'enregistrement et d'autres informations concernant votre domaine

Pour afficher les informations du domaine à l'aide de l'GetDomainDetailAPI, vous pouvez utiliser n'importe lequel des SDKs ou AWS CLI. Pour de plus amples informations, veuillez consulter get-domain-detail.

Pour afficher des informations sur les domaines avec **`get-domain-detail`** CLI

- Utilisez la commande CLI suivante :

```
aws route53domains get-domain-detail \
    --region us-east-1 \
    --domain-name example.com
```

> **Note**
>
> Cette commande ne s'exécute que dans us-east-1 Région AWS.

Toutes les informations concernant votre domaine seront répertoriées dans la sortie, y compris le bureau d'enregistrement, la date d'enregistrement, les paramètres de confidentialité, etc.

Affichage des informations sur les domaines enregistrés auprès de Route 53

Vous pouvez afficher des informations sur les domaines qui ont été enregistrés à l'aide de Route 53. Ces informations incluent des détails tels que la date d'enregistrement initial du domaine et les coordonnées du propriétaire du domaine et des contacts techniques, administratifs et de facturation.

WHOIS

Le WHOIS est un annuaire gratuit accessible au public contenant des informations sur les domaines sponsorisés par les bureaux d'enregistrement et les registres de domaines. Il est fourni à la fois en tant que service acceptant les requêtes sur le port 43 et en tant que site Web, chacun étant

accessible via IPv4 les deux IPv6. Le WHOIS est une recherche hiérarchique distribuée. Pour en savoir plus, consultez À propos de WHOIS.

Une demande WHOIS adressée à différents niveaux de la hiérarchie peut fournir différentes informations :

- Une demande adressée au WHOIS racine (whois.iana.org) fournit des informations sur le registre.
- Une demande d'enregistrement du WHOIS fournit des informations sur le bureau d'enregistrement et sur certaines informations publiques sur le domaine.
- Une demande adressée au bureau d'enregistrement WHOIS fournit toutes les informations publiques sur le domaine.

Étant donné qu'il existe plusieurs niveaux de WHOIS, y compris des recherches WHOIS effectuées par le registre TLD et le bureau d'enregistrement de domaines, la désactivation de votre protection de la confidentialité sur la console Route 53 peut uniquement la désactiver sur le WHOIS fourni par le bureau d'enregistrement. Certains registres maintiennent intentionnellement des services de protection de la vie privée ou de rédaction pour leurs services de recherche dans le WHOIS, que vous les ayez ou non désactivés avec Route 53. Pour obtenir des informations complètes sur votre domaine, nous vous recommandons d'utiliser le WHOIS fourni par le bureau d'enregistrement.

Remarques :

Envoi d'e-mails aux contacts du domaine en cas d'activation de la protection de la confidentialité

Si la protection de la confidentialité est activée pour le domaine, les informations de contact pour l'inscrit, et les contacts techniques et administratifs sont remplacés par les informations de contact pour le service de confidentialité du bureau d'enregistrement Amazon. Par exemple, si le domaine exemple.com est enregistré auprès du bureau d'enregistrement Amazon et si la protection de la confidentialité est activée, la valeur d'adresse e-mail de l'inscrit dans la réponse à une requête WHOIS sera similaire à propriétaire1234@exemple.com.protection-identité.org.

Pour communiquer avec un ou plusieurs contacts de domaine lorsque la protection de confidentialité est activée, envoyez un e-mail aux adresses e-mail correspondantes. Nous transmettons automatiquement votre e-mail aux contacts concernés.

Signaler des abus

Pour signaler toute activité illégale ou violation de la Politique d'utilisation acceptable, y compris un contenu inapproprié, un hameçonnage, un logiciel malveillant ou un spam, envoyez un e-mail à trustandsafety@support.aws.com.

Pour afficher des informations sur les domaines enregistrés auprès de Route 53

1. Dans un navigateur web, accédez à l'un des sites web suivants :
   - WHOIS du bureau d'enregistrement Amazon : https://registrar.amazon.com /whois
   - Amazon Registrar RDAP : https://registrar.amazon.com /rdap
   - WHOIS de Gandi : https://whois.gandi.net
2. Entrez le nom du domaine sur lequel vous souhaitez afficher des informations, puis choisissez Search (Rechercher).

Suppression d'un enregistrement de nom de domaine

Pour la plupart des domaines de premier niveau (TLDs), vous pouvez supprimer l'enregistrement si vous ne le souhaitez plus. Si le registre vous permet de supprimer l'enregistrement, exécutez la procédure de cette rubrique.

Remarques :

Les frais d'inscription ne sont pas remboursables

Si vous supprimez un enregistrement de nom de domaine avant la date d'expiration prévue de l'enregistrement, AWS ne rembourse pas les frais d'enregistrement.

TLDs qui vous permettent de supprimer un enregistrement de domaine

Pour déterminer si vous pouvez supprimer l'enregistrement de votre domaine, consultez Domaines que vous pouvez enregistrer avec Amazon Route 53. Si la section de votre TLD n'inclut pas une sous-section « Suppression de l'enregistrement de domaine », vous pouvez supprimer le domaine. Avant de supprimer le domaine, assurez-vous que le verrouillage de domaine est désactivé. Pour plus d'informations sur la désactivation du verrouillage de domaine, consultez DisableDomainTransferLock.

Que se passe-t-il si vous ne pouvez pas supprimer un enregistrement de domaine ?

Si le registre de votre domaine ne vous permet pas de supprimer un enregistrement de nom de domaine, vous devez attendre que le domaine expire. Pour vous assurer que le domaine n'est pas renouvelé automatiquement, désactivez le renouvellement automatique pour ce domaine. À la date d'expiration indiquée dans le champ Expires on (Expire le), Route 53 supprime automatiquement l'enregistrement du domaine. Pour plus d'informations sur la modification

du paramètre de renouvellement automatique, consultez Activation ou désactivation du renouvellement automatique pour un domaine.

Délai avant la suppression d'un domaine et sa disponibilité pour être enregistré à nouveau

Presque tous les registres empêchent l'enregistrement immédiat d'un domaine qui vient d'expirer. En général, le délai est d'un à trois mois, selon le domaine de premier niveau (TLD). Pour plus d'informations, consultez la section « Délais pour le renouvellement et la restauration de domaines » pour votre TLD dans Domaines que vous pouvez enregistrer avec Amazon Route 53.

> **Important**
>
> Ne supprimez pas un domaine et attendez-vous à le réenregistrer si vous souhaitez simplement transférer le domaine entre AWS comptes ou le transférer vers un autre bureau d'enregistrement. Consultez la documentation correspondante :
>
> - Transférer un domaine vers un autre AWS compte
> - Transfert d'un domaine depuis Amazon Route 53 vers un autre bureau d'enregistrement

Pour supprimer un enregistrement de nom de domaine

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le panneau de navigation, choisissez Registered domains (Domaines membres).
3. Choisissez le nom de votre domaine.

   Si vous souhaitez supprimer un domaine .co.uk, .me.uk, .org.uk ou .uk, consultez Pour supprimer les enregistrements de noms de domaine .co.uk, .me.uk, .org.uk et .uk.
4. Si le registre de votre domaine de premier niveau permet la suppression d'un nom de domaine, choisissez Supprimer le domaine.

   Certains domaines peuvent exiger que nous envoyons un e-mail au contact inscrit du domaine afin de vérifier qu'il souhaite supprimer le domaine. Si vous recevez un e-mail, il proviendra de l'une des adresses e-mail suivantes :

   - noreply@registrar.amazon — pour les personnes TLDs enregistrées auprès d'Amazon Registrar.

- noreply@domainnameverification.net — pour les TLDs inscriptions auprès de notre associé au bureau d'enregistrement, Gandi.

Pour déterminer le bureau d'enregistrement pour votre domaine de premier niveau, consultez Domaines que vous pouvez enregistrer avec Amazon Route 53.

5. Si vous recevez l'e-mail de vérification, cliquez sur le lien présent dans l'e-mail, puis approuvez ou rejetez la demande de suppression du domaine.

> **Important**
>
> Le contact du titulaire doit immédiatement suivre les instructions contenues dans l'e-mail, ou nous devons annuler la demande de suppression au plus tard un jour, comme l'exige l'ICANN.

Vous recevrez un autre e-mail lorsque votre domaine aura été supprimé. Pour déterminer l'état actuel de votre demande, consultez Affichage du statut de l'enregistrement d'un domaine.

6. Supprimez les enregistrements dans la zone hébergée du domaine supprimé, puis supprimez la zone hébergée. Une fois la zone hébergée supprimée, Route 53 cesse de vous facturer les frais mensuels associés à une zone hébergée. Pour plus d'informations, consultez la documentation suivante :

   - Suppression d'enregistrements
   - Suppression d'une zone hébergée publique
   - Tarification Route 53

7. Si vous rencontrez des problèmes lors de la suppression de l'enregistrement d'un nom de domaine, vous pouvez contacter le AWS Support gratuitement. Pour de plus amples informations, veuillez consulter Contacter le AWS Support à propos de problèmes d'enregistrement de domaine.

Pour supprimer les enregistrements de noms de domaine .co.uk, .me.uk, .org.uk et .uk

Si vous souhaitez supprimer un domaine .co.uk, .me.uk, .org.uk ou .uk, vous devez créer un compte auprès de Nominet, le registre des domaines .uk. Pour plus d'informations, consultez « Cancelling your domain name » sur le site web de Nominet, https://www.nominet.uk/domain-support/.

> **Important**
>
> Si vous supprimez (annulez) un nom de domaine .uk, il sera supprimé au bout de quelques jours et pourra être enregistré par tout le monde. Si vous voulez simplement transférer le domaine, ne le supprimez pas.

Voici la procédure générale :

1. Sur le site de Nominet, suivez les instructions pour vous connecter la première fois. Consultez https://secure.nominet.org.uk/auth/login.html. Nominet vous envoie un e-mail avec des instructions pour créer un mot de passe.
2. Suivez les instructions contenues dans l'e-mail envoyé par Nominet.
3. Connectez-vous au site web Nominet et suivez les instructions pour annuler (supprimer) un nom de domaine.

Contacter le AWS Support à propos de problèmes d'enregistrement de domaine

AWS propose un plan d'assistance de base, gratuit, à tous les AWS clients. Le programme comprend une assistance pour les problèmes suivants liés à l'enregistrement de domaine :

- Transfert de domaines à ou depuis Amazon Route 53
- Transfert de domaines entre AWS comptes
- Augmentation des quotas applicables aux entités Route 53, tels que le nombre de domaines que vous pouvez enregistrer (consultez Quotas).
- Modification du propriétaire d'un domaine
- Modification des informations de contact pour le propriétaire d'un domaine
- Renvoi des e-mails de confirmation et d'autorisation
- Renouvellement de domaines
- Restauration de domaines expirés
- Obtention d'informations sur la facturation Route 53
- Fourniture d'une preuve d'identité pour les domaines .uk

- Supprimer des domaines ou désactiver le renouvellement automatique après la fermeture de votre compte AWS

Pour contacter le AWS Support à propos de ces problèmes et d'autres liés à l'enregistrement de domaines, suivez la procédure applicable.

Rubriques

- Contacter AWS le Support lorsque vous pouvez vous connecter à votre AWS compte
- Contacter AWS le Support lorsque vous ne parvenez pas à vous connecter à votre AWS compte

Contacter AWS le Support lorsque vous pouvez vous connecter à votre AWS compte

Pour contacter le AWS Support lorsque vous serez en mesure de vous connecter à votre AWS compte, effectuez la procédure suivante :

1. À l'aide du AWS compte sur lequel le domaine est actuellement enregistré, connectez-vous au AWS Support.

   > **Important**
   >
   > Vous devez vous connecter l'aide du compte racine auquel le domaine est actuellement enregistré. Cette exigence empêche les utilisateurs non autorisés de détourner votre compte.

2. Choisissez le compte et la facturation
3. Indiquez l’une des valeurs suivantes :

   Regarding

   Acceptez la valeur par défaut Account and Billing Support.

   Service

   Acceptez la valeur par défaut de Domains.

   Catégorie

   Acceptez la valeur par défaut de Registration Issue.

Sévérité

Choisissez la gravité applicable.

Sujet

Entrez un bref résumé du problème.

Description

Décrivez le problème que vous avez plus en détail et joignez les captures d'écran ou documents pertinents.

Contact method

Choisissez la méthode de contact, Web. Nous vous contacterons à l'aide de l'adresse e-mail associée à votre AWS compte.

4. Sélectionnez Envoyer.

Contacter AWS le Support lorsque vous ne parvenez pas à vous connecter à votre AWS compte

Pour contacter le AWS Support lorsque vous ne parvenez pas à vous connecter à votre AWS compte, effectuez la procédure suivante :

1. Accédez à la page Je suis AWS client et je recherche une solution de facturation ou d'assistance relative à mon compte.
2. Remplissez le formulaire.
3. Sélectionnez Envoyer.

Téléchargement d'un rapport de facturation de domaine

Si vous gérer plusieurs domaines et si vous souhaitez afficher les frais par domaine pour une durée déterminée, vous pouvez télécharger un rapport de facturation de domaine. Ce rapport indique tous les frais qui s'appliquent à l'enregistrement de domaine, y compris les éléments suivants :

- Enregistrement d'un domaine
- Renouvellement d'un enregistrement de domaine
- Transfert d'un domaine vers Amazon Route 53

- Changer le propriétaire d'un domaine (pour certains TLDs, cette opération est gratuite)

Parfois, votre rapport de facturation peut indiquer des périodes de facturation ultérieures. Cela se produit parce que le processus de renouvellement automatique du domaine commence le mois précédant l'expiration du domaine. Par conséquent, par exemple, dans votre rapport du mois d'août, vous pouvez voir une période de facturation qui commence le mois de septembre suivant et se termine en septembre de l'année suivante.

Lorsque vous exécutez le rapport à l'aide de la console, vous pouvez choisir les options suivantes :

- Last 12 months (12 derniers mois) : le rapport inclut les frais remontant à un an par rapport à la date à laquelle vous avez exécuté le rapport. Par exemple, si vous exécutez le rapport le 3 juin, il inclut les frais à partir du 3 juin de l'année précédente jusqu'à la date du jour.
- Individual months in the last year (Mois individuels de la dernière année): le rapport inclut les frais pour le mois spécifié.

Si vous exécutez le rapport par programme, vous pouvez générer les frais pour n'importe quelle plage de dates, à compter du 31 juillet 2014. Il s'agit de la date à partir de laquelle Route 53 a commencé à prendre en charge l'enregistrement de domaine. Par exemple, consultez view-billing dans la Référence des commandes AWS CLI .

Le rapport de facturation est au format CSV et son contenu est décrit par l'ViewBillingAPI.

Pour télécharger un rapport de facturation de domaine

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le panneau de navigation, sélectionnez Registered Domains (Domaines enregistrés).
3. Choisissez Domain billing report.
4. Sélectionnez la plage de dates pour le rapport, puis sélectionnez Download domain report.
5. Suivez les instructions pour ouvrir le rapport ou l'enregistrer.
6. Si vous rencontrez des problèmes lors du téléchargement d'un rapport de facturation de domaine, vous pouvez contacter le AWS Support gratuitement. Pour de plus amples informations, veuillez consulter Contacter le AWS Support à propos de problèmes d'enregistrement de domaine.

Domaines que vous pouvez enregistrer avec Amazon Route 53

> **Important**
>
> Les restrictions relatives aux domaines de premier niveau ci-dessous s'appliquent uniquement à l'enregistrement de domaines. Vous pouvez utiliser le service DNS Route 53 avec n'importe quel domaine de premier niveau de votre choix et avec n'importe quel bureau d'enregistrement de domaines. Les informations de cette page concernent uniquement les domaines que vous pouvez enregistrer auprès de Route 53. Pour plus d'informations sur Route 53 en tant que service DNS, consultez Acheminement du trafic Internet vers votre site web ou votre application web.

Les listes suivantes de domaines génériques et géographiques de premier niveau indiquent les domaines de premier niveau (TLDs) que vous pouvez utiliser pour enregistrer des domaines auprès d'Amazon Route 53.

Enregistrement de domaines via Route 53

Les registres TLD ont attribué des tarifs spéciaux ou premium à certains noms de domaine. Vous ne pouvez pas utiliser Route 53 pour enregistrer un domaine qui dispose d'un tarif spécial ou premium. Les TLDs informations que vous pouvez enregistrer auprès de Route 53 sont incluses dans les listes suivantes. Si le TLD n'est pas inclus, vous ne pouvez pas enregistrer le domaine avec Route 53.

Transfert de domaines vers Route 53

Vous pouvez transférer un domaine vers Route 53 si le domaine de premier niveau (TLD) est inclus dans les listes suivantes. Si le TLD n'est pas inclus, vous ne pouvez pas transférer le domaine vers Route 53.

Dans la plupart des cas TLDs, vous devez obtenir un code d'autorisation auprès du bureau d'enregistrement actuel pour transférer un domaine. Pour déterminer si vous avez besoin d'un code d'autorisation, consultez la section « Code d'autorisation requis pour les transferts » de votre TLD.

Tarification de transfert et d'enregistrement de domaines

Pour plus d'informations sur le coût d'enregistrement d'un domaine ou leur transfert vers Route 53, consultez Tarification Amazon Route 53 pour l'enregistrement de domaine.

Utilisation de Route 53 en tant que service DNS

Vous pouvez utiliser Route 53 en tant que service DNS pour tout domaine, même si le domaine de premier niveau (TLD) n'est pas inclus dans les listes suivantes. Pour plus d'informations sur Route 53 en tant que service DNS, consultez Acheminement du trafic Internet vers votre site web ou votre application web. Pour plus d'informations sur le transfert d'un service DNS pour votre domaine vers Route 53, consultez Configuration d'Amazon Route 53 en tant que service DNS d'un domaine existant.

Noms de domaine internationaux

Tous ne prennent pas TLDs en charge les noms de domaine internationalisés (IDNs), c'est-à-dire les noms de domaine contenant des caractères autres que les caractères ASCII a-z, 0-9 et - (tiret). La liste de chaque TLD indique si ce TLD est compatible. IDNs Pour plus d'informations sur les noms de domaine internationaux, consultez Format de nom de domaine DNS.

Enregistrement de domaines géographiques auprès de TLDs

Les règles d'enregistrement géographique TLDs varient selon les pays. Certains pays n'imposent pas de restriction, ce qui signifie que n'importe qui dans le monde peut utiliser l'extension, tandis que d'autres imposent certaines conditions, par exemple la résidence. La liste de chaque TLD géographique indique toutes les restrictions.

Index vers les domaines de premier niveau pris en charge

Rubriques

- Domaines de premier niveau génériques
- Domaines géographiques de premier niveau

Domaines de premier niveau génériques

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | WXYZ

A

.ac, .academy, .accountants, .actor, .adult, .agency, .airforce, .apartments, .associates, .auction, .audio

B

.band, .bargains, .bière,.bet, .bid, .bike, .bingo, .biographie, .biz, black, .blue, .boutique, .builders, .business, .buzz

C

.cab, .cafe, .camera, .camp, .capital, .cards, .care, .careers, .cash, .casino, .catering, .cc, .center, .ceo, .chat, .cheap, .noël, .church, .city, .claims, .cleaning, .click, .clinic, .clothing, .cloud, .club, .coach, .codes, .coffee, .college, .com, .community, .company, .computer, .condos, .construction, .consulting, .contacter, .contractors, .cool, .coupons, .credit, .creditcard, .cruises

D

.dance, .dating, .deals, .degree, .delivery, .democrat, .dental, .design, .diamonds, .diet, .digital, .direct, .directory, .discount, .dog, .domains

E

.education, .email, .energy, .engineering, .enterprises, .equipment, .estate, .events, .exchange, .expert, .exposed, .express

F

.fail, .ventilateur, .farm, .finance, .financial, .fish, .fitness, .flights, .florist, .flowers, .fm, .football, .forsale, .foundation, .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, .healthcare, .help, .hiv, .hockey, .holdings, .holiday, .host, .hosting, .house

I

.im, .immo, .immobilien, .industries, .info, .ink, .institute, .insure, .international, .investments, .io, .irish

J

.jewelry, .juegos

K

.kaufen, .kim, .kitchen, .kiwi

L

.land, .droit, .lease, .legal, .lgbt, .life, .lighting, .limited, .limo, .link, .live, .llc, .loan, .loans, .lol, .ltd

M

.maison, .management, .marketing, .mba, .media, .memorial, .mobi, .moda, .money, .mortgage, .movie

N

.name, .net, .network, .news, .ninja

O

.onl, .online, .org

P

.partners, .parts, .photo, .photography, .photos, .pics, .pictures, .pink, .pizza, .place, .plumbing, .plus, .poker, .porn, .press, .pro, .productions, .properties, .property, .pub. .pw (Palaos)

Q

.qpon

R

.recipes, .red, .reise, .reisen, .rentals, .repair, .report, .republican, .restaurant, .reviews, .rip, .rocks, .run

S

.sale, .sarl, .school, .schule, .services, .sex, .sexy, .shiksha, .shoes, .achats, .show, .singles, .site, .ski, .soccer, .social, .solar, .solutions, .logiciel, .space, .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, .voter, .voyage

WXYZ

.watch, .website, .wedding, .wiki, .wine, .travail, .works, .world, .wtf, .xyz, .zone

Domaines géographiques de premier niveau

Afrique

.ac (Ile de l'Ascension), .co.za (Afrique du Sud), .sh (Sainte-Hélène)

Amériques

.ca (Canada), .cl (Chili), .co (Colombie), .com.ar (Argentine), .com.br (Brésil), com.mx (Mexique), .mx (Mexique), .us (États-Unis), .vc (Saint-Vincent-et-les-Grenadines), .vg (Iles Vierges Britanniques)

Asie/Océanie

.au (Australie), .cc (Iles Coco), .co.nz (Nouvelle-Zélande), .com.au (Australie), .com.sg (République de Singapour), .fm (États fédérés de Micronésie), .in (Inde), .jp (Japon), .io (Territoire Britannique de l'Océan Indien), .net.au (Australie), .net.nz (Nouvelle-Zélande), .org.nz (Nouvelle-Zélande), .pw (Palaos), .qa (Qatar), .ru (Fédération de Russie), .sg (République de Singapour)

Europe

.be (Belgique), .berlin (ville de Berlin en Allemagne), .ch (Suisse), .co.uk (Royaume-Uni), .cz (République tchèque), .de (Allemagne), .es (Espagne) , .eu (Union européenne), .fi (Finlande), .fr (France), .gg (Guernesey), .im (Ile de Man), .it (Italie), .me (Monténégro), .me.uk (Royaume-Uni), .nl (Pays-Bas), .org.uk (Royaume-Uni), .ruhr (région de la Ruhr, ouest de l'Allemagne), .se (Suède), .uk (Royaume-Uni), .wien (ville de Vienne en Autriche)

Domaines de premier niveau génériques

Les domaines génériques de premier niveau (gTLDs) sont des extensions globales utilisées et reconnues dans le monde entier, telles que .com, .net et .org. Ils comprennent également des domaines spécialisés comme .bike, .condos et .marketing.

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | WXYZ

A

.ac, .academy, .accountants, .actor, .adult, .agency, .airforce, .apartments, .associates, .auction, .audio

B

.band, .bargains, .bière, .bet, .bid, .bike, .bingo, .biographie, .biz, black, .blue, .boutique, .builders, .business, .buzz

C

.cab, .cafe, .camera, .camp, .capital, .cards, .care, .careers, .cash, .casino, .catering, .cc, .center, .ceo, .chat, .cheap, .church, .noël, .city, .claims, .cleaning, .click, .clinic, .clothing, .cloud, .club, .coach, .codes, .coffee, .college, .com, .community, .company, .computer, .condos, .construction, .consulting, .contacter, .contractors, .cool, .coupons, .credit, .creditcard, .cruises

D

.dance, .dating, .deals, .degree, .delivery, .democrat, .dental, .design, .diamonds, .diet, .digital, .direct, .directory, .discount, .dog, .domains

E

.education, .email, .energy, .engineering, .enterprises, .equipment, .estate, .events, .exchange, .expert, .exposed, .express

F

.fail, .ventilateur, .farm, .finance, .financial, .fish, .fitness, .flights, .florist, .flowers, .fm, .football, .forsale, .foundation, .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, .healthcare, .help, .hiv, .hockey, .holdings, .holiday, .host, .hosting, .house

I

.im, .immo, .immobilien, .industries, .info, .ink, .institute, .insure, .international, .investments, .io, .irish

J

.jewelry, .juegos

K

.kaufen, .kim, .kitchen, .kiwi

L

.land, .droit, .lease, .legal, .lgbt, .life, .lighting, .limited, .limo, .link, .live, .llc, .loan, .loans, .lol , .ltd

M

.maison, .management, .marketing, .mba, .media, .memorial, .mobi, .moda, .money, .mortgage, .movie

N

.name, .net, .network, .news, .ninja

O

.onl, .online, .org

P

.partners, .parts, .photo, .photography, .photos, .pics, .pictures, .pink, .pizza, .place, .plumbing, .plus, .poker, .porn, .press, .pro, .productions, .properties, .property, .pub

Q

.qpon

R

.recipes, .red, .reise, .reisen, .rentals, .repair, .report, .republican, .restaurant, .reviews, .rip, .rocks, .run

S

.sale, .sarl, .school, .schule, .services, .sex, .sexy, .shiksha, .shoes, .achats, .show, .singles, .site, .ski, .soccer, .social, .solar, .solutions, .logiciel, .space, .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, .voter, .voyage

WXYZ

.watch, .website, .wedding, .wiki, .wine, .travail, .works, .world, .wtf, .xyz, .zone

.ac

Consultez .ac (Ile de l'Ascension).

Return to index

.academy

Utilisé par les établissements d'enseignement comme les écoles et universités. Egalement utilisé par les recruteurs, conseillers, publicitaires, étudiants, enseignants et administrateurs qui sont affiliés avec les établissements scolaires.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.accountants

Utilisé par les entreprises, les groupes et les personnes du secteur de la comptabilité.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.actor

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration

- Un domaine est supprimé du registre : 75 jours après l'expiration

.adult

Utilisé pour les sites web hébergeant du contenu réservé aux adultes.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.agency

Utilisé par les entreprises ou les groupes identifiés en tant qu'agences.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.airforce

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.apartments

Utilisé par les agences immobilières, les propriétaires et locataires.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.associates

Utilisé par les entreprises et les sociétés dont le nom comporte le terme « associates ». Egalement utilisé par les groupes ou les organismes qui souhaitent indiquer la nature professionnelle de leur organisation.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.auction

Utilisé pour les événements liés aux enchères et les achats/ventes basés sur les enchères.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le chinois, le français, l'allemand, l'espagnol et le latin.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.audio

> **Important**
>
> Vous ne pouvez plus utiliser Route 53 pour enregistrer de nouveaux domaines .audio ou transférer des domaines .audio vers Route 53. Nous continuons à prendre en charge les domaines .audio qui sont déjà inscrits auprès de Route 53.

Utilisé par le secteur audiovisuel et toute personne intéressée par la diffusion, le matériel audio, la production audio et le streaming audio.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le cyrillique (russe principalement), le français, l'allemand, l'italien, le portugais et l'espagnol.

Code d'autorisation requis pour les transferts

Non pris en charge. Vous ne pouvez plus transférer de domaines .audio vers Route 53.

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.band

Utilisé pour le partage d'informations sur les groupes de musique et les événements musicaux. Egalement utilisé par les musiciens pour se connecter avec leurs fans et commercialiser des objets dérivés.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le chinois, le français, l'allemand, l'espagnol et le latin.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.bargains

Utilisé pour les informations sur les ventes et promotions.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.bière

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.bet

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Non pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration

- Un domaine est supprimé du registre : 75 jours après l'expiration

.bid

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.bike

Utilisé par les entreprises ou les groupes du secteur du cycle, comme les magasins de vélos, les revendeurs de motos et ateliers de réparation.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.bingo

Utilisé pour les sites de jeux en ligne ou pour le partage d'informations sur le bingo.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.biographie

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.biz

Utilisé à des fins commerciales et professionnelles.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le chinois simplifié, le chinois traditionnel, le danois, le finnois, l'allemand, le hongrois, le japonais, le coréen, le letton, le lituanien, le norvégien, le polonais, le portugais, l'espagnol et le suédois.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

black

Utilisé par les adeptes de la couleur noire et les entreprises qui veulent associer la couleur noire à leur activité ou à leur marque.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Non pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.blue

Utilisé par les adeptes de la couleur bleue et les entreprises qui veulent associer la couleur bleue à leur activité ou à leur marque.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Non pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.boutique

Utilisé pour les informations sur les boutiques et les petits magasins spécialisés.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.builders

Utilisé par les entreprises et les personnes du secteur du bâtiment.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.business

Utilisé par n'importe quel type d'entreprise. Peut être utilisé comme alternative à l'extension .biz.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration

- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.buzz

Utilisé pour les informations sur les dernières actualités et événements récents.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration

- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.cab

Utilisé par les entreprises et les personnes du secteur des taxi.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.cafe

Utilisé par les cafés et les personnes qui s'intéressent à la culture des cafés.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le chinois, le français, l'allemand et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.camera

Utilisé par les amateurs de photographie et ceux qui souhaitent partager des photos.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.camp

Utilisé par les parcs et les zones de loisirs, les colonies de vacances, les ateliers d'écriture, les camps de remise en forme et les adeptes du camping.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.capital

Utilisé comme catégorie générale associée au terme « capital », comme le capital financier ou le capital d'une ville.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.cards

Utilisé par les entreprises spécialisés dans les cartes, comme les cartes électroniques, les cartes imprimées, les cartes de visite et les cartes à jouer. Egalement idéal pour les joueurs qui souhaitent échanger sur les règles et les stratégies de jeux de cartes.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.care

Utilisé par des entreprises ou organismes du secteur des soins. Egalement utilisé par des organismes de bienfaisance.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.careers

Utilisé pour les informations sur le recrutement professionnel.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.cash

Utilisé par les organisations, groupes ou personnes exerçant des activités liées à l'argent.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.casino

Utilisé par l'industrie du jeu ou par les joueurs qui souhaitent partager des informations sur le jeu et les jeux de casino.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration

- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.catering

Utilisé par les entreprises du secteur de la restauration ou par les personnes qui souhaitent partager des informations sur les événements liés à la restauration.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration

- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.cc

Consultez .cc (Iles Coco).

Return to index

.center

Utilisé comme extension générique pour tout, des organismes de recherche aux centres communautaires.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration

- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.ceo

Utilisé pour des informations sur CEOs et leurs égaux.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour l'allemand.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Non pris en charge.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.chat

Utilisé par tout type de site web de chat en ligne.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.cheap

Utilisé par les sites web e-commerce pour promouvoir et vendre des produits à bas prix.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.noël

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 43 jours après l'expiration
- Un domaine est supprimé de Route 53 : 44 jours après l'expiration
- La restauration avec le registre est possible : entre 44 jours et 86 jours après l'expiration
- Le domaine est supprimé du registre : 86 jours après son expiration

.church

Utilisé par les églises de toutes tailles et de toutes confessions pour se connecter avec leurs communautés et pour publier des informations sur les événements et les activités liés à l'église.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.city

Utilisé pour fournir des informations sur des villes spécifiques, comme les points d'intérêt, les meilleurs sites à visiter ou les activités de quartier.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.claims

Utilisé par les entreprises qui gèrent les déclarations de sinistres ou fournissent des services juridiques.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.cleaning

Utilisé par les entreprises ou les personnes qui fournissent des services de nettoyage.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.click

Utilisé par les entreprises qui souhaitent associer l'action « cliquer » à leur site web, par exemple, cliquer sur les produits d'un site web pour les acheter.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité

Pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le cyrillique (russe principalement), le français, l'allemand, l'italien, le portugais et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.clinic

Utilisé par le secteur médical et les professionnels de la santé.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration

- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.clothing

Utilisé par les acteurs du secteur de la mode, notamment les revendeurs, les magasins, les créateurs, les tailleurs et les points de vente.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.cloud

Utilisé comme extension générale, mais idéal pour les entreprises qui fournissent technologies et des services de cloud computing.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Non pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.club

Utilisé par tous les types de clubs ou organisations.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour l'espagnol et le japonais.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.coach

Utilisé par les personnes intéressées par le coaching, comme les professionnels du sport, les conseillers en mode de vie ou les coachs en entreprise.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.codes

Utilisé comme extension générique pour tous les types de codes, comme les codes de conduite, les codes de construction ou les codes de programmation.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.coffee

Utilisé par les professionnels du secteur du café.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.college

Utilisé par les établissements d'enseignement comme les écoles et universités. Egalement utilisé par les recruteurs, conseillers, publicitaires, étudiants, enseignants et administrateurs qui sont affiliés avec les établissements scolaires.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour l'arabe, le chinois simplifié et traditionnel, le cyrillique, le grec, l'hébreu, le japonais et le thaïlandais.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.com

Utilisé pour les sites web commerciaux. C'est l'extension la plus couramment utilisée sur Internet.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité

Toutes les informations sont masquées.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.community

Utilisé par tous les types de communautés, clubs, organisations ou groupes d'intérêt.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.company

Utilisé comme extension générique pour tous les types d'entreprises.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.computer

Utilisé comme extension générique pour les informations relatives aux ordinateurs.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration

- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.condos

Utilisé par les personnes et entreprises concernées par la copropriété.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.construction

Utilisé par les acteurs du secteur de la construction, comme les constructeurs et les sous-traitants.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.consulting

Utilisé par les consultants et autres entités du secteur du conseil.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour l'arabe, le chinois, le français, le cyrillique, le devanagari, l'allemand, le grec, l'hébreu, le japonais, le coréen, le latin, l'espagnol, le tamoul et le thaï.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.contacter

Utilisé par les églises de toutes tailles et de toutes confessions pour se connecter avec leurs communautés et pour publier des informations sur les événements et les activités liés à l'église.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.contractors

Utilisé par les sous-traitants, comme les sous-traitants du secteur de la construction.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.cool

Utilisé par les organisations et les groupes qui souhaitent associer leur marque avec les dernières tendances.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.coupons

Utilisé par les détaillants et les fabricants qui fournissent des bons de réduction en ligne et des codes promo.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le chinois, le français, l'allemand et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.credit

Utilisé par le secteur du crédit.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.creditcard

Utilisé par les entreprises ou les banques qui émettent des cartes de crédit.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.cruises

Utilisé par le secteur du voyage.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration

- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.dance

Utilisé par les danseurs, les professeurs de danse et les écoles de danse.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le chinois, le français, l'allemand, le latin et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Non pris en charge.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.dating

Utilisé pour les sites de rencontre.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.deals

Utilisé pour fournir des informations sur les bonnes affaires et les soldes en ligne.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.degree

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.delivery

Utilisé par les entreprises offrant tout type de service ou produit.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.democrat

Utilisé pour les informations sur le Parti démocrate. Egalement utilisé par les candidats aux élections, les élus, les passionnés de politique, les consultants et les conseillers.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le chinois, le français, l'allemand, le latin et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Non pris en charge.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.dental

Utilisé par les professionnels du secteur dentaire et les fournisseurs de produits dentaires.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.design

Utilisé par les églises de toutes tailles et de toutes confessions pour se connecter avec leurs communautés et pour publier des informations sur les événements et les activités liés à l'église.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.diamonds

Utilisé par les passionnés de diamants et les acteurs de l'industrie du diamant, notamment les vendeurs, les revendeurs et les merchandisers.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration

- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.diet

> **Important**
>
> Vous ne pouvez plus utiliser Route 53 pour enregistrer de nouveaux domaines .diet ou transférer des domaines .diet vers Route 53. Nous continuons à prendre en charge les domaines .diet qui sont déjà inscrits auprès de Route 53.

Utilisé par les professionnels de la santé et de la remise en forme.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le cyrillique (russe principalement), le français, l'allemand, l'italien, le portugais et l'espagnol.

Code d'autorisation requis pour les transferts

Non pris en charge. Vous ne pouvez plus transférer de domaines .diet vers Route 53.

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.digital

Utilisé pour tout ce qui a trait au numérique, mais idéal pour les entreprises technologiques.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration

- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.direct

Utilisé comme extension générale, mais idéal pour ceux qui vendent des produits directement aux clients via un site web de e-commerce.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.directory

Utilisé par le secteur des médias.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.discount

Utilisé pour les sites web de remise et les entreprises qui cassent les prix.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.dog

Utilisé par les cynophiles et ceux qui fournissent des produits et services canins.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le chinois, le français, l'allemand et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.domains

Utilisé pour les informations sur les noms de domaine.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.education

Utilisé pour les informations sur l'éducation.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.email

Utilisé pour les informations sur la promotion des e-mails.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.energy

Utilisé comme extension générale, mais idéal pour les acteurs du secteur de l'énergie ou de l'économie d'énergie.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.engineering

Utilisé par les ingénieurs et les entreprises d'ingénierie.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.enterprises

Utilisé pour les informations sur les entreprises.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration

- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.equipment

Utilisé pour les informations sur les équipements, les fournisseurs ou les fabricants d'équipements, et les magasins de location.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.estate

Utilisé pour les informations sur l'habitat et le secteur du logement.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.events

Utilisé pour les informations sur tous les types d'événements.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.exchange

Utilisé pour tout type d'échange : la bourse, l'échange de produits ou même le simple échange d'informations.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.expert

Utilisé par ceux qui ont des connaissances spécialisées dans différents domaines.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.exposed

Utilisé comme extension générique pour un grand nombre de sujets, y compris la photo, les tabloïdes et le journalisme d'investigation.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.express

Utilisé comme extension générale, mais idéal pour ceux qui souhaitent mettre en valeur la rapidité de livraison de biens ou de services.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le chinois, le français, l'allemand et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.fail

Utilisé lorsqu'une personne a commis une erreur, mais idéal pour la publication de bêtises et d'échecs drôles.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.ventilateur

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration

- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.farm

Utilisé par les acteurs du secteur de l'agriculture, comme les agriculteurs et les ingénieurs agricoles.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.finance

Utilisé par le secteur financier.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.financial

Utilisé par le secteur financier.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.fish

Utilisé comme extension générale, mais idéal pour les sites web associés aux poissons et à la pêche.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.fitness

Utilisé pour promouvoir la forme physique et les services de remise en forme.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.flights

Utilisé par les agences de voyage, les compagnie aériennes et les professionnels du voyage.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.florist

Utilisé par les fleuristes.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.flowers

> **Important**
>
> Vous ne pouvez plus utiliser Route 53 pour enregistrer de nouveaux domaines .flowers ou transférer des domaines .flowers vers Route 53. Nous continuons à prendre en charge les domaines .flowers qui sont déjà inscrits auprès de Route 53.

Utilisé pour tout ce qui concerne les fleurs, comme les ventes de fleurs en ligne ou les informations sur la floriculture et la production de fleurs.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le cyrillique (russe principalement), le français, l'allemand, l'italien, le portugais et l'espagnol.

Code d'autorisation requis pour les transferts

Non pris en charge. Vous ne pouvez plus transférer de domaines .flowers vers Route 53.

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.fm

Consultez .fm (États fédérés de Micronésie).

Return to index

.football

Utilisé par tous ceux qui sont impliqués dans le football.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.forsale

Utilisé pour la vente de produits et de services.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le chinois, le français, l'allemand, le latin et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.foundation

Utilisé par les organismes à but non lucratif, les associations caritatives et d'autres types de fondations.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.fun

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.fund

Utilisé comme extension générale pour tout ce qui concerne le financement.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration

- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.furniture

Utilisé par les fabricants et les vendeurs de meubles et tous les acteurs du secteur de l'ameublement.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.futbol

Utilisé pour les informations sur le football.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le chinois, le français, l'allemand, le latin et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Non pris en charge.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.fyi

Utilisé comme extension générale, mais idéal pour partager toutes sortes d'informations. « FYI » est l'acronyme de « for your information » (pour votre information)

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le chinois, le français, l'allemand et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.gallery

Utilisé par les propriétaires de galeries.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.games

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.gift

Utilisé par les entreprises ou les organisations qui vendent des cadeaux ou fournissent des services liés aux cadeaux.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le cyrillique (russe principalement), le français, l'allemand, l'italien, le portugais et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.gifts

Utilisé par les entreprises ou les organisations qui vendent des cadeaux ou fournissent des services liés aux cadeaux.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.gives

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration

- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.glass

Utilisé par les acteurs de l'industrie du verre, comme les vitriers et les installateurs de fenêtres.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration

- Un domaine est supprimé du registre : 75 jours après l'expiration

.global

Utilisé par les entreprises ou les groupes ayant une portée internationale ou agissant sur le marché international.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour l'arabe, le biélorusse, le bosniaque, le bulgare, le chinois (simplifié), le chinois (traditionnel), le danois, l'allemand, l'hindi, le hongrois, l'islandais, le coréen, le letton, le lituanien, le macédonien, le monténégrin, le polonais, le russe, le serbe, l'espagnol, le suédois et l'ukrainien.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.gmbh

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge

Noms de domaine internationaux

Pris en charge

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.gold

Utilisé comme extension générale, mais idéal pour les entreprises qui achètent ou vendent de l'or ou des produits liés à l'or.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le chinois, le français, l'allemand et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.golf

Utilisé pour les sites web consacrés au golf.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le chinois, le français, l'allemand et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.graphics

Utilisé par les professionnels du graphisme.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.gratis

Utilisé pour les sites web qui offrent des produits gratuits, comme des articles promotionnels, des téléchargements ou des bons de réduction. « Gratis » est un mot d'origine latine qui signifie « gratuit ».

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.green

Utilisé pour les sites web consacrés à la sauvegarde, à l'écologie, à l'environnement et au mode de vie écologique.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Non pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.gripe

Utilisé pour le partage de réclamations et de critiques.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.group

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration

- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.guide

Utilisé comme extension générale, mais idéal pour les sites web consacrés aux destinations, services et produits de voyage.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration

- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.guitars

> **Important**
>
> Vous ne pouvez plus utiliser Route 53 pour enregistrer de nouveaux domaines .guitars ou transférer des domaines .guitars vers Route 53. Nous continuons à prendre en charge les domaines .guitars qui sont déjà inscrits auprès de Route 53.

Utilisé par les amateurs de guitare.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le cyrillique (russe principalement), le français, l'allemand, l'italien, le portugais et l'espagnol.

Code d'autorisation requis pour les transferts

Non pris en charge. Vous ne pouvez plus transférer de domaines .guitars vers Route 53.

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration

- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.guru

Utilisé par ceux qui veulent partager leurs connaissances sur divers sujets.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration

- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.haus

Utilisé par les secteurs de l'immobilier et de la construction. « Haus » est un mot allemand qui signifie « maison ».

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le chinois, le français, l'allemand, le latin et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.healthcare

Utilisé par le secteur de la santé.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.help

Utilisé comme extension générale, mais idéal pour les sites web qui fournissent des informations et une aide en ligne.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le cyrillique (russe principalement), le français, l'allemand, l'italien, le portugais et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.hiv

Utilisé pour les sites web consacrés à la lutte contre le sida.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le cyrillique (russe principalement), le français, l'allemand, l'italien, le portugais et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.hockey

Utilisé pour les sites web consacrés au hockey.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le chinois, le français, l'allemand et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.holdings

Utilisé par les conseillers financiers, les agents de change et les spécialistes de l'investissement.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.holiday

Utilisé par les professionnels du voyage, ainsi que les particuliers et les entreprises intervenant dans l'organisation de soirées et d'événements spéciaux.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.host

Utilisé par les entreprises qui fournissent des plateformes et des services d'hébergement sur Internet.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour l'arabe, le chinois simplifié, le chinois traditionnel, le grec, l'hébreu, le coréen et le thaï.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.hosting

> **Important**
>
> Vous ne pouvez plus utiliser Route 53 pour enregistrer de nouveaux domaines .hosting ou transférer des domaines .hosting vers Route 53. Nous continuons à prendre en charge les domaines .hosting qui sont déjà inscrits auprès de Route 53.

Utilisé pour les sites web d'hébergement et par le secteur de l'hébergement.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le chinois, le français, l'allemand et l'espagnol.

Code d'autorisation requis pour les transferts

Non pris en charge. Vous ne pouvez plus transférer de domaines .hosting vers Route 53.

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.house

Utilisé par les agences immobilières, ainsi que les acheteurs et les vendeurs de maisons.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.im

Consultez .im (Ile de Man).

Return to index

.immo

Utilisé par le secteur immobilier.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.immobilien

Utilisé pour les informations sur l'immobilier.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le chinois, le français, l'allemand et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Non pris en charge.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration

- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.industries

Utilisé par les entreprises commerciales souhaitant être associées à un secteur.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.info

Utilisé pour la diffusion d'informations.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.ink

Utilisé par les amateurs de tatouage ou toutes les activités liées à l'encre, comme le secteur de l'impression et de la publication.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour l'arabe et le latin.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.institute

Utilisé par tous les groupes ou organisations, notamment dans les domaines de la recherche et de l'éducation.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.insure

Utilisé par les compagnies d'assurance et de courtiers en assurances.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.international

Utilisé par les entreprises ayant des réseaux internationaux, les personnes qui se déplacent à travers le monde ou les associations caritatives ayant un rayonnement international.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.investments

Utilisé comme extension générale, mais idéal pour la promotion des opportunités d'investissement.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.io

Consultez .io (Territoire Britannique de l'Océan Indien).

Return to index

.irish

Utilisé pour la promotion des organisations et de la culture irlandaises.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour l'arabe, le chinois simplifié, le chinois traditionnel, le français, l'allemand, le grec, l'hébreu, le japonais, le coréen, l'espagnol, le tamoul et le thaï.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.jewelry

Utilisé par les acheteurs et les vendeurs de bijoux.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le chinois, le français, l'allemand et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.juegos

> **Important**
>
> Vous ne pouvez plus utiliser Route 53 pour enregistrer de nouveaux domaines .juegos ou transférer des domaines .juegos vers Route 53. Nous continuons à prendre en charge les domaines .juegos qui sont déjà inscrits auprès de Route 53.

Utilisé pour les sites web de jeux de toutes sortes. « Juegos » est un mot espagnol qui signifie « jeux ».

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le cyrillique (russe principalement), le français, l'allemand, l'italien, le portugais et l'espagnol.

Code d'autorisation requis pour les transferts

Non pris en charge. Vous ne pouvez plus transférer de domaines .juegos vers Route 53.

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.kaufen

Utilisé pour les informations sur l'e-commerce.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le chinois, le français, l'allemand, le latin et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Non pris en charge.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.kim

Utilisé par les personnes dont le nom ou le prénom est Kim.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.kitchen

Utilisé par les distributeurs de cuisines, les cuisiniers, les blogueurs culinaires et les acteurs de l'industrie alimentaire.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration

- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.kiwi

Utilisé par les entreprises et les personnes qui souhaitent encourager la culture néo-zélandaise. Egalement utilisé comme plateforme pour l'aide caritative destinée à la reconstruction de Christchurch, ville endommagée par les tremblements de terre en 2010 et 2011.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le maori.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.land

Utilisé par les agriculteurs, les agences immobilières, les développeurs dans le domaine commercial et toute personne intéressées par la propriété.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.droit

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.lease

Utilisé par les agents immobiliers, les propriétaires et les locataires.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.legal

Utilisé par les membres du corps juridique.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.lgbt

Utilisé par la communauté de personnes lesbiennes, gay, bisexuelles et transgenres.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Non pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.life

Utilisé comme extension générale. Convient pour une large palette d'entreprises, de groupes et d'individus.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.lighting

Utilisé par les photographes, les créateurs, les architectes, les ingénieurs et les personnes qui s'intéressent à l'éclairage.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.limited

Utilisé comme extension générale. Convient pour une large palette d'entreprises, de groupes et d'individus.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.limo

Utilisé par les chauffeurs, les agences de location et les entreprises spécialisés dans les limousines.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration

- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.link

Utilisé pour les informations sur la création de liens rapides en ligne.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité

Uniregistry est le registre des domaines .LINK. En raison de la politique de Uniregistry, le WHOIS au niveau du registre affiche "REDACTED FOR PRIVACY". La suppression de notre fonction de protection de la vie privée n'affectera que les informations affichées au niveau du registre WHOIS d'Amazon Registrar.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le cyrillique (russe principalement), le français, l'allemand, l'italien, le portugais et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.live

Utilisé comme extension générale. Convient pour une large palette d'entreprises, de groupes et d'individus.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le chinois, le français, l'allemand, le latin et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.llc

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.loan

Utilisé par les organismes de prêt, les emprunteurs et les professionnels du crédit.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le danois, l'allemand, le norvégien et le suédois.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.loans

Utilisé par les organismes de prêt, les emprunteurs et les professionnels du crédit.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.lol

Utilisé pour les sites web liés à l'humour et à la comédie. « LOL » est l'acronyme de « laugh out loud » (éclater de rire).

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le cyrillique, le français, l'allemand, l'italien, le portugais et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.ltd

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.maison

Utilisé par le secteur immobilier.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.management

Utilisé pour les informations sur le mode des affaires et la gestion d'entreprise.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration

- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.marketing

Utilisé par le secteur marketing à différentes fins.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.mba

Utilisé pour les sites web qui fournissent des informations sur le MBA (maîtrise en administration des entreprises).

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le chinois, le français, l'allemand et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.media

Utilisé par les secteurs des médias et du divertissement.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.memorial

Utilisé par les organismes de commémoration visant à honorer des événements et des personnes.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.mobi

Utilisé par les entreprises et les personnes qui souhaitent que leurs sites web soient accessibles sur les téléphones mobiles.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Non pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.moda

Utilisé pour les informations sur la mode.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le chinois, le français, l'allemand, le latin et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Non pris en charge.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.money

Utilisé pour les sites web consacrés à l'argent et aux activités liées à l'argent.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.mortgage

Utilisé par le secteur des hypothèques.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le chinois, le français, l'allemand, le latin et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.movie

Utilisé pour les sites web qui fournissent des informations sur les films et le cinéma. Adapté aux professionnels et aux cinéphiles.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le chinois, le français, l'allemand et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration

- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.name

Utilisé par tous ceux qui veulent créer une présence web personnalisée.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Restrictions

Verisign, le registre pour .name TLDs, vous permet d'enregistrer à la fois des domaines de deuxième niveau (nom .name) et des domaines de troisième niveau (prénom). nom de famille (.name). Route 53 ne prend en charge que les domaines de deuxième niveau, à la fois pour l'enregistrement de domaines et pour le transfert de domaines existants vers Route 53.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration

- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.net

Utilisé pour tous les types de sites web. L'extension .net est l'abréviation du mot « network » (réseau).

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité

Toutes les informations sont masquées.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.network

Utilisé par les professionnels des réseaux ou ceux qui veulent créer des connexions par le biais de la mise en réseau.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.news

Utilisé pour distribuer les informations ayant un intérêt médiatique, comme les événements actuels ou les informations relatives au journalisme et à la communication.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le chinois, le français, l'allemand, le latin et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.ninja

Utilisé par les personnes et les entreprises qui souhaitent être associées à l'univers des ninjas.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le chinois, le français, l'allemand, le latin et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.onl

L'extension .onl est l'abréviation du mot « online » (en ligne). Il s'agit également de abréviation de l'équivalent de l'expression « organisation à but non lucratif » en espagnol.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.online

L'extension .onl est l'abréviation du mot « online » (en ligne). Il s'agit également de abréviation de l'équivalent de l'expression « organisation à but non lucratif » en espagnol.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.org

Utilisé par tous les types d'organisations.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité

Toutes les informations sont masquées.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.partners

Utilisé par les cabinets d'avocats, les investisseurs et diverses entreprises. Egalement utilisé pour les sites web de réseaux sociaux ayant vocation à faciliter les relations.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.parts

Utilisé comme extension générale, mais idéal pour les acheteurs, vendeurs et fabricants de pièces.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration

- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.photo

Utilisé par les photographes et les amateurs de photographie.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le cyrillique (russe principalement), le français, l'allemand, l'italien, le portugais et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.photography

Utilisé par les photographes et les amateurs de photographie.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.photos

Utilisé par les photographes et les amateurs de photographie.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.pics

Utilisé par les photographes et les amateurs de photographie.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le cyrillique (russe principalement), le français, l'allemand, l'italien, le portugais et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.pictures

Utilisé par les personnes intéressées par la photographie, l'art et les médias.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.pink

Utilisé par les adeptes de la couleur rose et les entreprises qui veulent associer la couleur rose à leur activité ou à leur marque.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.pizza

Utilisé par les pizzerias et les amateurs de pizza.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.place

Utilisé comme extension générale, mais idéal pour les secteurs de la maison et des voyages.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.plumbing

Utilisé par les professionnels de la plomberie.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.plus

Utilisé comme extension générale, mais idéal pour les vêtements de grande taille, les logiciels complémentaires ou tout produit offrant des fonctionnalités ou dimension en plus.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le chinois, le français, l'allemand et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration

- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.poker

Utilisé par les joueurs et les sites de jeux.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Non pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.porn

Utilisé pour les sites web pour adultes uniquement.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.press

Utilisé pour les sites web pour adultes uniquement.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.pro

Utilisé par les professionnels et les organisations professionnelles agréés et qualifiés.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Non pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.productions

Utilisé par les studios et les sociétés de production qui produisent des publicités, des annonces radio et des clips.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.properties

Utilisé pour les informations concernant les propriétés, notamment la propriété immobilière ou la propriété intellectuelle. Egalement utilisé par les propriétaires de maisons, de bâtiments ou de terres à vendre ou à louer.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.property

Utilisé pour les informations concernant les propriétés, notamment la propriété immobilière ou la propriété intellectuelle. Egalement utilisé par les propriétaires de maisons, de bâtiments ou de terres à vendre ou à louer.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le cyrillique (russe principalement), le français, l'allemand, l'italien, le portugais et l'espagnol.

Code d'autorisation requis pour les transferts

Non pris en charge. Vous ne pouvez plus transférer de domaines .property vers Route 53.

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.pub

Utilisé par les professionnels de la publication, de la publicité ou de la conception.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le chinois, le français, l'allemand, le latin et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.qpon

Utilisé pour les bons de réduction et les codes promo.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.recipes

Utilisé pour le partage de recettes.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration

- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.red

Utilisé par les adeptes de la couleur rouge et les entreprises qui veulent associer la couleur rouge à leur activité ou à leur marque.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.reise

Utilisé pour les sites web associés aux voyages. « Reise » est un mot allemand qui signifie « augmenter », « se lever » ou « entreprendre un voyage ».

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le chinois, le français, l'allemand et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.reisen

Utilisé pour les sites web associés aux voyages. « Reisen » est un mot allemand signifiant « voyager ».

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.rentals

Utilisé pour tous les types de location.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.repair

Utilisé par les services de réparation ou pour partager ses connaissances sur les réparations de tous types d'objets.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.report

Utilisé comme extension générale, mais idéal pour les informations sur les rapports d'activité, les publications communautaires, les critiques de livres ou l'actualité.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.republican

Utilisé pour les informations sur le Parti républicain. Egalement utilisé par les candidats aux élections, les élus, les passionnés de politique, les consultants et les conseillers.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le chinois, le français, l'allemand, le latin et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.restaurant

Utilisé par le secteur de la restauration.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.reviews

Utilisé pour donner son opinion et lire les commentaires des autres.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le chinois, le français, l'allemand, le latin et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Non pris en charge.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.rip

Utilisé pour les sites web dédiés à la mort et au souvenir. « RIP » est l'acronyme de « rest in peace » (repose en paix).

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le chinois, le français, l'allemand, le latin et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration

- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.rocks

Utilisé comme extension générale, mais idéal pour toute personne géniale (« who rocks ») : musiciens, géologues, bijoutiers, alpinistes et plus encore.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le chinois, le français, l'allemand, le latin et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.run

Utilisé comme extension générale, mais idéal pour le secteur du sport et de la remise en forme.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le chinois, le français, l'allemand et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.sale

Utilisé par les sites web e-commerce.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le chinois, le français, l'allemand, le latin et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.sarl

Utilisé par les sociétés à responsabilité limité généralement situées en France. « SARL » est l'acronyme de Société à responsabilité limitée.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.school

Utilisé pour les informations sur l'enseignement, les établissements d'enseignement et les activités liées à l'école.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.schule

Utilisé pour les informations sur l'enseignement, les établissements d'enseignement et les activités liées à l'école en allemand. « Schule » est un mot allemand qui signifie « école ».

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.services

Utilisé pour les sites web axés sur tous types de services.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.sex

Utilisé pour le contenu réservé aux adultes.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.sexy

Utilisé pour le contenu à caractère sexuel. Egalement utilisé pour décrire les marques, produits, informations et sites web les plus populaires et excitants.

Return to index

> **Important**
>
> Vous ne pouvez plus utiliser Route 53 pour enregistrer de nouveaux domaines .sexy ou transférer des domaines .sexy vers Route 53. Nous continuons à prendre en charge les domaines .sexy qui sont déjà enregistrés sur Route 53.

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le cyrillique (russe principalement), le français, l'allemand, l'italien, le portugais et l'espagnol.

Code d'autorisation requis pour les transferts

Non pris en charge. Vous ne pouvez plus transférer des domaines .sexy vers Route 53.

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.shiksha

Utilisé par les établissements éducatifs. « Shiksha » est un terme indien qui signifie « école ».

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.shoes

Utilisé par les revendeurs, designers, fabricants et bloggeurs mode dans l'univers de la chaussure.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration

- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.achats

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.show

Utilisé comme extension générale, mais idéal pour le monde du spectacle.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le chinois, le français, l'allemand et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.singles

Utilisé par les clubs de rencontres, les établissements et autres entreprises qui s'adressent aux personnes qui veulent entrer en relation.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.site

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.ski

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.soccer

Utilisé pour les sites web dédiés au football.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le chinois, le français, l'allemand et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.social

Utilisé pour les informations sur les réseaux sociaux, les forums et les conversations en ligne.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le chinois, le français, l'allemand, le latin et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.solar

Utilisé pour plus d'informations sur le système solaire ou l'énergie solaire.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.solutions

Utilisé par les consultants, do-it-yourself les services et les conseillers de toutes sortes.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.logiciel

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration

- Un domaine est supprimé du registre : 75 jours après l'expiration

.space

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.store

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.stream

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.studio

Utilisé comme extension générale, mais idéal pour les acteurs du secteur immobilier, de l'art et du divertissement.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le chinois, le français, l'allemand, le latin et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.style

Utilisé comme extension générale, mais idéal pour les sites web dédiés aux dernières tendances, notamment dans le monde de la mode, de la conception, de l'architecture et de l'art.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.sucks

Utilisé comme extension générale, mais idéal pour partager des expériences négatives ou avertir d'escroqueries, de fraudes ou de produits défectueux.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Non pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.supplies

Utilisé par les entreprises qui vendent des biens en ligne.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.supply

Utilisé par les entreprises qui vendent des biens en ligne.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration

- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.support

Utilisé par les entreprises, groupes ou associations qui offrent des services d'aide, comme un support client, produit ou système, ou une aide émotionnelle, financière ou spirituelle.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.surgery

Utilisé pour les informations sur la chirurgie, les médicaments et soins de santé.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.systems

Principalement utilisé par le secteur des technologies et les professionnels des services technologiques.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.tattoo

Utilisé par les amateurs de tatouages et le secteur du tatouage.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le cyrillique (russe principalement), le français, l'allemand, l'italien, le portugais et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.tax

Utilisé pour les informations sur les taxes, la préparation de déclaration de revenus et le droit fiscal.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.taxi

Utilisé par les taxis, les chauffeurs et les services de navette.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le chinois, le français, l'allemand et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.team

Utilisé par les entreprises ou organisations qui souhaitent être identifiées comme une équipe.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le chinois, le français, l'allemand et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.tech

Utilisé par les amateurs de technologie et les spécialistes de la technologie dans les entreprises, services et chez les fabricants.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.technology

Utilisé par les amateurs de technologie et les spécialistes de la technologie dans les entreprises, services et chez les fabricants.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.tennis

Utilisé pour les informations relatives au tennis.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration

- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.theater

Utilisé pour les sites web dédiés au théâtre, aux pièces et aux comédies musicales.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le chinois, le français, l'allemand et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.tienda

Utilisé par les entreprises de vente au détail qui souhaitent entrer en relation avec les consommateurs hispanophones.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.tips

Utilisé pour partager des connaissances et des conseils sur tous les sujets.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.tires

Utilisé par les fabricants, distributeurs ou acheteur de pneus.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.today

Utilisé pour les informations sur les événements, actualités, informations météorologiques, divertissement actuels, etc.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.tools

Utilisé pour les informations sur tous types d'outils.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.tours

Utilisé comme extension générale, mais idéal pour les agences de voyage.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le chinois, le français, l'allemand et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.town

Utilisé pour promouvoir les quartiers, la culture et la communauté d'une ville.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.toys

Utilisé par l'industrie du jouet.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.trade

Utilisé comme extension générale, mais idéal pour les sites web de commerce ou les services commerciaux.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le danois, l'allemand, le norvégien et le suédois.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration

- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.training

Utilisé par des formateurs, les entraîneurs et les éducateurs.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration

- Un domaine est supprimé du registre : 75 jours après l'expiration

.tv

Utilisé pour les informations sur la télévision et les médias.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Restrictions

Aucune.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Non pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.university

Utilisé par les universités et d'autres types d'établissements scolaires.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.uno

Utilisé pour les informations sur les communautés hispanique, portugaise et italienne.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.vacations

Utilisé par l'industrie du tourisme.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.vegas

Utilisé pour promouvoir la ville de Las Vegas et le mode de vie qu'elle représente.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Non pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.ventures

Utilisé par les entrepreneurs, les start-ups, les sociétés de capital risque, les banques d'investissement et les financiers.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.vg

Consultez .vg (Iles Vierges Britanniques).

Return to index

.viajes

Utilisé par les agences de voyage, les tour opérateurs, les blogs de voyage, les voyagistes, les services de location, les blogueurs voyage et les fournisseurs de voyage.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.video

Utilisé par l'industrie de la vidéo et des médias.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le chinois, le français, l'allemand, le latin et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.villas

Utilisé par les agences immobilières et les propriétaires qui souhaitent vendre ou louer des villas.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.vision

Utilisé comme extension générale, mais idéal pour les spécialistes de la vue, comme les optométristes et les ophtalmologistes.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.voter

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration

- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.voyage

Utilisé par les agences de voyage, les tour opérateurs, les blogs de voyage, les voyagistes, les services de location, les blogueurs voyage et les fournisseurs de voyage.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration

- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.watch

Utilisé pour obtenir des informations sur les sites Web de streaming, TVs le Web, les vidéos ou les montres.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.website

Utilisé pour les informations sur la création, la promotion, les améliorations et les expériences relatives aux sites web.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour l'arabe, le chinois simplifié, le chinois traditionnel, le grec, l'hébreu, le japonais, le coréen et le thaï.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.wedding

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Restrictions

Aucune.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le chinois, le français, l'allemand et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.wiki

Utilisé pour les informations sur la documentation en ligne.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour l'arabe et le latin.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.wine

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité

Pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.travail

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.works

Utilisé par les entreprises, organisations et personnes pour les informations relatives à l'emploi, aux postes et aux agences pour l'emploi. Cette extension peut servir d'alternative aux extensions .com, .net ou .org.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.world

Utilisé par les personnes qui souhaitent fournir des informations sur des sujets internationaux.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.wtf

Utilisé pour être identifié avec l'acronyme populaire (mais vulgaire) « WTF ».

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration

- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.xyz

Utilisé comme extension générale pour n'importe quel but.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Restrictions

Le registre pour les domaines .xyz, Generation XYZ, considère certains noms de domaine comme des noms de domaine premium. Vous ne pouvez pas enregistrer des domaines .xyz premium avec Route 53 ni les transférer vers celui-ci. Pour plus d'informations, consultez le site web Generation XYZ.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.zone

Utilisé pour les informations relatives à tout type de zone, y compris les fuseaux horaires, les zones climatiques et les zones dans le cadre sportif.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour le français et l'espagnol.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration

- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

Domaines géographiques de premier niveau

Les extensions de domaine suivantes sont regroupées par zone géographique et incluent des extensions officielles spécifiques à un pays, connues sous le nom de domaines de premier niveau de code de pays (ccTLDs). Par exemple : .be (Belgique), .in (Inde) et .mx (Mexique). Les règles d'enregistrement du CC TLDs varient selon les pays. Certains pays n'imposent pas de restriction, ce qui signifie que n'importe qui dans le monde peut utiliser l'extension, tandis que d'autres imposent certaines conditions, par exemple la résidence. La liste de chaque domaine de premier niveau national indique toutes les restrictions.

> **Important**
>
> Lors du transfert d'un cc TLDs vers Route 53, à l'exception des fichiers .cc et .tv, les mises à jour du contact du propriétaire sont ignorées et les coordonnées du propriétaire issues du registre sont utilisées. Une fois le transfert terminé, vous pouvez mettre à jour les coordonnées du propriétaire. Pour de plus amples informations, veuillez consulter Mise à jour des informations de contact et de la propriété pour un domaine.

Return to index

Afrique

.ac (Ile de l'Ascension), .co.za (Afrique du Sud), .sh (Sainte-Hélène)

Amériques

.ca (Canada), .cl (Chili), .co (Colombie), .com.ar (Argentine), .com.br (Brésil), com.mx (Mexique), .mx (Mexique), .us (États-Unis), .vc (Saint-Vincent-et-les-Grenadines), .vg (Iles Vierges Britanniques)

Asie/Océanie

.au (Australie), .cc (Iles Coco), .co.nz (Nouvelle-Zélande), .com.au (Australie), .com.sg (République de Singapour), .fm (États fédérés de Micronésie), .in (Inde), .jp (Japon), .io (Territoire

Britannique de l'Océan Indien), .net.au (Australie), .net.nz (Nouvelle-Zélande), .org.nz (Nouvelle-Zélande), .pw (Palaos), .qa (Qatar), .ru (Fédération de Russie), .sg (République de Singapour)

Europe

.be (Belgique), .berlin (ville de Berlin en Allemagne), .ch (Suisse), .co.uk (Royaume-Uni), .cz (République tchèque), .de (Allemagne), .es (Espagne) , .eu (Union européenne), .fi (Finlande), .fr (France), .gg (Guernesey), .im (Ile de Man), .it (Italie), .me (Monténégro), .me.uk (Royaume-Uni), .nl (Pays-Bas), .org.uk (Royaume-Uni), .ruhr (région de la Ruhr, ouest de l'Allemagne), .se (Suède), .uk (Royaume-Uni), .wien (ville de Vienne en Autriche)

Afrique

Vous pouvez utiliser les domaines de premier niveau (TLDs) suivants pour l'Afrique afin d'enregistrer des domaines auprès d'Amazon Route 53.

, ,

Return to index

.ac (Ile de l'Ascension)

Return to index

Egalement utilisé comme domaine de premier niveau générique populaire dans le monde universitaire.

Durée de validité de l'enregistrement et du renouvellement

Un an.

Restrictions

Accessible publiquement, sans aucune restriction.

Protection de la confidentialité

Déterminé par le registre.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Le domaine est supprimé du registre : 80 jours après l'expiration

.co.za (Afrique du Sud)

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un an.

Restrictions

Seuls les domaines de deuxième niveau sont disponibles pour l'extension .za. Route 53 prend en charge le domaine de deuxième niveau .co.za.

Accessible publiquement, avec les restrictions suivantes :

- Enregistrement accessible aux personnes morales identifiables (personnes physiques et personnes morales).
- Le nom de domaine doit réussir un contrôle de zone pendant le processus d'enregistrement.

Protection de la confidentialité

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Non pris en charge.

Code d'autorisation requis pour les transferts

Non

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Le renouvellement est possible : jusqu'à un jour avant la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : Non
- Un domaine est supprimé de Route 53 : 1 jour avant l'expiration
- La restauration avec le registre est possible : entre 1 jour et 9 jours après l'expiration
- Le domaine est supprimé du registre : 9 jours après l'expiration

.sh (Sainte-Hélène)

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Restrictions

Accessible publiquement, sans aucune restriction.

Protection de la confidentialité

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Le domaine est supprimé du registre : 80 jours après l'expiration

Amériques

Vous pouvez utiliser les domaines de premier niveau (TLDs) suivants pour les Amériques afin d'enregistrer des domaines auprès d'Amazon Route 53.

, , , , , , , , ,

Return to index

.ca (Canada)

Return to index

Les variantes, avec (à) ou sans (a) un accent, d'un nom de domaine sont automatiquement réservées au titulaire et font partie d'un ensemble administratif. Pour activer un domaine dans un bundle, le titulaire doit faire une demande d'enregistrement pour le domaine. Tous les domaines d'un bundle doivent être enregistrés par le même titulaire et auprès du même bureau d'enregistrement. Le titulaire devra également soumettre une demande de transfert pour tous les domaines d'un bundle pour terminer le transfert.

E-mail de confirmation du registre TLD

Lorsque vous enregistrez un domaine .ca, vous recevez un e-mail contenant un lien vers la procédure d'acceptation du contrat d'enregistrement. Vous devez exécuter la procédure sous sept jours. A défaut, votre domaine ne sera pas enregistré.

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Restrictions

Accessible publiquement, avec les restrictions suivantes :

- L'enregistrement est accessible aux personnes physiques ou aux organisations ayant un lien avec le Canada, comme défini dans le document Canadian Presence Requirements for Registrants.
- Contact inscrit : vous devez fournir le nom juridique complet et exact du propriétaire du domaine.
- Contacts administratif et technique : vous devez spécifier le type de contact Person et fournir des informations de contact pour les personnes vivant au Canada.
- Vous devez sélectionner l'un des types autorisés suivants pendant le processus d'enregistrement :
  - ABO : Peuples autochtones (individus ou groupes) autochtones au Canada
  - ASS : Association canadienne non constituée en personne morale
  - CCO : Société canadienne, ou province ou territoire canadien
  - CCT : Citoyen canadien
  - EDU : Établissement d'enseignement canadien
  - GOV : Gouvernement ou entité gouvernementale au Canada
  - HOP : Hôpital canadien
  - INB : Bande indienne reconnue par la Loi sur les Indiens du Canada
  - LAM : Bibliothèque, archives ou musée canadiens
  - LGR : Représentant légal d'un citoyen canadien ou d'un résident permanent
  - MAJ : Her/His Majesté la Reine/Roi
  - OMK : Marque officielle enregistrée au Canada
  - PLT : Parti politique canadien
  - PRT : Société de personnes enregistrée au Canada

- RES : Résident permanent du Canada
- TDM : Marque déposée au Canada (par un type de propriétaire non canadien)
- TRD : Syndicat canadien
- TRS : Fiducie établie au Canada

Protection de la confidentialité

- Personne — Pour tous les contacts, le nom, l'adresse, le numéro de téléphone, le numéro de télécopieur et l'adresse électronique du contact sont masqués, car la CIRA applique automatiquement sa protection de la vie privée à une personne. L'option de protection de la vie privée sera appliquée uniquement au Whois du bureau d'enregistrement.
- Entreprise, association ou organisme public : non pris en charge au niveau du registre.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : variable. Contactez AWS Support.

Suppression de l'enregistrement de domaine

Le registre des domaines .ca ne permet pas de supprimer les enregistrements de domaine. Au lieu de cela, vous devez désactiver le renouvellement automatique et attendre l'expiration du

domaine. Pour de plus amples informations, veuillez consulter Suppression d'un enregistrement de nom de domaine.

.cl (Chili)

> **Important**
>
> Vous ne pouvez plus utiliser Route 53 pour enregistrer de nouveaux domaines .cl ou transférer des domaines .cl vers Route 53. Nous continuons à prendre en charge les domaines .cl qui sont déjà inscrits auprès de Route 53.

Return to index

Période de renouvellement

Deux ans.

Protection de la confidentialité

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Non pris en charge. Nous vous recommandons d'empêcher les transferts non autorisés en limitant l'accès à l'action de l'RetrieveDomainAuthCodeAPI. (Lorsque vous limitez l'accès à cette API Route 53, vous limitez également les personnes autorisées à générer un code d'autorisation à l'aide de la console Route 53 et d'autres méthodes de programmation.) AWS SDKs Pour de plus amples informations, veuillez consulter Identity and Access Management dans Amazon Route 53.

Code d'autorisation requis pour les transferts

Non pris en charge. Vous ne pouvez plus transférer de domaines .cl vers Route 53.

DNSSEC

Non pris en charge.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : contactez AWS Support.
- Un renouvellement tardif avec Route 53 est possible : contactez AWS Support.
- Un domaine est supprimé de Route 53 : contactez AWS Support.

- Une restauration auprès du registre est possible : contactez AWS Support.
- Un domaine est supprimé du registre : contactez AWS Support.

.co (Colombie)

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à cinq ans.

Restrictions

Le registre pour les domaines .co, Go.co, considère certains noms de domaine comme noms de domaine premium. Vous ne pouvez pas enregistrer des domaines .co premium avec Route 53 ni les transférer vers celui-ci. Pour plus d'informations, consultez le site web Go.co.

Protection de la confidentialité (s'applique à : personne)

Toutes les informations sont masquées.

Si le type de contact n'est pas une personne, le nom de l'entreprise et le pays sont affichés par le WHOIS.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 29 jours après l'expiration
- Un domaine est supprimé de Route 53 : 30 jours après l'expiration

- Une restauration auprès du registre est possible : entre 30 jours et 45 jours après l'expiration
- Une domaine est supprimé du registre : 50 jours après l'expiration

.com.ar (Argentine)

> **Important**
>
> Vous ne pouvez plus utiliser Route 53 pour enregistrer de nouveaux domaines .com.ar ou transférer des domaines .com.ar vers Route 53. Nous continuons à prendre en charge les domaines .com.ar qui sont déjà inscrits auprès de Route 53.

Return to index

Période de renouvellement

Un an.

Protection de la confidentialité

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Non pris en charge. Pour empêcher les transferts non autorisés, limitez l'accès à l'adresse e-mail du titulaire et à la Route 53 APIs qui pourrait permettre le changement de propriétaire, UpdateDomainContactpar exemple. Pour plus d'informations, consultez la rubrique Actions, ressources et clés de condition pour les domaines Route 53 dans la section Référence de l'autorisation de service et Exemples d'autorisations pour un propriétaire d'enregistrement de domaine.

Code d'autorisation requis pour les transferts

Non pris en charge. Vous ne pouvez plus transférer de domaines .com.ar vers Route 53.

DNSSEC

Non pris en charge.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : contactez AWS Support.
- Un renouvellement tardif avec Route 53 est possible : contactez AWS Support.

- Un domaine est supprimé de Route 53 : contactez AWS Support.
- Une restauration auprès du registre est possible : contactez AWS Support.
- Un domaine est supprimé du registre : contactez AWS Support.

.com.br (Brésil)

> **Important**
>
> Vous ne pouvez plus utiliser Route 53 pour enregistrer de nouveaux domaines .com.br ou transférer des domaines .com.br vers Route 53. Nous continuons à prendre en charge les domaines .com.br qui sont déjà inscrits auprès de Route 53.

Return to index

Période de renouvellement

Un an.

Protection de la confidentialité

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Code d'autorisation requis pour les transferts

Non pris en charge. Vous ne pouvez plus transférer de domaines .com.br vers Route 53.

DNSSEC

Non pris en charge.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : entre 30 jours avant l'expiration et la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 119 jours après l'expiration
- Un domaine est supprimé de Route 53 : 119 jours après l'expiration
- Une restauration auprès du registre est possible : Non
- Un domaine est supprimé du registre : 119 jours après l'expiration

com.mx (Mexique)

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Restrictions

Accessible publiquement, sans aucune restriction.

Protection de la confidentialité

Déterminé par le registre.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Non pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.mx (Mexique)

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Restrictions

Accessible publiquement, sans aucune restriction.

Protection de la confidentialité

Déterminé par le registre.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Non pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.us (États-Unis)

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Restrictions

Le registre des domaines .us n'autorise pas les noms de domaine qui contiennent l'un des sept mots identifiés dans l'annexe « Appendix to Opinion of the Court » du document Federal Communications Commission v. Pacifica Foundation No. 77-528.

Accessible publiquement, avec une restriction :

- L'extension .us est réservée aux sites web ou aux activités situées aux États-Unis.

Protection de la confidentialité

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Non pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 29 jours après l'expiration
- Un domaine est supprimé de Route 53 : 30 jours après l'expiration
- Une restauration auprès du registre est possible : entre 30 jours et 60 jours après l'expiration
- Un domaine est supprimé du registre : 65 jours après l'expiration

.vc (Saint-Vincent-et-les-Grenadines)

Egalement utilisé comme domaine de premier niveau générique, souvent dans le domaine du capital risque-risque, des établissements universitaires, etc.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Restrictions

Accessible publiquement, sans aucune restriction.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Non pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Le domaine est supprimé du registre : 80 jours après l'expiration

.vg (Iles Vierges Britanniques)

Egalement utilisé comme domaine de premier niveau générique, souvent dans le domaine des jeux vidéo.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Restrictions

Accessible publiquement, sans aucune restriction.

Protection de la confidentialité

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Non pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Non pris en charge.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à 44 jours après la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : Oui
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Un domaine est supprimé du registre : 45 jours après l'expiration
- Une restauration auprès du registre est possible : entre 45 jours et 74 jours après l'expiration
- Le domaine est de nouveau disponible au grand public : 80 jours après l'expiration

Asie/Océanie

Vous pouvez utiliser les domaines de premier niveau (TLDs) suivants pour l'Asie et l'Océanie afin d'enregistrer des domaines auprès d'Amazon Route 53.

, , , , , , , , , , , , , ,

Return to index

.au (Australie)

Return to index

E-mail de confirmation du registre TLD

Notre associé au bureau d'enregistrement, Gandi, revend des domaines .au via. DomainDirectors Lorsque vous transférez un nom de domaine vers Route 53, DomainDirectors envoyez un e-mail au contact du titulaire du domaine afin de vérifier les informations de contact ou d'autoriser les demandes de transfert.

Durée de validité de l'enregistrement et du renouvellement

Un à cinq ans.

Restrictions

Accessible publiquement, avec les restrictions suivantes :

- Les domaines .au sont accessibles aux personnes morales, entités commerciales, partenariats ou entrepreneurs individuels enregistrés en Australie. Il est également accessible aux entreprises étrangères autorisées à exercer une activité en Australie, ainsi qu'aux propriétaires ou aux demandeurs d'une marque déposée australienne. Les particuliers ne peuvent pas enregistrer de domaines .au. Le contact inscrit doit être une entreprise.
- Votre nom de domaine doit être identique à votre nom (celui enregistré auprès des autorités australiennes compétentes) ou à votre marque (ou une abréviation ou un acronyme de celle-ci).
- Le nom de domaine doit indiquer votre activité. Par exemple, il doit indiquer un produit que vous vendez ou un service que vous fournissez.
- Pendant le processus d'enregistrement, vous devez indiquer les éléments suivants :
  - Votre type d'enregistrement : votre numéro ABN (Australian Business Number), votre numéro ACN (Australian Company Number), votre numéro) ou votre TM (marque déposée) si le nom de domaine correspond à votre marque.
  - Votre numéro d'identification. Il peut s'agir de votre numéro de carte d'assurance maladie Medicare, d'un numéro TFN (tax file number), de votre numéro de permis de conduire ou d'un numéro ABN (Australian Business Number).
  - Votre état ou province.

- Des informations de contact incorrectes ou non concordantes, y compris le nom, le numéro ABN ou le numéro de marque (TM), entraîneront des échecs d'enregistrement, de commerce et de renouvellement. Un changement de propriété peut s'avérer nécessaire pour corriger les informations relatives aux domaines existants.

Protection de la confidentialité

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Non pris en charge. Nous vous recommandons d'empêcher les transferts non autorisés en limitant l'accès à l'action de l'RetrieveDomainAuthCodeAPI. (Lorsque vous limitez l'accès à cette API Route 53, vous limitez également les personnes autorisées à générer un code d'autorisation à l'aide de la console Route 53 et d'autres méthodes de programmation.) AWS SDKs Pour de plus amples informations, veuillez consulter Identity and Access Management dans Amazon Route 53.

Noms de domaine internationaux

Non pris en charge.

Code d'autorisation requis pour les transferts

Oui. Outre la console Route 53, vous pouvez également obtenir le code de transfert à partir du registre .au.

DNSSEC

Prise en charge pour l'enregistrement de domaine. Lorsque vous définissez la clé, vous devez choisir l'algorithme de sécurité DNS 2 (DH). Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : entre 60 jours avant l'expiration et la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 29 jours après l'expiration
- Un domaine est supprimé de Route 53 : 29 jours après l'expiration
- Une restauration auprès du registre est possible : Non
- Un domaine est supprimé du registre : 30 jours après l'expiration

Suppression de l'enregistrement de domaine

Le registre des domaines .au ne permet pas de supprimer les enregistrements de domaine. Au lieu de cela, vous devez désactiver le renouvellement automatique et attendre l'expiration du

domaine. Pour de plus amples informations, veuillez consulter Suppression d'un enregistrement de nom de domaine.

Changement de propriété

Modifiez le propriétaire à l'aide de la console Route 53. Consultez Mise à jour des informations de contact pour un domaine. Effectuez ensuite le processus suivant pour effectuer le changement de propriétaire :

1. Les anciens et les nouveaux inscrits doivent cliquer sur le lien qu'ils reçoivent dans un e-mail envoyé par transfers@1api.net aux adresses e-mail répertoriées. Si ce processus n'est pas terminé dans les 14 jours, vous devez le recommencer.

2. Une fois les réponses confirmées, le changement de propriétaire dans le registre sera traité rapidement sans autre confirmation.

.cc (Iles Coco)

Return to index

Egalement utilisé comme domaine de premier niveau générique, souvent par des organismes dont le nom comprend « cc », par exemple des sociétés de conseil, des entreprises de cloud computing ou des clubs de cyclisme. Cette extension est une alternative populaire à « .com ».

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Restrictions

Accessible publiquement, sans aucune restriction.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

- Masqués – Adresse, numéro de téléphone, numéro de fax et adresse e-mail
- Non masqués – Nom du contact et nom de l'organisation

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Non pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre est possible : entre 30 jours et 60 jours après l'expiration
- Un domaine est supprimé du registre : 65 jours après l'expiration

.co.nz (Nouvelle-Zélande)

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Restrictions

Votre pouvez enregistrer les domaines de deuxième niveau suivants avec Route 53 : .co.nz, .net.nz et .org.nz. Vous ne pouvez pas enregistrer de domaines .nz (premier niveau) avec Route 53 ni transférer de domaines .nz vers Route 53.

Accessible publiquement, avec les restrictions suivantes :

- Les personnes physiques doivent être âgées d'au moins 18 ans.
- Les organisations doivent être enregistrées.

Protection de la confidentialité

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Non pris en charge. Nous vous recommandons d'empêcher les transferts non autorisés en limitant l'accès à l'action de l'RetrieveDomainAuthCodeAPI. (Lorsque vous limitez l'accès à cette API Route 53, vous limitez également les personnes autorisées à générer un code d'autorisation à

l'aide de la console Route 53 et d'autres méthodes de programmation.) AWS SDKs Pour de plus amples informations, veuillez consulter Identity and Access Management dans Amazon Route 53.

Noms de domaine internationaux

Pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 44 jours après l'expiration
- Une restauration auprès du registre est possible : entre 44 jours et 134 jours après l'expiration
- Le domaine est supprimé du registre : 134 jours après l'expiration

.com.au (Australie)

Return to index

E-mail de confirmation du registre TLD

Notre associé au bureau d'enregistrement, Gandi, revend les domaines .com.au via. DomainDirectors Lorsque vous transférez un nom de domaine vers Route 53, DomainDirectors envoyez un e-mail au contact du titulaire du domaine afin de vérifier les informations de contact ou d'autoriser les demandes de transfert.

Durée de validité de l'enregistrement et du renouvellement

Un à cinq ans.

Restrictions

Accessible publiquement, avec les restrictions suivantes :

- Les domaines .com.au et .net.au sont accessibles aux partenariats ou entrepreneurs individuels enregistrés en Australie, mais aussi aux entreprises étrangères autorisées à exercer une

activité en Australie, ainsi qu'aux propriétaires ou aux demandeurs d'une marque déposée australienne. Les individus ne peuvent pas enregistrer de domaines .com.au/.net.au. Le contact inscrit doit être une entreprise.

- Votre nom de domaine doit être identique à votre nom (celui enregistré auprès des autorités australiennes compétentes) ou à votre marque (ou à l'abréviation ou à l'acronyme de votre marque).
- Le nom de domaine doit indiquer votre activité. Par exemple, il doit indiquer un produit que vous vendez ou un service que vous fournissez.
- Pendant le processus d'enregistrement, vous devez fournir les informations suivantes :
  - Votre type d'enregistrement : votre numéro ABN (Australian Business Number), votre numéro ACN (Australian Company Number), votre numéro) ou votre TM (marque déposée) si le nom de domaine correspond à votre marque.
  - Votre ID d'enregistrement, peut être un numéro ABN (Australian Business Number), un numéro ACN (Australian Company Number) ou votre numéro de TM (marque déposée) si le nom de domaine correspond à votre marque.
  - Votre état ou province.
- Des informations de contact incorrectes ou non concordantes, y compris le nom, le numéro ABN ou le numéro de marque (TM), entraîneront des échecs d'enregistrement, de commerce et de renouvellement. Un changement de propriété peut s'avérer nécessaire pour corriger les informations relatives aux domaines existants.

Protection de la confidentialité

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Non pris en charge. Nous vous recommandons d'empêcher les transferts non autorisés en limitant l'accès à l'action de l'RetrieveDomainAuthCodeAPI. (Lorsque vous limitez l'accès à cette API Route 53, vous limitez également les personnes autorisées à générer un code d'autorisation à l'aide de la console Route 53 et d'autres méthodes de programmation.) AWS SDKs Pour de plus amples informations, veuillez consulter Identity and Access Management dans Amazon Route 53.

Noms de domaine internationaux

Non pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Lorsque vous définissez la clé, vous devez choisir l'algorithme de sécurité DNS 2 (DH). Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : entre 60 jours avant l'expiration et la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 29 jours après l'expiration
- Un domaine est supprimé de Route 53 : 29 jours après l'expiration
- Une restauration auprès du registre est possible : Non
- Un domaine est supprimé du registre : 30 jours après l'expiration

Suppression de l'enregistrement de domaine

Le registre des domaines .com.au ne permet pas de supprimer les enregistrements de domaine. Au lieu de cela, vous devez désactiver le renouvellement automatique et attendre l'expiration du domaine. Pour de plus amples informations, veuillez consulter Suppression d'un enregistrement de nom de domaine.

Changement de propriété

Modifiez le propriétaire, par programmation ou en utilisant la console Route 53. Consultez Mise à jour des informations de contact pour un domaine. Effectuez ensuite le processus suivant pour effectuer le changement de propriétaire :

1. Les anciens et les nouveaux inscrits doivent cliquer sur le lien qu'ils reçoivent dans un e-mail envoyé par transfers@1api.net aux adresses e-mail répertoriées. Si ce processus n'est pas terminé dans les 14 jours, vous devez le recommencer.

2. Une fois les réponses confirmées, le changement de propriétaire dans le registre sera traité rapidement sans autre confirmation.

.com.sg (République de Singapour)

> **Important**
>
> Vous ne pouvez plus utiliser Route 53 pour enregistrer de nouveaux domaines .com.sg ou transférer des domaines .com.sg vers Route 53. Nous continuons à prendre en charge les domaines .com.sg qui sont déjà inscrits auprès de Route 53.

Return to index

Période de renouvellement

Un ou deux ans.

Suppression de l'enregistrement de domaine

Le registre des domaines .com.sg ne permet pas de supprimer les enregistrements de domaine. Au lieu de cela, vous devez désactiver le renouvellement automatique et attendre l'expiration du domaine. Pour de plus amples informations, veuillez consulter Suppression d'un enregistrement de nom de domaine.

Protection de la confidentialité

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Code d'autorisation requis pour les transferts

Non pris en charge. Vous ne pouvez plus transférer de domaines .com.sg vers Route 53.

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 29 jours après l'expiration
- Un domaine est supprimé de Route 53 : 30 jours après l'expiration
- Une restauration auprès du registre est possible : entre 30 jours et 60 jours après l'expiration
- Un domaine est supprimé du registre : 60 jours après l'expiration

.fm (États fédérés de Micronésie)

Egalement utilisé comme domaine de premier niveau générique, souvent par des organisations impliquées dans la diffusion et les médias en ligne.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Restrictions

Accessible publiquement, sans aucune restriction.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 44 jours après l'expiration
- Une restauration auprès du registre est possible : entre 44 jours et 79 jours après l'expiration
- Un domaine est supprimé du registre : 84 jours après l'expiration

.in (Inde)

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Restrictions

Accessible publiquement, sans aucune restriction.

Protection de la confidentialité

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Non pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Non pris en charge.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 29 jours après l'expiration
- Un domaine est supprimé de Route 53 : 30 jours après l'expiration
- Une restauration auprès du registre est possible : entre 30 jours et 60 jours après l'expiration
- Un domaine est supprimé du registre : 65 jours après l'expiration

.jp (Japon)

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un an.

Restrictions

Accessible publiquement, avec une restriction :

- Seuls les personnes physiques ou les entreprises situées au Japon peuvent enregistrer un nom de domaine .jp.

Protection de la confidentialité

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le japonais.

Code d'autorisation requis pour les transferts

Oui.

Le registre .jp gère le code d'autorisation avec un time-to-live et il est possible qu'il expire. Vous pouvez actualiser le code d'authentification en supprimant le statut transfer lock (clientTransferProhibited) de votre domaine s'il est présent. Si le domaine ne possède aucun verrou de transfert, vous pouvez actualiser le code d'authentification en l'activant d'abord, puis en le désactivant.

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : entre 30 jours et 7 jours avant la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : Non
- Un domaine est supprimé de Route 53 : 6 jours avant l'expiration
- Une restauration auprès du registre est possible : contactez AWS Support.
- Un domaine est supprimé du registre : contactez AWS Support.

> **Note**
>
> L'enregistrement de domaines non-general-purpose JP tels que .co.jp et .or.jp n'est actuellement pas possible.

.io (Territoire Britannique de l'Océan Indien)

Egalement utilisé comme domaine de premier niveau générique, souvent par des organisations dans le domaine informatique comme des services en ligne, des jeux basés sur un navigateur et des startups.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Restrictions

Accessible publiquement, sans aucune restriction.

Protection de la confidentialité

Toutes les informations sont masquées à state/province l'exception du pays.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge.

Code d'autorisation requis pour les transferts

Oui

Le registre pour le domaines .io utilise également le code d'autorisation en tant que mot de passe à usage unique pour certaines opérations, telles que l'activation ou la désactivation de la protection de la vie privée. Si vous souhaitez exécuter plus d'une opération nécessitant un mot de passe, vous devez générer un autre code d'autorisation pour chaque opération.

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration

- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Le domaine est supprimé du registre : 90 jours après son expiration

.net.au (Australie)

Return to index

E-mail de confirmation du registre TLD

Notre associé au bureau d'enregistrement, Gandi, revend les domaines .net.au via. DomainDirectors Lorsque vous transférez un nom de domaine vers Route 53, DomainDirectors envoyez un e-mail au contact du titulaire du domaine afin de vérifier les informations de contact ou d'autoriser les demandes de transfert.

Durée de validité de l'enregistrement et du renouvellement

Un à cinq ans.

Restrictions

Seuls les domaines de deuxième niveau sont disponibles. Route 53 prend en charge les domaines de deuxième niveau .com.au et net.au.

Accessible publiquement, avec les restrictions suivantes :

- Les domaines .com.au et .net.au sont accessibles aux personnes morales, entités commerciales, partenariats ou entrepreneurs individuels enregistrés en Australie. Il est également accessible aux entreprises étrangères autorisées à exercer une activité en Australie, ainsi qu'aux propriétaires ou aux demandeurs d'une marque déposée australienne.
- Votre nom de domaine doit être identique à votre nom (celui enregistré auprès des autorités australiennes compétentes) ou à votre marque (ou une abréviation ou un acronyme de celle-ci).
- Le nom de domaine doit indiquer votre activité. Par exemple, il doit indiquer un produit que vous vendez ou un service que vous fournissez.
- Pendant le processus d'enregistrement, vous devez indiquer les éléments suivants :
  - Votre type d'enregistrement : votre numéro ABN (Australian Business Number), votre numéro ACN (Australian Company Number), votre numéro) ou votre TM (marque déposée) si le nom de domaine correspond à votre marque.

  - Votre ID d'enregistrement, peut être un numéro ABN (Australian Business Number), un numéro ACN (Australian Company Number) ou votre numéro de TM (marque déposée) si le nom de domaine correspond à votre marque.
  - Votre état ou province.
- Des informations de contact incorrectes ou non concordantes, y compris le nom, le numéro ABN ou le numéro de marque (TM), entraîneront des échecs d'enregistrement, de commerce et de renouvellement. Un changement de propriété peut s'avérer nécessaire pour corriger les informations relatives aux domaines existants.

Protection de la confidentialité

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Non pris en charge. Nous vous recommandons d'empêcher les transferts non autorisés en limitant l'accès à l'action de l'RetrieveDomainAuthCodeAPI. (Lorsque vous limitez l'accès à cette API Route 53, vous limitez également les personnes autorisées à générer un code d'autorisation à l'aide de la console Route 53 et d'autres méthodes de programmation.) AWS SDKs Pour de plus amples informations, veuillez consulter Identity and Access Management dans Amazon Route 53.

Noms de domaine internationaux

Non pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Lorsque vous définissez la clé, vous devez choisir l'algorithme de sécurité DNS 2 (DH). Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : entre 60 jours avant l'expiration et la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 29 jours après l'expiration
- Un domaine est supprimé de Route 53 : 29 jours après l'expiration
- Une restauration auprès du registre est possible : Non
- Un domaine est supprimé du registre : 30 jours après l'expiration

Suppression de l'enregistrement de domaine

Le registre des domaines .net.au ne permet pas de supprimer les enregistrements de domaine. Au lieu de cela, vous devez désactiver le renouvellement automatique et attendre l'expiration du domaine. Pour de plus amples informations, veuillez consulter Suppression d'un enregistrement de nom de domaine.

Changement de propriété

Modifiez le propriétaire, par programmation ou en utilisant la console Route 53. Consultez Mise à jour des informations de contact pour un domaine. Effectuez ensuite le processus suivant pour effectuer le changement de propriétaire :

1. Les anciens et les nouveaux inscrits doivent cliquer sur le lien qu'ils reçoivent dans un e-mail envoyé par transfers@1api.net aux adresses e-mail répertoriées. Si ce processus n'est pas terminé dans les 14 jours, vous devez le recommencer.

2. Une fois les réponses confirmées, le changement de propriétaire dans le registre sera traité rapidement sans autre confirmation.

.net.nz (Nouvelle-Zélande)

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Restrictions

Votre pouvez enregistrer les domaines de deuxième niveau suivants avec Route 53 : .co.nz, .net.nz et .org.nz. Vous ne pouvez pas enregistrer de domaines .nz (premier niveau) avec Route 53 ni transférer de domaines .nz vers Route 53.

Accessible publiquement, avec les restrictions suivantes :

- Les personnes physiques doivent être âgées d'au moins 18 ans.
- Les organisations doivent être enregistrées.

Protection de la confidentialité

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Non pris en charge. Nous vous recommandons d'empêcher les transferts non autorisés en limitant l'accès à l'action de l'RetrieveDomainAuthCodeAPI. (Lorsque vous limitez l'accès à cette API Route 53, vous limitez également les personnes autorisées à générer un code d'autorisation à l'aide de la console Route 53 et d'autres méthodes de programmation.) AWS SDKs Pour de plus amples informations, veuillez consulter Identity and Access Management dans Amazon Route 53.

Noms de domaine internationaux

Pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 44 jours après l'expiration
- Une restauration auprès du registre est possible : entre 44 jours et 134 jours après l'expiration
- Le domaine est supprimé du registre : 134 jours après l'expiration

.org.nz (Nouvelle-Zélande)

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Restrictions

Votre pouvez enregistrer les domaines de deuxième niveau suivants avec Route 53 : .co.nz, .net.nz et .org.nz. Vous ne pouvez pas enregistrer de domaines .nz (premier niveau) avec Route 53 ni transférer de domaines .nz vers Route 53.

Accessible publiquement, avec les restrictions suivantes :

- Les personnes physiques doivent être âgées d'au moins 18 ans.
- Les organisations doivent être enregistrées.

Protection de la confidentialité

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Non pris en charge. Nous vous recommandons d'empêcher les transferts non autorisés en limitant l'accès à l'action de l'RetrieveDomainAuthCodeAPI. (Lorsque vous limitez l'accès à cette API Route 53, vous limitez également les personnes autorisées à générer un code d'autorisation à l'aide de la console Route 53 et d'autres méthodes de programmation.) AWS SDKs Pour de plus amples informations, veuillez consulter Identity and Access Management dans Amazon Route 53.

Noms de domaine internationaux

Pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 44 jours après l'expiration
- Une restauration auprès du registre est possible : entre 44 jours et 134 jours après l'expiration
- Le domaine est supprimé du registre : 134 jours après l'expiration

.pw (Palaos)

Return to index

Le .pw était à l'origine réservé aux résidents de Palau, un pays insulaire de la sous-région de Micronésie en Océanie, dans le Pacifique occidental, mais il est maintenant couramment utilisé pour représenter le « Web professionnel » et est accessible à tous.

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Protection de la confidentialité (s'applique à tous les types de contacts : personne, société, association et organisme public)

Toutes les informations sont masquées à l'exception du nom de l'organisation.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : 75 jours après l'expiration

.qa (Qatar)

> **Important**
>
> Vous ne pouvez plus utiliser Route 53 pour enregistrer de nouveaux domaines .qa ou transférer des domaines .qa vers Route 53. Nous continuons à prendre en charge les domaines .qa qui sont déjà inscrits auprès de Route 53.

Return to index

Période de renouvellement

Un à cinq ans.

Protection de la confidentialité

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Non pris en charge. Nous vous recommandons d'empêcher les transferts non autorisés en limitant l'accès à l'action de l'RetrieveDomainAuthCodeAPI. (Lorsque vous limitez l'accès à cette API Route 53, vous limitez également les personnes autorisées à générer un code d'autorisation à l'aide de la console Route 53 et d'autres méthodes de programmation.) AWS SDKs Pour de plus amples informations, veuillez consulter Identity and Access Management dans Amazon Route 53.

Code d'autorisation requis pour les transferts

Non pris en charge. Vous ne pouvez plus transférer de domaines .qa vers Route 53.

DNSSEC

Non pris en charge.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 29 jours après l'expiration
- Un domaine est supprimé de Route 53 : 30 jours après l'expiration
- Une restauration auprès du registre est possible : Non
- Un domaine est supprimé du registre : 31 jours après l'expiration

.ru (Fédération de Russie)

> **Important**
>
> Vous ne pouvez plus utiliser Route 53 pour enregistrer de nouveaux domaines .ru ou transférer des domaines .ru vers Route 53. Nous continuons à prendre en charge les domaines .ru qui sont déjà inscrits auprès de Route 53.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un an.

> **Note**
>
> Le registre pour les domaines .ru met à jour la date d'expiration d'un domaine le jour où le domaine expire. Les requêtes WHOIS afficheront l'ancienne date d'expiration pour le domaine jusqu'à cette date, quelle que soit la date à laquelle vous renouvelez le domaine avec Route 53.

Restrictions

Accessible publiquement, avec les restrictions suivantes :

- Les personnes physiques peuvent devoir fournir un numéro de passport ou le numéro d'identification émis par le gouvernement.
- Les entreprises étrangères peuvent devoir fournir l'ID de l'entreprise ou l'enregistrement de l'entreprise.

Protection de la confidentialité

Déterminé par le registre.

Domaine de verrouillage pour empêcher les transferts non autorisés

Non pris en charge. Nous vous recommandons d'empêcher les transferts non autorisés en limitant l'accès à l'action de l'RetrieveDomainAuthCodeAPI. (Lorsque vous limitez l'accès à cette API Route 53, vous limitez également les personnes autorisées à générer un code d'autorisation à l'aide de la console Route 53 et d'autres méthodes de programmation.) AWS SDKs Pour de plus amples informations, veuillez consulter Identity and Access Management dans Amazon Route 53.

Noms de domaine internationaux

Non pris en charge.

Code d'autorisation requis pour les transferts

Non pris en charge. Vous ne pouvez plus transférer de domaines .ru vers Route 53.

DNSSEC

Non pris en charge.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à 2 jours avant la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : Non
- Un domaine est supprimé de Route 53 : 2 jours avant l'expiration
- Une restauration auprès du registre est possible : entre 2 jour avant et 28 jours après l'expiration
- Un domaine est supprimé du registre : 28 jours après l'expiration

Suppression de l'enregistrement de domaine

Le registre des domaines .ru ne permet pas de supprimer les enregistrements de domaine. Au lieu de cela, vous devez désactiver le renouvellement automatique et attendre l'expiration du domaine. Pour de plus amples informations, veuillez consulter Suppression d'un enregistrement de nom de domaine.

.sg (République de Singapour)

> **Important**
>
> Vous ne pouvez plus utiliser Route 53 pour enregistrer de nouveaux domaines .sg ou transférer des domaines .sg vers Route 53. Nous continuons à prendre en charge les domaines .sg qui sont déjà inscrits auprès de Route 53.

Return to index

Période de renouvellement

Un ou deux ans.

Protection de la confidentialité

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Code d'autorisation requis pour les transferts

Non pris en charge. Vous ne pouvez plus transférer de domaines .sg vers Route 53.

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 29 jours après l'expiration
- Un domaine est supprimé de Route 53 : 30 jours après l'expiration
- Une restauration auprès du registre est possible : entre 30 jours et 60 jours après l'expiration
- Un domaine est supprimé du registre : 60 jours après l'expiration

Suppression de l'enregistrement de domaine

Le registre des domaines .sg ne permet pas de supprimer les enregistrements de domaine. Au lieu de cela, vous devez désactiver le renouvellement automatique et attendre l'expiration du domaine. Pour de plus amples informations, veuillez consulter Suppression d'un enregistrement de nom de domaine.

Europe

Vous pouvez utiliser les domaines de premier niveau (TLDs) suivants pour l'Europe afin d'enregistrer des domaines auprès d'Amazon Route 53.

, , , ,

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge.

Code d'autorisation requis pour les transferts

Oui. Vous pouvez obtenir le code de transfert sur le site Web de DNS Belgium.

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : Non
- Un domaine est supprimé de Route 53 : à la date d'expiration
- Une restauration auprès du registre est possible : jusqu'à 40 jours après l'expiration
- Un domaine est supprimé du registre : 40 jours après l'expiration

.berlin (ville de Berlin en Allemagne)

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Restrictions

Accessible publiquement, avec les restrictions suivantes :

- Le contact inscrit, administratif ou technique doit fournir une adresse à Berlin, et le contact administratif doit être une personne physique.
- Vous devez activer et utiliser votre domaine .berlin dans les 12 mois après son enregistrement (cela s'applique à un site web, à une redirection ou à une adresse e-mail).
- Si vous publiez un site web dans votre domaine .berlin ou si votre domaine .berlin redirige vers un autre site web, le contenu du site web doit avoir un lien avec Berlin.

Protection de la confidentialité

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le latin et le cyrillique.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Le domaine est supprimé du registre : 80 jours après l'expiration

.ch (Suisse)

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un an.

Restrictions

Accessible publiquement, sans aucune restriction.

Protection de la confidentialité

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Non pris en charge. Nous vous recommandons d'empêcher les transferts non autorisés en limitant l'accès à l'action de l'RetrieveDomainAuthCodeAPI. (Lorsque vous limitez l'accès à cette API Route 53, vous limitez également les personnes autorisées à générer un code d'autorisation à l'aide de la console Route 53 et d'autres méthodes de programmation.) AWS SDKs Pour de plus amples informations, veuillez consulter Identity and Access Management dans Amazon Route 53.

Noms de domaine internationaux

Pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 9 jours après l'expiration
- Un domaine est supprimé de Route 53 : 9 jours après l'expiration
- Une restauration auprès du registre est possible : entre 9 jours et 49 jours après l'expiration
- Un domaine est supprimé du registre : 49 jours après l'expiration

.co.uk (Royaume-Uni)

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Restrictions

Accessible publiquement, sans aucune restriction.

Protection de la confidentialité

Toutes les informations sont masquées.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge

Noms de domaine internationaux

Non pris en charge.

Code d'autorisation requis pour les transferts

Si vous transférez un domaine .co.uk vers Route 53, vous n'avez pas besoin de code d'autorisation. Au lieu de cela, utilisez la méthode fournie par votre bureau d'enregistrement de domaine actuel pour remplacer la valeur de la balise IPS pour le domaine par GANDI, écrit en majuscules. (Nominet, le registre des noms de domaine .uk, requiert une balise IPS). Si votre bureau d'enregistrement ne modifie pas la valeur de la balise IPS, contactez Nominet.

> **Note**
>
> Lorsque vous enregistrez un domaine .co.uk, Route 53 définit automatiquement la balise IPS du domaine sur GANDI.

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : entre 180 jours avant et 30 jours après la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : entre 30 jours et 90 jours après l'expiration
- Un domaine est supprimé de Route 53 : 90 jours après l'expiration
- Une restauration auprès du registre est possible : Non
- Un domaine est supprimé du registre : 92 jours après l'expiration

Suppression de l'enregistrement de domaine

Le registre des domaines .co.uk ne permet pas de supprimer les enregistrements de domaine. Au lieu de cela, vous devez désactiver le renouvellement automatique et attendre l'expiration du domaine. Pour de plus amples informations, veuillez consulter Suppression d'un enregistrement de nom de domaine.

.cz (République tchèque)

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Restrictions

Accessible publiquement, sans aucune restriction.

Protection de la confidentialité

Non prise en charge, mais l'adresse e-mail et le numéro de téléphone sont masqués pour tous les contacts.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Non pris en charge.

Code d'autorisation requis pour les transferts

Oui

Si votre bureau d'enregistrement actuel ne fournit pas de code d'autorisation, accédez à `https://www.nic.cz/whois/send-password/` pour demander qu'il soit envoyé à l'adresse e-mail du titulaire par le registre de domaines CZ.

DNSSEC

Non pris en charge.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 58 jours après l'expiration
- Un domaine est supprimé de Route 53 : 59 jours après l'expiration
- Une restauration auprès du registre est possible : Non
- Un domaine est supprimé du registre : 60 jours après l'expiration

.de (Allemagne)

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un an.

Restrictions

Accessible publiquement, avec les restrictions suivantes :

- Vous devez résider en Allemagne ou l'un de vos contacts administratifs (personne physique) doit résider en Allemagne et disposer d'une adresse autre qu'une boîte postale.
- Pendant l'enregistrement, le DNS (A, MX et CNAME) du nom de domaine doit être correctement configuré afin de passer avec succès la vérification de la zone de l'enregistrement. Trois serveurs de deux catégories C différentes sont requis.
- Si vous utilisez un service DNS autre que Route 53, les serveurs de noms du domaine doivent faire l'objet d'une vérification, afin de s'assurer qu'ils sont correctement configurés. Pour déterminer si les serveurs de noms de votre domaine passeront le test, consultez https://www.denic. de/en/service/tools/nast/.

Protection de la confidentialité

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Non pris en charge. Nous vous recommandons d'empêcher les transferts non autorisés en limitant l'accès à l'action de l'RetrieveDomainAuthCodeAPI. (Lorsque vous limitez l'accès à cette API Route 53, vous limitez également les personnes autorisées à générer un code d'autorisation à l'aide de la console Route 53 et d'autres méthodes de programmation.) AWS SDKs Pour de plus amples informations, veuillez consulter Identity and Access Management dans Amazon Route 53.

Noms de domaine internationaux

Pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : Non
- Un domaine est supprimé de Route 53 : à la date d'expiration
- Une restauration auprès du registre est possible : contactez AWS Support.
- Un domaine est supprimé du registre : contactez AWS Support.

.es (Espagne)

Return to index

Achat de domaine ou transfert

> **Important**
>
> Vous pouvez actuellement acheter de nouveaux noms de domaine .es ou transférer des domaines .es vers Route 53. Le type de contact pour le contact du titulaire n'est soumis à aucune restriction. Le type de contact administrateur/technique/facturation doit être une personne.

Durée de validité de l'enregistrement et du renouvellement

Un à cinq ans.

Restrictions

Accessible publiquement, à ceux qui éprouvent un intérêt ou qui ont un lien avec l'Espagne.

Depuis 2016, les titulaires de domaine .ES doivent fournir une adresse e-mail de contact. Si vous n'avez pas fourni ces informations, vous devez le faire auprès du bureau d'enregistrement actuel avant de transférer votre domaine vers Route 53.

Vous aurez besoin des informations suivantes :

- Identifiant ESNIC similaire à. `AAAA0-ESNIC-F0`
- Si vous ne connaissez pas l'identifiant ESNIC, vous pouvez l'obtenir du bureau d'enregistrement actuel. Vous pouvez trouver votre bureau d'enregistrement à l'adresse suivante : https://www.dominios.es/en.

Selon que vous vous souvenez ou non de votre mot de passe au bureau d'enregistrement, vous pouvez suivre l'une des procédures suivantes pour mettre à jour votre adresse e-mail d'inscrit :

- Si vous vous souvenez de votre mot de passe, connectez-vous sur https://www.nic. es/sgnd/login.action en utilisant vos identifiants ESNIC et votre mot de passe.

  Une fois connecté, vous pouvez modifier l'adresse e-mail de contact du titulaire en choisissant l'onglet Modifier sur la page de registre.
- Si vous avez oublié votre mot de passe, rendez-vous sur https://www.nic. es/sgnd/peticion/editCorreo.action ? request_locale=fr.

  Remplissez le formulaire avec votre identifiant ESNIC, votre nouvelle adresse e-mail de contact valide d'inscrit. Validez ensuite le formulaire en choisissant Traitement sans eID/certificat, puis téléchargez le document d'identité demandé.

Protection de la confidentialité

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge

Noms de domaine internationaux

Pris en charge.

Code d'autorisation requis pour les transferts

Oui

Le registre .es gère le code d'autorisation avec un time-to-live et il est possible qu'il expire. Vous pouvez actualiser le code d'authentification en supprimant le statut transfer lock (clientTransferProhibited) de votre domaine s'il est présent. Si le domaine ne possède aucun verrou de transfert, vous pouvez actualiser le code d'authentification en l'activant d'abord, puis en le désactivant.

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à 6 jours avant la date d'expiration

- Un renouvellement tardif avec Route 53 est possible : Non
- Un domaine est supprimé de Route 53 : 6 jours avant l'expiration
- Une restauration auprès du registre est possible : entre 6 jour avant et 4 jours après l'expiration
- Un domaine est supprimé du registre : 4 jours après l'expiration

.eu (Union européenne)

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Restrictions

Accessible publiquement, avec une restriction :

- Vous devez fournir une adresse postale valide provenant de l'un des 30 États de l'Espace économique européen (EEE) ; si vous êtes citoyen de l'un des 27 États membres de l'Union européenne (UE), vous devez indiquer votre pays de citoyenneté de l'UE.

Protection de la confidentialité

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Non pris en charge. Nous vous recommandons d'empêcher les transferts non autorisés en limitant l'accès à l'action de l'RetrieveDomainAuthCodeAPI. (Lorsque vous limitez l'accès à cette API Route 53, vous limitez également les personnes autorisées à générer un code d'autorisation à l'aide de la console Route 53 et d'autres méthodes de programmation.) AWS SDKs Pour de plus amples informations, veuillez consulter Identity and Access Management dans Amazon Route 53.

Noms de domaine internationaux

Pris en charge.

Code d'autorisation requis pour les transferts

Oui

Vous pouvez également générer le code d'authentification en utilisant le panneau « My.EU » du registre : https://my.eurid.eu/.

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : Non
- Un domaine est supprimé de Route 53 : à la date d'expiration
- Une restauration auprès du registre est possible : jusqu'à 40 jours après l'expiration
- Un domaine est supprimé du registre : 40 jours après l'expiration

Recherche WHOIS

Pour en savoir plus sur les domaines .eu existants, consultez https://whois.eurid.eu/en/.

.fi (Finlande)

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à cinq ans.

Restrictions

Accessible publiquement, avec les restrictions suivantes :

- L'extension .fi est disponible pour les personnes physiques qui ont un domicile en Finlande et un numéro d'identité finlandais, ainsi que les personnes morales ou entrepreneurs privés enregistrés en Finlande.
- Si l'adresse du contact inscrit est en Finlande, le numéro d'identité finlandais est requis pour un inscrit individuel et le numéro d'entreprise finlandais est requis pour une société inscrite et vous devez fournir les informations suivantes pendant l'inscription :
  - Si le contact s'appuie sur une personne physique ou morale en Finlande.
  - L'identifiant du registre dans lequel le nom est enregistré, s'il est basé sur le nom d'une personne morale.
  - Le numéro de l'enregistrement dans le registre dans lequel le nom est enregistré, s'il est basé sur le nom d'une personne morale.
  - Le numéro d'identification d'une personne morale en Finlande.

  - Le numéro d'identification d'une personne physique en Finlande.
  - Si le déclarant est une société non finlandaise, vous devez fournir le numéro d'entreprise sous forme de numéro de TVA.
- Si l'adresse de l'inscrit n'est pas située en Finlande, aucun numéro d'identité ou de société finlandais n'est requis.

Protection de la confidentialité

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Non pris en charge. Nous vous recommandons d'empêcher les transferts non autorisés en limitant l'accès à l'action de l'RetrieveDomainAuthCodeAPI. (Lorsque vous limitez l'accès à cette API Route 53, vous limitez également les personnes autorisées à générer un code d'autorisation à l'aide de la console Route 53 et d'autres méthodes de programmation.) AWS SDKs Pour de plus amples informations, veuillez consulter Identity and Access Management dans Amazon Route 53.

Noms de domaine internationaux

Pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 29 jours après l'expiration
- Un domaine est supprimé de Route 53 : 30 jours après l'expiration
- Une restauration auprès du registre est possible : Non
- Un domaine est supprimé du registre : Non

Suppression de l'enregistrement de domaine

Pour plus d'informations sur la suppression des domaines, consultez Suppression d'un enregistrement de nom de domaine.

.fr (France)

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Restrictions

Accessible publiquement, avec les restrictions suivantes :

- Les individus doivent être âgés d'au moins 18 ans et doivent fournir leurdate-of-birth.
- Les organisations doivent être situées dans l'espace économique européen ou en Suisse.
- Les organisations doivent remplir tous les champs d'identification de l'entreprise (numéros TVA, SIREN, WALDEC, DUNS, etc). Toute vérification effectuée par l'AFNIC ultérieurement sera ainsi simplifiée.
- Les mêmes conditions d'éligibilité s'appliquent au contact administratif.
- Les noms et les termes sont soumis à une vérification préalable par l'AFNIC (Charte de nommage, article 2.4) et aux conditions supplémentaires suivantes :
  - Les noms de domaine précédemment réservés ou interdits sont ouverts aux candidats qui justifient d'un droit légitime et agissent de bonne foi.
  - Les noms commençant par les termes ville, mairie, agglo, cc, cg et cr sont soumis aux conventions de nommage de l'AFNIC.

Protection de la confidentialité

Déterminé par le registre.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 27 jours après l'expiration
- Un domaine est supprimé de Route 53 : 28 jours après l'expiration
- Une restauration auprès du registre est possible : entre 28 jours et 58 jours après l'expiration
- Un domaine est supprimé du registre : 58 jours après l'expiration

.gg (Guernesey)

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un an.

Restrictions

Accessible publiquement, sans aucune restriction.

Protection de la confidentialité

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration

- Un renouvellement tardif avec Route 53 est possible : jusqu'à 29 jours après l'expiration
- Un domaine est supprimé de Route 53 : 30 jours après l'expiration
- Une restauration auprès du registre est possible : entre 30 jours et 35 jours après l'expiration
- Un domaine est supprimé du registre : 35 jours après l'expiration

.im (Ile de Man)

Egalement utilisé comme domaine de premier niveau générique, souvent par les services de messagerie instantanée ou les personnes qui souhaitent développer une marque personnelle.

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un ou deux ans.

Restrictions

Accessible publiquement, sans aucune restriction.

Protection de la confidentialité

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Non pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Non pris en charge.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 29 jours après l'expiration

- Un domaine est supprimé de Route 53 : 30 jours après l'expiration
- Une restauration auprès du registre est possible : Non
- Un domaine est supprimé du registre : 30 jours après l'expiration

.it (Italie)

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un an.

Restrictions

Accessible publiquement, avec les restrictions suivantes :

- Les personnes physiques ou les organisations doivent avoir une adresse enregistrée dans l'Union européenne.
- Si votre pays d'origine est l'Italie, vous devez entrer un code fiscal. Si votre pays d'origine est un pays de l'Union européenne, vous devez entrer un numéro de document d'identité (numéro ID).
- Les serveurs de noms de votre domaine doivent réussir un contrôle DNS. Nous vous suggérons de vérifier les serveurs de noms sur https://dns-check.nic.it/ avant de soumettre la demande de modification. Si votre nom de domaine n'est pas conforme aux exigences techniques (par exemple, il n'est pas associé à un serveur de noms opérationnel), et si vous ne le corrigez pas dans les 30 jours, il sera supprimé par le registre. Nous ne proposons pas de remboursement pour les domaines qui sont supprimés, car ils ne répondent aux exigences techniques.

Protection de la confidentialité

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Non pris en charge. Nous vous recommandons d'empêcher les transferts non autorisés en limitant l'accès à l'action de l'RetrieveDomainAuthCodeAPI. (Lorsque vous limitez l'accès à cette API Route 53, vous limitez également les personnes autorisées à générer un code d'autorisation à l'aide de la console Route 53 et d'autres méthodes de programmation.) AWS SDKs Pour de plus amples informations, veuillez consulter Identity and Access Management dans Amazon Route 53.

Noms de domaine internationaux

Pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Non pris en charge.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 13 jours après l'expiration
- Un domaine est supprimé du registre : 49 jours après l'expiration
- Une restauration auprès du registre est possible : entre 14 jours et 44 jours après l'expiration
- Un domaine est supprimé du registre : contactez AWS Support.

.me (Monténégro)

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Restrictions

Domain.me, le registre pour les domaines .me, considère les noms de domaine à deux lettres et certains noms de domaine plus longs comme des noms de domaine premium. Vous ne pouvez pas enregistrer des domaines .me premium avec Route 53 ni les transférer vers celui-ci. Pour plus d'informations sur les noms de domaine .me premium, consultez le site web domain.me.

Protection de la confidentialité

Toutes les informations sont masquées.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Prise en charge pour les langues suivantes : allemand, arabe, biélorusse, bosniaque, bulgare, chinois simplifié, chinois traditionnel, croate, danois, français, hindi, hongrois, islandais, italien, coréen, letton, lituanien, mongol, monténégrin, polonais, portugais, russe, serbe, espagnol, suédois, turc et ukrainien.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 29 jours après l'expiration
- Un domaine est supprimé de Route 53 : 30 jours après l'expiration
- Une restauration auprès du registre est possible : entre 30 jours et 60 jours après l'expiration
- Un domaine est supprimé du registre : 65 jours après l'expiration

.me.uk (Royaume-Uni)

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Restrictions

Accessible publiquement, sans aucune restriction.

Protection de la confidentialité

Toutes les informations sont masquées.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge

Noms de domaine internationaux

Non pris en charge.

Code d'autorisation requis pour les transferts

Si vous transférez un domaine .me.uk vers Route 53, vous n'avez pas besoin de code d'autorisation. Au lieu de cela, utilisez la méthode fournie par votre bureau d'enregistrement de domaine actuel pour remplacer la valeur de la balise IPS pour le domaine par GANDI, écrit en

majuscules. (Nominet, le registre des noms de domaine .uk, requiert une balise IPS). Si votre bureau d'enregistrement ne modifie pas la valeur de la balise IPS, contactez Nominet.

> **Note**
>
> Lorsque vous enregistrez un domaine .me.uk, Route 53 définit automatiquement la balise IPS du domaine sur GANDI.

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : entre 180 jours avant et 30 jours après la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : entre 30 jours et 90 jours après l'expiration
- Un domaine est supprimé de Route 53 : 90 jours après l'expiration
- Une restauration auprès du registre est possible : Non
- Un domaine est supprimé du registre : 92 jours après l'expiration

Suppression de l'enregistrement de domaine

Le registre des domaines .me.uk ne permet pas de supprimer les enregistrements de domaine. Au lieu de cela, vous devez désactiver le renouvellement automatique et attendre l'expiration du domaine. Pour de plus amples informations, veuillez consulter Suppression d'un enregistrement de nom de domaine.

.nl (Pays-Bas)

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un an.

Restrictions

Accessible publiquement, avec les restrictions suivantes :

- Le contact inscrit ou administratif doit fournir une adresse valide aux Pays-Bas. Une présence locale est obligatoire.
- Si vous n'avez pas d'adresse valide aux Pays-Bas, le registre SIDN vous fournira une adresse de résidence, conformément à la procédure relative aux adresses de résidence.
- Le nom de domaine doit comporter 3 à 63 caractères, à l'exclusion de .nl.

Protection de la confidentialité

Déterminé par le registre.

Domaine de verrouillage pour empêcher les transferts non autorisés

Non pris en charge. Nous vous recommandons d'empêcher les transferts non autorisés en limitant l'accès à l'action de l'RetrieveDomainAuthCodeAPI. (Lorsque vous limitez l'accès à cette API Route 53, vous limitez également les personnes autorisées à générer un code d'autorisation à l'aide de la console Route 53 et d'autres méthodes de programmation.) AWS SDKs Pour de plus amples informations, veuillez consulter Identity and Access Management dans Amazon Route 53.

Noms de domaine internationaux

Non pris en charge.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à 1 jour avant la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : Non
- Un domaine est supprimé de Route 53 : 1 jour avant l'expiration
- Une restauration auprès du registre est possible : entre 1 jour avant et 39 jours après l'expiration
- Un domaine est supprimé du registre : 39 jours après l'expiration

.org.uk (Royaume-Uni)

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Restrictions

Accessible publiquement, sans aucune restriction.

Protection de la confidentialité

Toutes les informations sont masquées.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge

Noms de domaine internationaux

Non pris en charge.

Code d'autorisation requis pour les transferts

Si vous transférez un domaine .org.uk vers Route 53, vous n'avez pas besoin de code d'autorisation. Au lieu de cela, utilisez la méthode fournie par votre bureau d'enregistrement de domaine actuel pour remplacer la valeur de la balise IPS pour le domaine par GANDI, écrit en majuscules. (Nominet, le registre des noms de domaine .uk, requiert une balise IPS). Si votre bureau d'enregistrement ne modifie pas la valeur de la balise IPS, contactez Nominet.

> **Note**
>
> Lorsque vous enregistrez un domaine .org.uk, Route 53 définit automatiquement la balise IPS du domaine sur GANDI.

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : entre 180 jours avant et 30 jours après la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : entre 30 jours et 90 jours après l'expiration
- Un domaine est supprimé de Route 53 : 90 jours après l'expiration

- Une restauration auprès du registre est possible : Non
- Un domaine est supprimé du registre : 92 jours après l'expiration

Suppression de l'enregistrement de domaine

Le registre des domaines .org.uk ne permet pas de supprimer les enregistrements de domaine. Au lieu de cela, vous devez désactiver le renouvellement automatique et attendre l'expiration du domaine. Pour de plus amples informations, veuillez consulter Suppression d'un enregistrement de nom de domaine.

.ruhr (région de la Ruhr, ouest de l'Allemagne)

Return to index

L'extension .ruhr correspond à la région de la Ruhr (ouest de l'Allemagne).

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Restrictions

Accessible publiquement, avec une restriction :

- Le contact administratif doit être une personne physique ayant une adresse en Allemagne.

Protection de la confidentialité

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge (ä, ö, ü, ß).

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Un domaine est supprimé du registre : contactez AWS Support.

.se (Suède)

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Restrictions

Accessible publiquement, avec les restrictions suivantes :

- Si vous êtes situé en Suède, vous devez fournir un numéro d'identification suédoise valide. Le format du numéro d'identification est`YYMMDD-NNNN`.
- Si vous êtes situé en dehors de la Suède, vous devez entrer un numéro d'identification valide, par exemple un numéro d'identification fiscale.

Protection de la confidentialité

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Non pris en charge. Nous vous recommandons d'empêcher les transferts non autorisés en limitant l'accès à l'action de l'RetrieveDomainAuthCodeAPI. (Lorsque vous limitez l'accès à cette API Route 53, vous limitez également les personnes autorisées à générer un code d'autorisation à l'aide de la console Route 53 et d'autres méthodes de programmation.) AWS SDKs Pour de plus amples informations, veuillez consulter Identity and Access Management dans Amazon Route 53.

Noms de domaine internationaux

Pris en charge pour le latin, le suédois et le yiddish.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à 1 jour avant la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : Non
- Un domaine est supprimé de Route 53 : 1 jour avant l'expiration
- Une restauration auprès du registre est possible : entre 1 jour avant et 59 jours après l'expiration
- Un domaine est supprimé du registre : 64 jours après l'expiration

.uk (Royaume-Uni)

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Restrictions

Accessible publiquement, sans aucune restriction.

Protection de la confidentialité

Toutes les informations sont masquées.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge

Noms de domaine internationaux

Non pris en charge.

Code d'autorisation requis pour les transferts

Si vous transférez un domaine .uk vers Route 53, vous n'avez pas besoin de code d'autorisation. Au lieu de cela, utilisez la méthode fournie par votre bureau d'enregistrement de domaine actuel pour remplacer la valeur de la balise IPS pour le domaine par GANDI, écrit en majuscules. (Nominet, le registre des noms de domaine .uk, requiert une balise IPS). Si votre bureau d'enregistrement ne modifie pas la valeur de la balise IPS, contactez Nominet.

> **Note**
>
> Lorsque vous enregistrez un domaine .uk, Route 53 définit automatiquement la balise IPS du domaine sur GANDI.

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : entre 180 jours avant et 30 jours après la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : entre 30 jours et 90 jours après l'expiration
- Un domaine est supprimé de Route 53 : 90 jours après l'expiration
- Une restauration auprès du registre est possible : Non
- Un domaine est supprimé du registre : 92 jours après l'expiration

Suppression de l'enregistrement de domaine

Le registre des domaines .uk ne permet pas de supprimer les enregistrements de domaine. Au lieu de cela, vous devez désactiver le renouvellement automatique et attendre l'expiration du domaine. Pour de plus amples informations, veuillez consulter Suppression d'un enregistrement de nom de domaine.

.wien (ville de Vienne en Autriche)

Return to index

Durée de validité de l'enregistrement et du renouvellement

Un à dix ans.

Restrictions

Accessible publiquement, avec les restrictions suivantes :

- Vous devez présenter une affinité d'ordre économique, culturel, touristique, historique, social ou toute autre affinité avec la ville de Vienne en Autriche.

- Les noms de domaine .wien doivent être utilisés dans le cadre des conditions ci-dessus, tout au long de la durée de l'enregistrement.

Protection de la confidentialité

Non pris en charge.

Domaine de verrouillage pour empêcher les transferts non autorisés

Pris en charge.

Noms de domaine internationaux

Pris en charge pour le latin.

Code d'autorisation requis pour les transferts

Oui

DNSSEC

Prise en charge pour l'enregistrement de domaine. Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

Délais pour le renouvellement et la restauration de domaines

- Un renouvellement est possible : jusqu'à la date d'expiration
- Un renouvellement tardif avec Route 53 est possible : jusqu'à 44 jours après l'expiration
- Un domaine est supprimé de Route 53 : 45 jours après l'expiration
- Une restauration auprès du registre : entre 45 jours et 75 jours après l'expiration
- Le domaine est supprimé du registre : 80 jours après l'expiration

Configuration d'Amazon Route 53 en tant que service DNS

Vous pouvez utiliser Amazon Route 53 en tant que service DNS pour votre domaine, par exemple, example.com. Lorsque Route 53 est votre service DNS, il achemine le trafic Internet vers votre site web en traduisant les noms de domaine descriptifs, tels que www.example.com, en adresses IP numériques, telles que 192.0.2.1, qui sont utilisées par les ordinateurs pour se connecter les uns aux autres. Lorsque quelqu'un entre votre nom de domaine dans un navigateur ou vous envoie un e-mail, une requête DNS est envoyée à Route 53, qui répond avec la valeur appropriée. Par exemple, Route 53 peut répondre avec l'adresse IP du serveur web pour example.com.

Dans ce chapitre, nous expliquons comment configurer Route 53 pour acheminer le trafic Internet vers les emplacements appropriés. Nous expliquons également comment migrer le service DNS vers Route 53 si vous utilisez actuellement un autre service DNS, et comment utiliser Route 53 en tant que service DNS pour un nouveau domaine.

Rubriques

- Configuration d'Amazon Route 53 en tant que service DNS d'un domaine existant
- Configuration du routage DNS pour un nouveau domaine
- Acheminement du trafic vers vos ressources
- Utilisation de zones hébergées
- Utilisation des enregistrements
- Configuration de la signature DNSSEC dans Amazon Route 53
- Utilisation AWS Cloud Map pour créer des dossiers et des bilans de santé
- Contraintes et comportements DNS

Configuration d'Amazon Route 53 en tant que service DNS d'un domaine existant

Si vous transférez un ou plusieurs enregistrements de domaine vers Route 53, et que vous utilisez actuellement un bureau d'enregistrement de domaine qui ne fournit pas de service DNS payant, vous devez migrer le service DNS avant de migrer le domaine. Dans le cas contraire, le serveur d'inscription arrête de fournir le service DNS lorsque vous transférez vos domaines et les sites Web et applications Web associés deviennent indisponibles sur Internet. (Vous pouvez également migrer le service DNS à partir du bureau d'enregistrement actuel vers un autre fournisseur de services DNS.

Vous n'êtes pas obligé d'utiliser Route 53 comme fournisseur de services DNS pour les domaines enregistrés avec Route 53.)

Le processus varie selon que vous utilisez actuellement le domaine :

- Si le domaine reçoit actuellement du trafic (par exemple, si vos utilisateurs utilisent le nom de domaine pour naviguer sur un site web ou accéder à une application web), consultez Configuration de Route 53 en tant que service DNS pour un domaine en cours d'utilisation.
- Si le domaine ne reçoit aucun trafic (ou un trafic très limité), consultez Configuration de Route 53 en tant que service DNS d'un domaine inactif.

Dans les deux cas, votre domaine doit rester disponible pendant toute la durée du processus de migration. Cependant, dans le cas peu probable où il y aurait des problèmes, la première option vous permet d'annuler rapidement la migration. Avec la deuxième option, votre domaine peut rester indisponible pendant quelques jours.

Si vous souhaitez entrer en contact avec un expert AWS, rendez-vous sur le site d'assistance aux ventes.

Configuration de Route 53 en tant que service DNS pour un domaine en cours d'utilisation

Si vous souhaitez migrer le service DNS vers Amazon Route 53 pour un domaine qui reçoit actuellement du trafic (par exemple, si vos utilisateurs utilisent le nom de domaine pour naviguer sur un site web ou accéder à une application web), suivez les procédures décrites dans cette section.

Rubriques

- Étape 1 : Récupérer votre configuration DNS actuelle à partir du fournisseur de services DNS actuel (facultatif, mais recommandé)
- Étape 2 : Créer une zone hébergée
- Étape 3 : Créer des enregistrements
- Étape 4 : Diminuer les paramètres de durée de vie (TTL)
- Étape 5 : (si vous avez configuré DNSSEC) supprimer le registre DS de la zone parent
- Étape 6 : attendre l'expiration de l'ancienne TTL
- Étape 7 : mettre à jour les registres NS pour utiliser les serveurs de noms Route 53
- Étape 8 : Surveiller le trafic pour le domaine

- Étape 9 : Modifier la durée de vie de l'enregistrement NS pour la rétablir à une valeur supérieure
- Étape 10 : transférer un enregistrement de domaine vers Amazon Route 53
- Étape 11 : réactiver la signature DNSSEC (si nécessaire)

Étape 1 : Récupérer votre configuration DNS actuelle à partir du fournisseur de services DNS actuel (facultatif, mais recommandé)

Lorsque vous migrez le service DNS d'un autre fournisseur vers Route 53, reproduisez votre configuration DNS actuelle dans Route 53. Dans Route 53, créez une zone hébergée qui porte le même nom que votre domaine et créez des registres dans la zone hébergée. Chaque enregistrement indique la façon dont vous allez acheminer le trafic pour un nom de domaine ou de sous-domaine spécifié. Par exemple, lorsque quelqu'un saisit votre nom de domaine dans un navigateur Web, souhaitez-vous que le trafic soit acheminé vers un serveur Web de votre centre de données, vers une EC2 instance Amazon, vers une CloudFront distribution ou vers un autre emplacement ?

La procédure à suivre dépend de la complexité de votre configuration DNS actuelle :

- Si votre configuration DNS actuelle est simple – Si vous acheminez du trafic Internet pour seulement quelques sous-domaines vers un nombre restreint de ressources, comme des serveurs web ou des compartiments Amazon S3, vous pouvez créer manuellement quelques registres dans la console Route 53.
- Si votre configuration DNS actuelle est plus complexe, et si vous souhaitez simplement reproduire votre configuration actuelle – Vous pouvez simplifier la migration en récupérant un fichier de zone auprès de votre fournisseur de services DNS actuel, puis importer le fichier de zone dans Route 53. (Tous les fournisseurs de services DNS ne proposent pas de fichiers de zone.) Lorsque vous importez un fichier de zone, Route 53 reproduit automatiquement la configuration existante en créant les registres correspondants dans votre zone hébergée.

  Demandez au service client de votre fournisseur de services DNS actuel comment obtenir un fichier de zone ou une liste d'enregistrements. Pour plus d'informations sur le format requis du fichier de zone, consultez Création d'enregistrements par importation d'un fichier de zone.
- Si votre configuration DNS actuelle est plus complexe, et si les fonctions de routage Route 53 vous intéressent – Consultez la documentation ci-dessous pour déterminer si vous allez utiliser des fonctions Route 53 qui ne sont pas disponibles auprès d'autres fournisseurs de services DNS. Si tel est le cas, vous pouvez créer des enregistrements manuellement ou importer un fichier de zone, puis créer ou mettre à jour des enregistrements ultérieurement :

- Choix entre des enregistrements avec ou sans aliasexplique les avantages des enregistrements d'alias Route 53, qui acheminent gratuitement le trafic vers certaines AWS ressources, telles que les CloudFront distributions et les compartiments Amazon S3.
- Sélection d'une stratégie de routage décrit les options de routage Route 53, par exemple, le routage en fonction de l'emplacement de vos utilisateurs, le routage en fonction de la latence entre vos utilisateurs et vos ressources, le routage en fonction de l'état de vos ressources et le routage vers des ressources en fonction des pondérations que vous spécifiez.

> **Note**
>
> Vous pouvez également importer un fichier de zone et modifier ultérieurement votre configuration afin de tirer parti des enregistrements d'alias et des politiques de routage complexes.

Si vous ne parvenez pas à obtenir un fichier de zone ou si vous souhaitez créer manuellement des registres dans Route 53, les registres que vous êtes susceptible de migrer sont les suivants :

- Enregistrements A (Adresse) : associez un nom de domaine ou un nom de sous-domaine à l' IPv4 adresse (par exemple, 192.0.2.3) de la ressource correspondante
- Enregistrements AAAA (adresse) : associez un nom de domaine ou un nom de sous-domaine à l' IPv6 adresse (par exemple, 2001:0 db 8:85 a 3:0000:0000:abcd : 0001:2345) de la ressource correspondante
- Registres de serveur de mail (MX) – Acheminez le trafic vers des serveurs de mail
- Registres CNAME – Réacheminez le trafic d'un nom de domaine (example.net) vers un autre nom de domaine (example.com)
- Registres pour d'autres types de registres DNS pris en charge – Pour obtenir la liste des types de registres pris en charge, consultez Types d'enregistrements DNS pris en charge.

Étape 2 : Créer une zone hébergée

Pour indiquer à Amazon Route 53 la façon dont vous souhaitez acheminer le trafic pour votre domaine, créez une zone hébergée qui porte le même nom que votre domaine, puis créez des registres dans la zone hébergée.

> **Important**
>
> Vous pouvez créer une zone hébergée uniquement pour un domaine pour lequel vous disposez d'une autorisation d'administration. Généralement, cela signifie que le domaine vous appartient, mais il est également possible que vous développiez une application pour l'inscrit du domaine.

Lorsque vous créez une zone hébergée, Route 53 crée automatiquement un registre de serveur de noms (NS) et un registre de source de noms (SOA) pour la zone. Le registre NS identifie les quatre serveurs de noms que Route 53 a associés à votre zone hébergée. Pour configurer Route 53 en tant que service DNS de votre domaine, mettez à jour l'enregistrement du domaine afin qu'il utilise ces quatre serveurs de noms.

> **Important**
>
> Ne créez pas d'autre enregistrement NS (name server) ou SOA (start of authority) et ne supprimez pas les enregistrements NS et SOA existants.

Pour créer une zone hébergée

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Si vous découvrez Route 53, choisissez Get started (Mise en route) sous DNS management (Gestion DNS), puis Create hosted zones (Créer des zones hébergées).

   Si vous utilisez déjà Route 53, choisissez Hosted zones (Zones hébergées) dans le panneau de navigation, puis Create hosted zones (Créer des zones hébergées).
3. Dans le volet Create hosted zone (Créer une zone hébergée), saisissez un nom de domaine et, éventuellement, un commentaire. Pour plus d'informations sur un paramètre, ouvrez le panneau d'aide à droite.

   Pour plus d'informations sur la spécification d'autres caractères que a-z, 0-9 et - (trait d'union), et de noms de domaine internationaux, consultez Format de nom de domaine DNS.
4. Pour Type, acceptez la valeur par défaut de Public hosted zone (Zone hébergée publique).
5. Choisissez Create hosted zone (Créer une zone hébergée).

Étape 3 : Créer des enregistrements

Après avoir créé une zone hébergée, vous devez créer dans cette zone hébergée des enregistrements qui définissent l'emplacement où vous souhaitez acheminer le trafic pour un domaine (exemple.com) ou un sous-domaine (www.exemple.com). Par exemple, si vous souhaitez acheminer le trafic pour exemple.com et www.exemple.com vers un serveur Web sur une EC2 instance Amazon, vous devez créer deux enregistrements, l'un nommé exemple.com et l'autre nommé www.exemple.com. Dans chaque enregistrement, vous spécifiez l'adresse IP de votre EC2 instance.

Vous pouvez créer des enregistrements de diverses manières :

Importer un fichier de zone

Il s'agit de la méthode la plus simple si vous avez obtenu un fichier de zone de votre service DNS actuel dans Étape 1 : Récupérer votre configuration DNS actuelle à partir du fournisseur de services DNS actuel (facultatif, mais recommandé). Amazon Route 53 ne peut pas prédire à quel moment il doit créer des registres d'alias ou utiliser des types de routage particuliers (pondérés ou de basculement, par exemple). Par conséquent, si vous importez un fichier de zone, Route 53 crée des registres DNS standard en utilisant la politique de routage simple.

Pour de plus amples informations, veuillez consulter Création d'enregistrements par importation d'un fichier de zone.

Créer individuellement des enregistrements dans la console

Si vous n'avez pas obtenu de fichier de zone et si vous voulez simplement créer quelques registres avec une politique de routage simple pour commencer, vous pouvez créer les registres dans la console Route 53. Vous pouvez créer à la fois des enregistrements d'alias et des enregistrements sans alias.

Pour plus d’informations, consultez les rubriques suivantes :

- Sélection d'une stratégie de routage
- Choix entre des enregistrements avec ou sans alias
- Création d'enregistrements à l'aide de la console Amazon Route 53

Créer des enregistrements par programmation

Vous pouvez créer des enregistrements à l'aide AWS SDKs de AWS CLI l'un des AWS Tools for Windows PowerShell Pour plus d'informations, consultez la documentation AWS.

Si vous utilisez un langage de programmation qui AWS ne fournit pas de SDK pour, vous pouvez également utiliser l'API Route 53. Pour plus d'informations, consultez la référence d'API Amazon Route 53.

Étape 4 : Diminuer les paramètres de durée de vie (TTL)

Le paramètre de durée de vie d'un enregistrement spécifie la durée pendant laquelle vous voulez que les résolveurs DNS mettent en cache l'enregistrement et utilisent les informations mises en cache. À la date d'expiration, un résolveur envoie une autre requête au fournisseur de services DNS d'un domaine afin d'obtenir les informations les plus récentes.

Le paramètre de durée de vie d'un enregistrement NS est de 172 800 secondes, soit deux jours. L'enregistrement NS répertorie les serveurs de noms que le système de noms de domaine (DNS) peut utiliser pour obtenir des informations sur la manière d'acheminer le trafic pour votre domaine. Le fait de réduire la TTL du registre NS, à la fois auprès de votre fournisseur de services DNS actuel et auprès d'Amazon Route 53, permet de réduire les temps d'arrêt de votre domaine si vous rencontrez un problème pendant la migration du DNS vers Route 53. Si vous ne réduisez pas la durée de vie, votre domaine risque d'être indisponible sur Internet pendant deux jours en cas de problème.

> **Note**
>
> Certains résolveurs complets peuvent mettre en cache le TTL de l'enregistrement NS du serveur d'autorité parent. Par conséquent, le TTL des enregistrements NS enregistrés sur le serveur DNS officiel parent doit également être réduit.

Nous vous recommandons de modifier la durée de vie sur les enregistrements NS suivants :

- Sur l'enregistrement NS dans la zone hébergée du fournisseur de services DNS actuel. (Votre fournisseur actuel peut utiliser une terminologie différente.)
- Sur l'enregistrement NS dans la zone hébergée que vous avez créée dans Étape 2 : Créer une zone hébergée.

Pour réduire le paramètre de durée de vie sur l'enregistrement NS avec le fournisseur de services DNS actuel

- Utilisez la méthode indiquée par votre fournisseur de services DNS actuel du domaine afin de modifier la durée de vie de l'enregistrement NS dans la zone hébergée de votre domaine.

Pour réduire le paramètre TTL du registre NS dans une zone hébergée Route 53

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation, sélectionnez Hosted Zones (Zones hébergées).
3. Choisissez le nom de la zone hébergée.
4. Choisissez le registre NS, puis Edit (Modifier).
5. Modifiez la valeur du champ TTL (Seconds) (Durée de vie (secondes)). Nous vous recommandons de spécifier une valeur comprise entre 60 secondes et 900 secondes (15 minutes).
6. Sélectionnez Enregistrer les modifications.

Étape 5 : (si vous avez configuré DNSSEC) supprimer le registre DS de la zone parent

Si vous avez configuré DNSSEC pour votre domaine, supprimez le registre Delegation Signer (DS) de la zone parent avant de migrer votre domaine vers Route 53.

Si la zone parent est hébergée via Route 53 ou un autre bureau d'enregistrement, contactez-les pour supprimer l'enregistrement DS.

Comme il n'est actuellement pas possible d'activer la signature DNSSEC sur deux fournisseurs, vous devez supprimer tout DS ou DNSKEYs désactiver le DNSSEC. Cela indique temporairement aux résolveurs DNS de désactiver la validation DNSSEC. Lors de l'étape 11, vous pouvez réactiver la validation DNSSEC si vous le souhaitez, une fois la transition vers Route 53 terminée.

Pour de plus amples informations, veuillez consulter Suppression de clés publiques pour un domaine.

Étape 6 : attendre l'expiration de l'ancienne TTL

Si votre domaine est en cours d'utilisation (par exemple, si vos utilisateurs utilisent le nom de domaine pour naviguer sur un site web ou accéder à une application web), cela signifie que les résolveurs DNS ont mis en cache les noms des serveurs de noms qui ont été fournis par votre fournisseur de services DNS actuel. Un résolveur DNS qui a mis en cache ces informations il y a quelques minutes les conservera pendant près de deux jours.

Pour vous assurer que la migration du service DNS vers Route 53 s'exécute en une seule fois, attendez deux jours après avoir réduit la TTL. Une fois ce délai de deux jours passé et une fois que les résolveurs ont demandé les serveurs de noms pour votre domaine, les résolveurs obtiendront les

serveurs de noms actuels ainsi que la nouvelle durée de vie que vous avez spécifiée dans Étape 4 : Diminuer les paramètres de durée de vie (TTL).

Étape 7 : mettre à jour les registres NS pour utiliser les serveurs de noms Route 53

Pour commencer à utiliser Amazon Route 53 en tant que service DNS pour un domaine, utilisez la méthode fournie par le bureau d'enregistrement, ou la zone parent, pour remplacer les serveurs de noms actuels dans le registre NS par des serveurs de noms Route 53.

> **Note**
>
> Lorsque vous mettez à jour le registre NS avec le fournisseur de services DNS actuel pour utiliser des serveurs de noms Route 53, vous mettez à jour la configuration DNS pour le domaine. (Cela revient à mettre à jour le registre NS de la zone hébergée Route 53 pour un domaine, sauf que vous mettez à jour le paramètre avec le service DNS depuis lequel vous effectuez la migration.)

Pour mettre à jour le registre NS au niveau du bureau d'enregistrement, ou de la zone parent, afin d'utiliser les serveurs de noms Route 53

1. Dans la console Route 53, récupérez les serveurs de noms pour votre zone hébergée :
   a. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
   b. Dans le panneau de navigation, choisissez Zones hébergées.
   c. Sur la page Hosted zones (Zones hébergées), choisissez le nom de la zone hébergée concernée.
   d. Prenez note des quatre noms répertoriés dans Name servers (Serveurs de noms) dans la section Hosted zone details (Détails de la zone hébergée).
2. Utilisez la méthode indiquée par le service DNS actuel du domaine pour mettre à jour l'enregistrement NS pour la zone hébergée. Si le domaine est enregistré auprès de Route 53, consultez Ajout ou modification de serveurs de noms et d'enregistrements de type glue pour un domaine. Le processus varie selon que le service DNS actuel vous permet ou non de supprimer des serveurs de noms :

   Si vous pouvez supprimer des serveurs de noms

- Notez les noms des serveurs de noms actuels dans l'enregistrement NS pour la zone hébergée. Si vous avez besoin de rétablir la configuration DNS actuelle, il s'agit des serveurs que vous allez spécifier.
- Supprimez les serveurs de noms actuels de l'enregistrement NS.
- Mettez à jour le registre NS avec les noms des quatre serveurs de noms Route 53 que vous avez obtenus lors de l'étape 1 de cette procédure.

> **Note**
>
> Lorsque vous avez terminé, les seuls serveurs de noms du registre NS seront les quatre serveurs de noms Route 53.

Si vous ne pouvez pas supprimer les serveurs de noms

- Choisissez l'option permettant d'utiliser des serveurs de noms personnalisés.
- Ajoutez les quatre serveurs de noms Route 53 que vous avez obtenus lors de l'étape 1 de cette procédure.

Étape 8 : Surveiller le trafic pour le domaine

Surveillez le trafic pour le domaine, y compris le trafic du site Web ou de l'application et la messagerie :

- Si le trafic ralentit ou s'interrompt – Utilisez la méthode indiquée par le précédent service DNS pour rétablir les serveurs de noms précédents du domaine. Il s'agit des serveurs de noms que vous avez notés à l'étape 7 de Pour mettre à jour le registre NS au niveau du bureau d'enregistrement, ou de la zone parent, afin d'utiliser les serveurs de noms Route 53. Déterminez ce qui s'est mal passé.
- Si le trafic n'est pas affecté – Passez à Étape 9 : Modifier la durée de vie de l'enregistrement NS pour la rétablir à une valeur supérieure.

Étape 9 : Modifier la durée de vie de l'enregistrement NS pour la rétablir à une valeur supérieure

Dans la zone hébergée Amazon Route 53 du domaine, modifiez la TTL du registre NS en utilisant une valeur plus classique, par exemple 172 800 secondes (deux jours). Cette étape permet d'améliorer la latence pour vos utilisateurs car ils n'auront plus besoin d'attendre aussi souvent que les résolveurs DNS envoient une requête pour les serveurs de noms de votre domaine.

Pour modifier la TTL du registre NS dans la zone hébergée Route 53

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation, sélectionnez Hosted Zones (Zones hébergées).
3. Choisissez le nom de la zone hébergée.
4. Dans la liste des enregistrements de la zone hébergée, sélectionnez l'enregistrement NS.
5. Choisissez Edit (Modifier).
6. Modifiez la valeur du champ TTL (Seconds) (Durée de vie (secondes)) en indiquant le nombre de secondes pendant lequel vous voulez que les résolveurs DNS mettent en cache les noms des serveurs de noms de votre domaine. Nous vous recommandons une valeur de 172 800 secondes.
7. Sélectionnez Enregistrer les modifications.

Étape 10 : transférer un enregistrement de domaine vers Amazon Route 53

Maintenant que vous avez transféré le service DNS d'un domaine vers Amazon Route 53, vous pouvez éventuellement transférer l'enregistrement du domaine vers Route 53. Pour de plus amples informations, veuillez consulter Transfert d'un enregistrement de domaine vers Amazon Route 53.

Étape 11 : réactiver la signature DNSSEC (si nécessaire)

Maintenant que vous avez transféré le service DNS d'un domaine vers Amazon Route 53, vous pouvez réactiver la signature DNSSEC.

La signature DNSSEC s'active en deux étapes :

- Étape 1 : Activez la signature DNSSEC pour Route 53 et demandez à Route 53 de créer une clé de signature (KSK) basée sur une clé gérée par le client dans AWS Key Management Service ().AWS KMS

- Étape 2 : créez une chaîne d'approbation pour la zone hébergée en ajoutant un registre Delegation Signer (DS) à la zone parent, afin que les réponses DNS puissent être authentifiées avec des signatures de chiffrement fiables.

  Pour obtenir des instructions, consultez Activation de la signature DNSSEC et établissement d'une chaîne d'approbation.

Configuration de Route 53 en tant que service DNS d'un domaine inactif

Si vous souhaitez migrer le service DNS vers Amazon Route 53 pour un domaine qui ne reçoit aucun trafic (ou très peu de trafic), suivez les procédures décrites dans cette section.

Rubriques

- Étape 1 : Récupérer votre configuration DNS actuelle à partir du fournisseur de services DNS actuel (domaines inactifs)
- Étape 2 : Créer une zone hébergée (domaines inactifs)
- Étape 3 : Créer des enregistrements (domaines inactifs)
- Étape 4 : mettre à jour l'enregistrement de domaine pour utiliser les serveurs de noms Amazon Route 53 (domaines inactifs)

Étape 1 : Récupérer votre configuration DNS actuelle à partir du fournisseur de services DNS actuel (domaines inactifs)

Lorsque vous migrez le service DNS d'un autre fournisseur vers Route 53, reproduisez votre configuration DNS actuelle dans Route 53. Dans Route 53, créez une zone hébergée qui porte le même nom que votre domaine et créez des registres dans la zone hébergée. Chaque enregistrement indique la façon dont vous allez acheminer le trafic pour un nom de domaine ou de sous-domaine spécifié. Par exemple, lorsque quelqu'un saisit votre nom de domaine dans un navigateur Web, souhaitez-vous que le trafic soit acheminé vers un serveur Web de votre centre de données, vers une EC2 instance Amazon, vers une CloudFront distribution ou vers un autre emplacement ?

La procédure à suivre dépend de la complexité de votre configuration DNS actuelle :

- Si votre configuration DNS actuelle est simple – Si vous acheminez du trafic Internet pour seulement quelques sous-domaines vers un nombre restreint de ressources, comme des serveurs web ou des compartiments Amazon S3, vous pouvez créer manuellement quelques registres dans la console Route 53.

- Si votre configuration DNS actuelle est plus complexe, et si vous souhaitez simplement reproduire votre configuration actuelle – Vous pouvez simplifier la migration en récupérant un fichier de zone auprès de votre fournisseur de services DNS actuel, puis importer le fichier de zone dans Route 53. (Tous les fournisseurs de services DNS ne proposent pas de fichiers de zone.) Lorsque vous importez un fichier de zone, Route 53 reproduit automatiquement la configuration existante en créant les registres correspondants dans votre zone hébergée.

  Demandez au service client de votre fournisseur de services DNS actuel comment obtenir un fichier de zone ou une liste d'enregistrements. Pour plus d'informations sur le format requis du fichier de zone, consultez Création d'enregistrements par importation d'un fichier de zone.
- Si votre configuration DNS actuelle est plus complexe, et si les fonctions de routage Route 53 vous intéressent – Consultez la documentation ci-dessous pour déterminer si vous allez utiliser des fonctions Route 53 qui ne sont pas disponibles auprès d'autres fournisseurs de services DNS. Si tel est le cas, vous pouvez créer des enregistrements manuellement ou importer un fichier de zone, puis créer ou mettre à jour des enregistrements ultérieurement :
  - Choix entre des enregistrements avec ou sans aliasexplique les avantages des enregistrements d'alias Route 53, qui acheminent gratuitement le trafic vers certaines AWS ressources, telles que les CloudFront distributions et les compartiments Amazon S3.
  - Sélection d'une stratégie de routage décrit les options de routage Route 53, par exemple, le routage en fonction de l'emplacement de vos utilisateurs, le routage en fonction de la latence entre vos utilisateurs et vos ressources, le routage en fonction de l'état de vos ressources et le routage vers des ressources en fonction des pondérations que vous spécifiez.

> **Note**
>
> Vous pouvez également importer un fichier de zone et modifier ultérieurement votre configuration afin de tirer parti des enregistrements d'alias et des politiques de routage complexes.

Si vous ne parvenez pas à obtenir un fichier de zone ou si vous souhaitez créer manuellement des registres dans Route 53, les registres que vous êtes susceptible de migrer sont les suivants :

- Enregistrements A (Adresse) : associez un nom de domaine ou un nom de sous-domaine à l' IPv4 adresse (par exemple, 192.0.2.3) de la ressource correspondante

- Enregistrements AAAA (adresse) : associez un nom de domaine ou un nom de sous-domaine à l' IPv6 adresse (par exemple, 2001:0 db 8:85 a 3:0000:0000:abcd : 0001:2345) de la ressource correspondante
- Registres de serveur de mail (MX) – Acheminez le trafic vers des serveurs de mail
- Registres CNAME – Réacheminez le trafic d'un nom de domaine (example.net) vers un autre nom de domaine (example.com)
- Registres pour d'autres types de registres DNS pris en charge – Pour obtenir la liste des types de registres pris en charge, consultez Types d'enregistrements DNS pris en charge.

Étape 2 : Créer une zone hébergée (domaines inactifs)

Pour indiquer à Amazon Route 53 la façon dont vous souhaitez acheminer le trafic pour votre domaine, créez une zone hébergée qui porte le même nom que votre domaine, puis créez des registres dans la zone hébergée.

> **Important**
>
> Vous pouvez créer une zone hébergée uniquement pour un domaine pour lequel vous disposez d'une autorisation d'administration. Généralement, cela signifie que le domaine vous appartient, mais il est également possible que vous développiez une application pour l'inscrit du domaine.

Lorsque vous créez une zone hébergée, Route 53 crée automatiquement un registre de serveur de noms (NS) et un registre de source de noms (SOA) pour la zone. Le registre NS identifie les quatre serveurs de noms que Route 53 a associés à votre zone hébergée. Pour configurer Route 53 en tant que service DNS de votre domaine, mettez à jour l'enregistrement du domaine afin qu'il utilise ces quatre serveurs de noms.

> **Important**
>
> Ne créez pas d'autre enregistrement NS (name server) ou SOA (start of authority) et ne supprimez pas les enregistrements NS et SOA existants.

Pour créer une zone hébergée

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Si vous débutez avec Route 53, choisissez Get started (Mise en route).

   Si vous utilisez déjà Route 53, choisissez Hosted Zones (Zones hébergées) dans le panneau de navigation.
3. Choisissez Create hosted zone (Créer une zone hébergée).
4. Dans le volet Create hosted zone (Créer une zone hébergée), saisissez un nom de domaine et, éventuellement, un commentaire. Pour plus d'informations sur un paramètre, arrêtez le pointeur de la souris sur son étiquette pour afficher une info-bulle.

   Pour plus d'informations sur la spécification d'autres caractères que a-z, 0-9 et - (trait d'union), et de noms de domaine internationaux, consultez Format de nom de domaine DNS.
5. Pour Record type (Type de registre), acceptez la valeur par défaut de Public hosted zone (Zone hébergée publique).
6. Choisissez Create hosted zone (Créer une zone hébergée).

Étape 3 : Créer des enregistrements (domaines inactifs)

Après avoir créé une zone hébergée, vous devez créer dans cette zone des enregistrements qui définissent l'emplacement où vous souhaitez acheminer le trafic pour un domaine (exemple.com) ou un sous-domaine (www.exemple.com). Par exemple, si vous souhaitez acheminer le trafic pour exemple.com et www.exemple.com vers un serveur Web sur une EC2 instance Amazon, vous devez créer deux enregistrements, l'un nommé exemple.com et l'autre nommé www.exemple.com. Dans chaque enregistrement, vous spécifiez l'adresse IP de votre EC2 instance.

Vous pouvez créer des enregistrements de diverses manières :

Importer un fichier de zone

Il s'agit de la méthode la plus simple si vous avez obtenu un fichier de zone de votre service DNS actuel dans Étape 1 : Récupérer votre configuration DNS actuelle à partir du fournisseur de services DNS actuel (domaines inactifs). Amazon Route 53 ne peut pas prédire à quel moment il doit créer des registres d'alias ou utiliser des types de routage particuliers (pondérés ou de basculement, par exemple). Par conséquent, si vous importez un fichier de zone, Route 53 crée des registres DNS standard en utilisant la politique de routage simple.

Pour de plus amples informations, veuillez consulter Création d'enregistrements par importation d'un fichier de zone.

Créer individuellement des enregistrements dans la console

Si vous n'avez pas obtenu de fichier de zone et si vous voulez simplement créer quelques registres avec une politique de routage simple pour commencer, vous pouvez créer les registres dans la console Route 53. Vous pouvez créer à la fois des enregistrements d'alias et des enregistrements sans alias.

Pour plus d'informations, consultez les rubriques suivantes :

- Sélection d'une stratégie de routage
- Choix entre des enregistrements avec ou sans alias
- Création d'enregistrements à l'aide de la console Amazon Route 53

Créer des enregistrements par programmation

Vous pouvez créer des enregistrements à l'aide AWS SDKs de AWS CLI l'un des AWS Tools for Windows PowerShell Pour plus d'informations, consultez la documentation AWS.

Si vous utilisez un langage de programmation qui AWS ne fournit pas de SDK pour, vous pouvez également utiliser l'API Route 53. Pour plus d'informations, consultez la référence d'API Amazon Route 53.

Étape 4 : mettre à jour l'enregistrement de domaine pour utiliser les serveurs de noms Amazon Route 53 (domaines inactifs)

Lorsque vous avez terminé de créer des registres pour le domaine, vous pouvez modifier le service DNS de votre domaine pour le configurer sur Amazon Route 53. Exécutez la procédure suivante pour mettre à jour les paramètres auprès du serveur d'inscriptions de domaine.

Pour mettre à jour les serveurs de noms du domaine

1. Dans la console Route 53, récupérez les serveurs de noms pour votre zone hébergée Route 53 :
   a. Ouvrez la console Route 53 à l'adresse https://console.aws.amazon.com/route53/.
   b. Dans le panneau de navigation, choisissez Zones hébergées.
   c. Sur la page Hosted zones (Zones hébergées), choisissez la case d'option (pas le nom) de la zone hébergée, puis View details (Afficher les détails).

   d. Sur la page des détails de la zone hébergée, choisissez Hosted zone details (Détails de la zone hébergée).
   e. Notez les quatre serveurs répertoriés dans Name servers (Serveurs de noms).
2. Utilisez la méthode indiquée par le bureau d'enregistrement du domaine pour remplacer les serveurs de noms du domaine afin d'utiliser les quatre serveurs de noms Route 53 obtenus lors de l'étape 2 de cette procédure.

   Si le domaine est enregistré auprès de Route 53, consultez Ajout ou modification de serveurs de noms et d'enregistrements de type glue pour un domaine.

Configuration du routage DNS pour un nouveau domaine

Un nouveau domaine que vous avez acheté auprès de Route 53

Lorsque vous enregistrez un domaine avec Route 53, ce dernier est automatiquement configuré en tant que service DNS pour le domaine. Route 53 crée une zone hébergée portant le même nom que le domaine, affecte quatre serveurs de noms à la zone hébergée, et met à jour le domaine pour utiliser les serveurs de noms.

Un nouveau domaine que vous avez acheté auprès d'un autre bureau d'enregistrement

Lorsque vous achetez un domaine auprès d'un autre bureau d'enregistrement, par exemple, parce que le domaine de premier niveau (TLD) n'est pas proposé par Route 53, vous pouvez toujours gérer le routage DNS à l'aide de Route 53. Pour de plus amples informations, veuillez consulter Domaines que vous pouvez enregistrer avec Amazon Route 53.

Suivez ces instructions pour créer une zone hébergée publique, puis utilisez les serveurs de noms créés avec le bureau d'enregistrement :

Pour créer une zone hébergée pour un domaine autre que Route 53

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le panneau de navigation, choisissez Zones hébergées, puis choisissez Créer une zone hébergée.
3. Pour le nom, entrez le nom du domaine pour lequel vous souhaitez créer une zone hébergée, par exemple`example.com`, une description facultative, choisissez Zone hébergée publique puis Créer une zone hébergée.

4. Après avoir créé la zone hébergée, notez les quatre enregistrements de serveur de noms (NS) qui ont été créés. Chacune d'entre elles commencera par « ns- ».

   Dans votre bureau d'enregistrement de domaines, entrez les serveurs de noms ci-dessus pour déléguer la gestion des domaines à votre zone hébergée Route 53.

Acheminer le trafic DNS

Pour spécifier la façon dont vous voulez que Route 53 achemine le trafic Internet pour le domaine, créez des registres dans la zone hébergée. Par exemple, si vous souhaitez acheminer des demandes pour exemple.com vers un serveur Web exécuté sur une EC2 instance Amazon, vous créez un enregistrement dans la zone hébergée exemple.com et vous spécifiez l'adresse IP élastique de l' EC2 instance. Pour plus d'informations, consultez les rubriques suivantes :

- Pour plus d'informations sur la création de registres dans votre zone hébergée, consultez Utilisation des enregistrements.
- Pour plus d'informations sur la manière d'acheminer le trafic vers AWS des ressources sélectionnées, consultezAcheminement du trafic Internet vers vos AWS ressources.
- Pour en savoir plus sur le fonctionnement de DNS, consultez Acheminement du trafic Internet vers votre site web ou votre application web.
- Pour vérifier le repos du DNS, voirVérification des réponses DNS à partir de Route 53.

Acheminement du trafic vers vos ressources

Lorsque les utilisateurs font une demande à votre site web ou application web, par exemple, en saisissant le nom de votre domaine dans un navigateur web, Amazon Route 53 achemine les utilisateurs vers vos ressources, telles qu'un compartiment Amazon S3 ou un serveur web dans votre centre de données. Pour configurer Route 53 pour qu'il achemine le trafic vers vos ressources, procédez comme suit :

1. Créez une zone hébergée. Vous pouvez créer une zone hébergée publique ou une zone hébergée privée :

   Zone hébergée publique

   Créez une zone hébergée publique si vous souhaitez acheminer le trafic Internet vers vos ressources, par exemple, afin que vos clients puissent consulter le site Web de l'entreprise que

vous hébergez sur EC2 des instances. Pour de plus amples informations, veuillez consulter Utilisation de zones hébergées publiques.

Zone hébergée privée

Créez une zone hébergée privée si vous souhaitez acheminer le trafic au sein d'un VPC Amazon. Pour de plus amples informations, veuillez consulter Utilisation des zones hébergées privées.

2. Créez des enregistrements dans la zone hébergée. Les enregistrements définissent l'endroit où vous souhaitez acheminer le trafic pour chaque nom de domaine ou sous-domaine. Par exemple, pour acheminer le trafic de www.exemple.com vers un serveur web de votre centre de données, vous devez généralement créer un enregistrement www.exemple.com dans la zone hébergée exemple.com.

   Pour plus d'informations, consultez les rubriques suivantes :

   - Utilisation des enregistrements
   - Acheminement du trafic pour les sous-domaines
   - Acheminement du trafic Internet vers vos AWS ressources

Acheminement du trafic pour les sous-domaines

Si vous souhaitez acheminer le trafic vers vos ressources pour un sous-domaine, par exemple acme.exemple.com ou zenith.exemple.com, deux options s'offrent à vous :

Création d'enregistrements dans la zone hébergée du domaine

En règle générale, pour acheminer le trafic pour un sous-domaine, vous devez créer un enregistrement dans la zone hébergée qui porte le même nom que le domaine. Par exemple, pour acheminer le trafic Internet pour acme.exemple.com vers un serveur Web de votre centre de données, vous devez créer un enregistrement nommé acme.exemple.com dans la zone hébergée www.exemple.com. Pour de plus amples informations, veuillez consulter la rubrique Utilisation des enregistrements et ses sous-rubriques.

Création d'une zone hébergée pour le sous-domaine et création d'enregistrements dans la nouvelle zone hébergée

Vous pouvez également créer une zone hébergée pour le sous-domaine. L'utilisation d'une zone hébergée distincte pour acheminer le trafic Internet pour un sous-domaine est appelée parfois « déléguer la responsabilité d'un sous-domaine à une zone hébergée » ou « déléguer la

responsabilité d'un sous-domaine à d'autres serveurs de noms », ou une combinaison de termes similaires. Voici comment cela fonctionne :

1. Vous créez une zone hébergée portant le même nom que le sous-domaine pour lequel vous souhaitez acheminer le trafic, par exemple acme.exemple.com.
2. Vous créez des enregistrements dans la nouvelle zone hébergée qui définissent la façon dont vous souhaitez acheminer le trafic pour le sous-domaine (acme.exemple.com) et ses sous-domaines, par exemple backend.acme.exemple.com.
3. Vous obtenez les serveurs de noms affectés par Route 53 à la nouvelle zone hébergée lors de sa création.
4. Vous créez un nouvel enregistrement NS dans la zone hébergée pour le domaine (exemple.com), et vous spécifiez les quatre serveurs de noms que vous avez obtenus à l'étape 3.

Lorsque vous utilisez une zone hébergée distincte dans le but d'acheminer le trafic pour un sous-domaine, vous pouvez utiliser des autorisations IAM pour limiter l'accès à la zone hébergée du sous-domaine. Si vous disposez de plusieurs sous-domaines et qu'ils sont gérés par différents groupes, le fait de créer une zone hébergée pour chaque sous-domaine peut réduire considérablement le nombre de personnes devant avoir accès aux enregistrements dans la zone hébergée du domaine.

L'utilisation d'une zone hébergée distincte pour un sous-domaine vous permet également d'utiliser des services DNS différents pour le domaine et le sous-domaine. Pour de plus amples informations, veuillez consulter Utilisation d'Amazon Route 53 comme service DNS pour des sous-domaines sans migration du domaine parent.

Cette configuration a un léger impact sur les performances de la première requête DNS de chaque résolveur DNS. Le résolveur doit obtenir des informations auprès de la zone hébergée du domaine racine, puis auprès de la zone hébergée du sous-domaine. À l'issue de la première requête DNS pour un sous-domaine, le résolveur met les informations en cache et n'a plus pas besoin de les obtenir tant que la durée de vie (TTL) n'a pas expiré et qu'un autre client n'a pas demandé le sous-domaine à ce résolveur. Pour plus d'informations, veuillez consulter TTL (secondes) dans la section Valeurs à spécifier lorsque vous créez ou modifiez des enregistrements Amazon Route 53.

Rubriques

- Création d'une autre zone hébergée pour acheminer le trafic pour un sous-domaine

- Acheminement du trafic pour d'autres niveaux de sous-domaines

Création d'une autre zone hébergée pour acheminer le trafic pour un sous-domaine

Un moyen d'acheminer le trafic pour un sous-domaine est de créer une zone hébergée pour celui-ci et de créer dans la zone hébergée des enregistrements pour le sous-domaine. (La solution la plus courante consiste à créer des enregistrements pour le sous-domaine dans la zone hébergée du domaine.)

> **Note**
>
> Bien que nous décrivions ici le processus de création et de délégation à une zone hébergée de sous-domaine sur Route 53, vous pouvez également créer une zone DNS sur d'autres serveurs de noms et créer, de la même manière, des registres de serveur de noms (NS) qui délèguent la responsabilité à ces serveurs de noms.

Voici la procédure générale :

1. Créez une zone hébergée pour le sous-domaine. Pour de plus amples informations, veuillez consulter Création d'une zone hébergée pour un sous-domaine.
2. Ajoutez des enregistrements à la zone hébergée du sous-domaine. Si la zone hébergée du domaine contient des enregistrements qui appartiennent à la zone hébergée du sous-domaine, dupliquez ces enregistrements dans la zone hébergée pour le sous-domaine. Pour de plus amples informations, veuillez consulter Création d'enregistrements dans la zone hébergée du sous-domaine.
3. Créez un enregistrement NS pour le sous-domaine dans la zone hébergée du domaine, ce qui délègue la responsabilité du sous-domaine aux serveurs de noms de la nouvelle zone hébergée. Si la zone hébergée du domaine contient des enregistrements qui appartiennent à la zone hébergée du sous-domaine, supprimez ces enregistrements de la zone hébergée du domaine. (Vous avez créé des copies dans la zone hébergée du sous-domaine à l'étape 2.) Pour de plus amples informations, veuillez consulter Mise à jour de la zone hébergée du domaine.

Création d'une zone hébergée pour un sous-domaine

Pour créer une zone hébergée pour un sous-domaine à l'aide de la console Route 53, exécutez la procédure suivante.

Pour créer une zone hébergée pour un sous-domaine (console)

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Si vous débutez avec Route 53, choisissez Get started (Mise en route).

   Si vous utilisez déjà Route 53, choisissez Hosted Zones (Zones hébergées) dans le panneau de navigation.
3. Choisissez Create hosted zone (Créer une zone hébergée).
4. Dans le volet droit, entrez le nom du sous-domaine, par exemple acme.example.com. Vous pouvez également entrer un commentaire facultatif.

   Pour plus d'informations sur la spécification d'autres caractères que a-z, 0-9 et - (trait d'union), et de noms de domaine internationaux, consultez Format de nom de domaine DNS.
5. Pour Type, acceptez la valeur par défaut de Public hosted zone (Zone hébergée publique).
6. En bas du volet droit, choisissez Create hosted zone (Créer une zone hébergée).

Création d'enregistrements dans la zone hébergée du sous-domaine

Pour définir la façon dont Route 53 doit acheminer le trafic pour le sous-domaine (acme.example.com) et ses sous-domaines (backend.acme.example.com), créez des registres dans la zone hébergée du sous-domaine.

Notez les points suivants à propos de la création d'enregistrements dans la zone hébergée du sous-domaine :

- Ne créez pas d'enregistrements de serveur de noms (NS) ou de source de noms (SOA) supplémentaires dans la zone hébergée du sous-domaine et ne supprimez pas les enregistrements NS et SOA existants.
- Créez tous les enregistrements pour le sous-domaine dans la zone hébergée du sous-domaine. Par exemple, si vous disposez de zones hébergées pour example.com et pour le domaine acme.example.com, créez tous les enregistrements pour le sous-domaine acme.example.com dans la zone hébergée acme.example.com. Cela inclut les enregistrements tels que backend.acme.example.com et beta.backend.acme.example.com.
- Si la zone hébergée du domaine (example.com) contient déjà des enregistrements qui appartiennent à la zone hébergée du sous-domaine (acme.example.com), dupliquez ces

enregistrements dans la zone hébergée du sous-domaine. Dans la dernière étape du processus, vous supprimerez les enregistrements en double de la zone hébergée du domaine ultérieurement.

> **Important**
>
> Si certains enregistrements pour le sous-domaine figurent à la fois dans la zone hébergée du domaine et la zone hébergée du sous-domaine, le comportement DNS sera incohérent. Le comportement dépendra des serveurs de noms qu'un résolveur DNS a mis en cache, des serveurs de noms pour la zone hébergée du domaine (example.com) ou des serveurs de noms pour la zone hébergée du sous-domaine (acme.example.com). Dans certains cas, Route 53 renvoie une réponse NXDOMAIN (domaine inexistant) lorsque l'enregistrement existe, mais pas dans la zone hébergée à laquelle les résolveurs DNS envoient la demande.

Pour de plus amples informations, veuillez consulter Utilisation des enregistrements.

Mise à jour de la zone hébergée du domaine

Lorsque vous créez une zone hébergée, Route 53 lui affecte automatiquement quatre serveurs de noms. L'enregistrement NS pour la zone hébergée identifie les serveurs de noms qui répondent aux requêtes DNS pour le domaine ou le sous-domaine. Pour commencer à utiliser les enregistrements de la zone hébergée du sous-domaine pour acheminer le trafic Internet, vous devez créer un enregistrement NS dans la zone hébergée du domaine (example.com) et lui attribuer le nom du sous-domaine (acme.example.com). Pour la valeur de l'enregistrement NS, vous spécifiez les noms des serveurs de noms de la zone hébergée du sous-domaine.

Voici ce qu'il se passe lorsque Route 53 reçoit une requête DNS d'un résolveur DNS pour le sous-domaine acme.example.com ou l'un de ses sous-domaines :

1. Route 53 recherche, dans la zone hébergée du domaine (example.com), le registre NS du sous-domaine (acme.example.com).
2. Route 53 obtient les serveurs de noms du registre NS acme.example.com dans la zone hébergée du domaine example.com, et renvoie ces serveurs de noms au résolveur DNS.
3. Le résolveur envoie à nouveau la requête pour acme.example.com aux serveurs de noms pour la zone hébergée acme.example.com.
4. Route 53 répond à la requête en utilisant un enregistrement contenu dans la zone hébergée acme.example.com.

Pour configurer Route 53 pour qu'il achemine le trafic pour le sous-domaine à l'aide de la zone hébergée du sous-domaine et supprime les registres en double de la zone hébergée du domaine, exécutez la procédure suivante :

Pour configurer Route 53 afin d'utiliser la zone hébergée du sous-domaine (console)

1. Dans la console Route 53, obtenez les serveurs de noms de la zone hébergée du sous-domaine :
   a. Dans le panneau de navigation, choisissez Zones hébergées.
   b. Sur la page Hosted zones (Zones hébergées), choisissez le nom de la zone hébergée du sous-domaine.
   c. Dans le volet droit, copiez les noms des quatre serveurs répertoriés dans Name servers (Serveurs de noms) dans la section Hosted zones details (Détails des zones hébergées).
2. Choisissez le nom de la zone hébergée du domaine (example.com), et non du sous-domaine.
3. Choisissez Créer un registre.
4. Choisissez Simple routing (Routage simple), puis Next (Suivant).
5. Choisissez Define simple record (Définir un registre simple).
6. Indiquez l’une des valeurs suivantes :

   Nom

   Entrez le nom du sous-domaine.

   Valeur/routage du trafic vers

   Choisissez IP address or another value depending on the record type (Adresse IP ou autre valeur selon le type de registre) et collez les noms des serveurs de noms que vous avez copiés lors de l'étape 1.

   Type de registre

   Choisissez NS – Name servers for a hosted zone (NS – Serveurs de noms pour une zone hébergée).

   TTL (secondes)

   Indiquez une valeur plus courante pour un enregistrement NS, par exemple 172 800 secondes.

7. Choisissez Define simple record (Définir un registre simple), puis Create records (Créer des registres).
8. Si la zone hébergée du domaine contient des enregistrements que vous avez recréés dans la zone hébergée du sous-domaine, supprimez ces enregistrements de la zone hébergée du domaine. Pour de plus amples informations, veuillez consulter Suppression d'enregistrements.

   Lorsque vous avez terminé, tous les enregistrements pour le sous-domaine doivent se trouver dans la zone hébergée du sous-domaine.

Acheminement du trafic pour d'autres niveaux de sous-domaines

Acheminer le trafic vers un sous-domaine d'un sous-domaine, par exemple backend.acme.example.com, revient au même que d'acheminer le trafic vers un sous-domaine, par exemple acme.example.com. Soit vous créez des enregistrements dans la zone hébergée du domaine, soit vous créez une zone hébergée pour le sous-domaine de niveau inférieur, puis créez des enregistrements dans cette nouvelle zone hébergée.

Si vous choisissez de créer une zone hébergée distincte pour le sous-domaine de niveau inférieur, créez l'enregistrement NS pour ce sous-domaine dans la zone hébergée du sous-domaine qui est plus proche d'un niveau du nom de domaine. Cela permet de garantir que le trafic est correctement acheminé vers vos ressources. Par exemple, supposons que vous voulez acheminer le trafic pour les sous-domaines suivants :

- subdomain1.example.com
- subdomain2.subdomain1.example.com

Pour utiliser une autre zone hébergée afin d'acheminer le trafic pour subdomain2.subdomain1.example.com, procédez comme suit :

1. Créez une zone hébergée nommée subdomain2.subdomain1.example.com.
2. Créez des enregistrements dans la zone hébergée subdomain2.subdomain1.example.com. Pour de plus amples informations, veuillez consulter Création d'enregistrements dans la zone hébergée du sous-domaine.
3. Copiez les noms des serveurs de noms de la zone hébergée subdomain2.subdomain1.example.com.

4. Dans la zone hébergée subdomain1.example.com, créez un enregistrement NS nommé subdomain2.subdomain1.example.com, puis collez-y les noms des serveurs de noms de la zone hébergée subdomain2.subdomain1.example.com.

   En outre, supprimez les enregistrements en double de subdomain1.exemple.com. Pour de plus amples informations, veuillez consulter Mise à jour de la zone hébergée du domaine.

   Une fois que vous avez créé ce registre NS, Route 53 commence à utiliser la zone hébergée subdomain2.subdomain1.example.com pour acheminer le trafic pour le sous-domaine subdomain2.subdomain1.example.com.

Utilisation de zones hébergées

Une zone hébergée est un conteneur d'enregistrements, lesquels comportent des informations sur la façon dont vous souhaitez acheminer le trafic d'un domaine spécifique (par exemple, example.com) et de ses sous-domaines (acme.example.com, zenith.example.com). Une zone hébergée a le même nom que le domaine correspondant. Il existe deux types de zones hébergées :

- Les zones hébergées publiques contiennent les enregistrements qui spécifient la façon dont vous souhaitez acheminer le trafic sur le réseau Internet. Pour de plus amples informations, veuillez consulter Utilisation de zones hébergées publiques.
- Les zones hébergées privées contiennent les enregistrements qui spécifient la façon dont vous souhaitez acheminer le trafic dans un VPC Amazon. Pour de plus amples informations, veuillez consulter Utilisation des zones hébergées privées.

Utilisation de zones hébergées publiques

Une zone hébergée publique est un conteneur qui comporte des informations sur la façon dont vous souhaitez acheminer le trafic sur le réseau Internet pour un domaine spécifique (par exemple, example.com) et ses sous-domaines (acme.example.com, zenith.example.com). Vous obtenez une zone hébergée publique de la manière suivante :

- Lorsque vous enregistrez un domaine avec Route 53, nous créons automatiquement une zone hébergée pour vous.
- Lorsque vous transférez le service DNS pour un domaine existant vers Route 53, commencez par créer une zone hébergée pour le domaine. Pour de plus amples informations, veuillez consulter Configuration d'Amazon Route 53 en tant que service DNS d'un domaine existant.

Dans les deux cas, vous créez ensuite des enregistrements dans la zone hébergée pour spécifier la façon dont vous voulez acheminer le trafic du domaine et de ses sous-domaines. Par exemple, vous pouvez créer un enregistrement pour acheminer le trafic de www.example.com vers une CloudFront distribution ou vers un serveur Web de votre centre de données. Pour plus d'informations sur les enregistrements , consultez la section Utilisation des enregistrements.

Cette rubrique explique comment utiliser la console Amazon Route 53 pour créer, répertorier et supprimer des zones hébergées publiques.

> **Note**
>
> Vous pouvez également utiliser une zone hébergée privée Route 53 pour acheminer le trafic au sein d'une ou de plusieurs zones VPCs que vous créez avec le service Amazon VPC. Pour de plus amples informations, veuillez consulter Utilisation des zones hébergées privées.

Rubriques

- Remarques sur l'utilisation des zones hébergées publiques
- Création d'une zone hébergée publique
- Obtention de la liste des serveurs de noms d'une zone hébergée publique
- Liste des zones hébergées publiques
- Affichage des métriques de requête DNS pour une zone hébergée publique
- Suppression d'une zone hébergée publique
- Vérification des réponses DNS à partir de Route 53
- Configuration de serveurs de noms en marque blanche
- Registres NS et SOA créés par Amazon Route 53 pour une zone hébergée publique

Remarques sur l'utilisation des zones hébergées publiques

Notez les remarques suivantes sur l'utilisation des zones hébergées publiques :

Enregistrements NS et SOA

Lorsque vous créez une zone hébergée, Amazon Route 53 crée automatiquement un registre de serveur de noms (NS) et un registre de source de noms (SOA) pour la zone. Le registre NS

identifie les quatre serveurs de noms que vous attribuez à votre bureau d'enregistrement ou à votre service DNS afin que les requêtes DNS soient acheminées vers les serveurs de noms Route 53. Pour plus d'informations sur les enregistrements NS et SOA, consultez Registres NS et SOA créés par Amazon Route 53 pour une zone hébergée publique.

Plusieurs zones hébergées ayant le même nom

Vous pouvez créer plusieurs zones hébergées avec le même nom et ajouter différents registres à chaque zone hébergée. Route 53 affecte quatre serveurs de noms à chaque zone hébergée, et les serveurs de noms sont différents pour chacune d'elles. Lorsque vous mettez à jour les registres de serveur de noms de votre bureau d'enregistrement, veillez à utiliser les serveurs de noms Route 53 correspondant à la zone hébergée appropriée, c'est-à-dire celle qui contient les registres que Route 53 doit utiliser pour répondre aux requêtes concernant votre domaine. Route 53 ne renvoie jamais les valeurs des registres d'autres zones hébergées ayant le même nom.

Ensembles de délégations réutilisables

Par défaut, Route 53 affecte un ensemble unique de quatre serveurs de noms (appelés collectivement « ensemble de délégations ») pour chaque zone hébergée que vous créez. Si vous souhaitez créer un grand nombre de zones hébergées, vous pouvez créer un ensemble de délégations réutilisables par programme. (Les ensembles de délégations réutilisables ne sont pas disponibles dans la console Route 53.) Ensuite, vous pouvez créer des zones hébergées par programme et affecter le même ensemble de délégations réutilisables (les quatre mêmes serveurs de noms) à chaque zone hébergée.

Les ensembles de délégations réutilisables simplifient la migration du service DNS vers Route 53, car vous pouvez demander à votre bureau d'enregistrement de nom de domaine d'utiliser les quatre mêmes serveurs de noms pour tous les domaines pour lesquels vous souhaitez utiliser Route 53 en tant que service DNS. Pour plus d'informations, consultez CreateReusableDelegationSetle manuel Amazon Route 53 API Reference.

Création d'une zone hébergée publique

Une zone hébergée publique est un conteneur qui comporte des informations sur la façon dont vous souhaitez acheminer le trafic sur le réseau Internet pour un domaine spécifique (par exemple, example.com) et ses sous-domaines (acme.example.com, zenith.example.com). Une fois que vous avez créé une zone hébergée, vous créez des enregistrements qui spécifient la façon dont vous voulez acheminer le trafic du domaine et de ses sous-domaines.

> **Important**
>
> Vous pouvez créer une zone hébergée uniquement pour un domaine pour lequel vous disposez d'une autorisation d'administration. Généralement, cela signifie que le domaine vous appartient, mais il est également possible que vous développiez une application pour l'inscrit du domaine.

Pour créer une zone hébergée publique à l'aide de la console Route 53

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Si vous découvrez Route 53, choisissez Get started (Pour démarrer) sous DNS management (Gestion DNS).

   Si vous utilisez déjà Route 53, choisissez Hosted Zones (Zones hébergées) dans le panneau de navigation.
3. Choisissez Create hosted zone (Créer une zone hébergée).
4. Dans le volet Create Hosted Zone (Créer une zone hébergée), entrez le nom du domaine pour lequel vous souhaitez acheminer le trafic. Vous pouvez également entrer un commentaire facultatif.

   Pour plus d'informations sur la spécification d'autres caractères que a-z, 0-9 et - (trait d'union), et de noms de domaine internationaux, consultez Format de nom de domaine DNS.
5. Pour Type, acceptez la valeur par défaut de Zone hébergée publique.
6. Sélectionnez Create (Créer).
7. Créez les enregistrements qui indiquent la façon dont vous souhaitez acheminer le trafic pour le domaine et les sous-domaines. Pour de plus amples informations, veuillez consulter Utilisation des enregistrements.
8. Pour utiliser des enregistrements de la nouvelle zone hébergée pour acheminer le trafic pour votre domaine, consultez la rubrique applicable :

   - Si vous configurez Route 53 en tant que service DNS d'un domaine enregistré auprès d'un autre bureau d'enregistrement, consultez Configuration d'Amazon Route 53 en tant que service DNS d'un domaine existant.

- Si le domaine est enregistré auprès de Route 53, consultez Ajout ou modification de serveurs de noms et d'enregistrements de type glue pour un domaine.

Obtention de la liste des serveurs de noms d'une zone hébergée publique

Vous obtenez les serveurs de noms pour une zone hébergée publique si vous souhaitez modifier le service DNS pour votre enregistrement de domaine. Pour plus d'informations sur la modification de votre service DNS, veuillez consulter Configuration d'Amazon Route 53 en tant que service DNS d'un domaine existant.

> **Note**
>
> Certains bureaux d'enregistrement vous permettent uniquement de spécifier des serveurs de noms à l'aide d'adresses IP. Ils ne vous permettent pas de spécifier des noms de domaine complets. Si votre bureau d'enregistrement nécessite l'utilisation d'adresses IP, vous pouvez obtenir les adresses IP de vos serveurs de noms à l'aide de l'utilitaire dig (pour Mac, Unix ou Linux) ou de l'utilitaire nslookup (pour Windows). La modification des adresses IP de serveurs de noms est rare. Si nous avons besoin de modifier des adresses IP, vous serez averti à l'avance.

Pour obtenir les serveurs de noms pour une zone hébergée à l'aide de la console Route 53

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le panneau de navigation, choisissez Hosted zones (Zones hébergées).
3. Sur la page Hosted zones (Zones hébergées), choisissez la case d'option (pas le nom) de la zone hébergée, puis View details (Afficher les détails).
4. Sur la page des détails de la zone hébergée, choisissez Hosted zone details (Détails de la zone hébergée).
5. Notez les quatre serveurs répertoriés dans Name servers (Serveurs de noms).

Liste des zones hébergées publiques

Vous pouvez utiliser la console Amazon Route 53 pour répertorier toutes les zones hébergées que vous avez créées avec le AWS compte actuel. Pour plus d'informations sur la façon de répertorier les

zones hébergées à l'aide de l'API Route 53, consultez ListHostedZonesle manuel Amazon Route 53 API Reference.

Pour répertorier les zones hébergées publiques associées à un AWS compte à l'aide de la console Route 53

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le panneau de navigation, choisissez Zones hébergées. La page affiche la liste des zones hébergées associées au AWS compte avec lequel vous êtes actuellement connecté.
3. Pour filtrer les zones hébergées, utilisez la barre de recherche située en haut de la table.

   Le comportement de recherche varie selon que la zone hébergée contient jusqu'à 2 000 enregistrements ou plus de 2 000 enregistrements :

   Up to 2,000 hosted zones (Jusqu'à 2 000 zones hébergées)

   - Pour afficher les registres comportant des valeurs spécifiques, cliquez sur la barre de recherche, choisissez une propriété dans la liste déroulante, puis saisissez une valeur. Vous pouvez également saisir une valeur directement dans la barre de recherche et appuyez sur Entrée. Par exemple, pour afficher les zones hébergées dont le nom commence par **abc**, saisissez cette valeur dans la barre de recherche et appuyez sur Entrée.
   - Pour afficher uniquement les zones hébergées ayant le même type de zone hébergée, sélectionnez le type dans la liste déroulante, puis saisissez le type.

   More than 2,000 hosted zones (Plus de 2 000 zones hébergées)

   - Vous pouvez rechercher des propriétés en fonction du nom de domaine exact, de toutes les propriétés et du type.
   - Faites une recherche à l'aide du nom de domaine exact pour obtenir des résultats de recherche plus rapides.

Affichage des métriques de requête DNS pour une zone hébergée publique

Vous pouvez afficher le nombre total de requêtes DNS auxquelles Route 53 répond pour une zone hébergée publique spécifiée ou une combinaison de zones hébergées publiques. Les statistiques apparaissent dans CloudWatch, ce qui vous permet de visualiser un graphique, de choisir la période

que vous souhaitez consulter et de personnaliser les mesures de différentes manières. Vous pouvez également créer des alarmes et configurer des notifications, afin d'être averti lorsque le nombre de requêtes DNS au cours d'une période donnée est supérieur ou inférieur à un niveau spécifié.

> **Note**
>
> Route 53 envoie automatiquement le nombre de requêtes CloudWatch DNS à toutes les zones hébergées publiques. Vous n'avez donc rien à configurer avant de pouvoir consulter les métriques des requêtes. Les métriques de requête DNS n'impliquent aucun frais.

Quelles requêtes DNS sont comptabilisées ?

Les métriques incluent uniquement les requêtes que les résolveurs DNS transmettent à Route 53. Si un résolveur DNS a déjà mis en cache la réponse à une requête (par exemple, l'adresse IP d'un équilibreur de charge pour example.com), le résolveur continuera à renvoyer la réponse en cache sans transférer la requête à Route 53 jusqu'à ce que la TTL du registre correspondant arrive à expiration.

Selon le nombre de requêtes DNS qui sont soumises pour un nom de domaine (example.com) ou nom de sous-domaine (www.example.com), les résolveurs auxquels vos utilisateurs ont recours et la durée de vie (TTL) de l'enregistrement, les métriques de requêtes DNS peuvent contenir des informations concernant une seule requête sur les plusieurs milliers de requêtes qui sont soumises aux résolveurs DNS. Pour en savoir plus sur la façon dont les requêtes DNS fonctionnent, consultez Comment Amazon Route 53 achemine le trafic de votre domaine.

À partir de quand les mesures de requête pour une zone hébergée commencent-elles à apparaître dans CloudWatch ?

Une fois que vous avez créé une zone hébergée, un délai de plusieurs heures est nécessaire avant que la zone hébergée puisse apparaître dans CloudWatch. En outre, vous devez soumettre une requête DNS pour un enregistrement dans la zone hébergée afin que les données apparaissent.

Les métriques sont disponibles uniquement dans la région USA Est (Virginie du Nord).

Pour obtenir les métriques sur la console, vous devez choisir la région USA Est (Virginie du Nord). Pour obtenir des métriques à l'aide de la AWS CLI, vous devez soit laisser la AWS région non spécifiée, soit la spécifier `us-east-1` comme région. Les métriques Route 53 ne sont pas disponibles si vous choisissez une autre région.

CloudWatch métrique et dimension pour les requêtes DNS

Pour plus d'informations sur la CloudWatch métrique et la dimension des requêtes DNS, consultezSurveillance des zones hébergées à l'aide d'Amazon CloudWatch. Pour plus d'informations sur CloudWatch les métriques, consultez la section Utilisation CloudWatch des métriques Amazon dans le guide de CloudWatch l'utilisateur Amazon.

Obtenir des données plus détaillées sur les requêtes DNS

Pour obtenir des informations plus détaillées sur chaque requête DNS à laquelle Route 53 répond, notamment les valeurs suivantes, vous pouvez configurer la journalisation des requêtes :

- Domaine ou sous-domaine demandé
- Date et heure de la requête
- Type de registre DNS (comme A ou AAAA)
- Emplacement périphérique Route 53 ayant répondu à la requête DNS
- Code de réponse DNS, tel que `NoError` ou `ServFail`

Pour de plus amples informations, veuillez consulter Journalisation des requêtes DNS publiques.

Comment obtenir des métriques de requête DNS

Peu de temps après avoir créé une zone hébergée, Amazon Route 53 commence à envoyer des métriques et des dimensions une fois par minute à CloudWatch. Vous pouvez utiliser les procédures suivantes pour afficher les métriques sur la CloudWatch console ou les afficher à l'aide du AWS Command Line Interface (AWS CLI).

Rubriques

- Afficher les métriques des requêtes DNS pour une zone hébergée publique dans la CloudWatch console
- Obtenir des métriques de requêtes DNS à l'aide du AWS CLI

Afficher les métriques des requêtes DNS pour une zone hébergée publique dans la CloudWatch console

Pour consulter les métriques des requêtes DNS pour les zones hébergées publiques dans la CloudWatch console, effectuez la procédure suivante.

Pour consulter les métriques des requêtes DNS pour une zone hébergée publique sur la CloudWatch console

1. Connectez-vous à la CloudWatch console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans le panneau de navigation, sélectionnez Métriques.
3. Dans la liste des AWS régions située dans le coin supérieur droit de la console, choisissez USA Est (Virginie du Nord). Les statistiques de Route 53 ne sont pas disponibles si vous choisissez une autre AWS région.
4. Sous l'onglet Toutes les métriques, choisissez Route 53.
5. Choisissez Hosted Zone Metrics (Métriques de la zone hébergée).
6. Cochez la case correspondant à une ou plusieurs zones hébergées portant le nom de la métrique DNSQueries.
7. Dans l'onglet Graphed metrics (Métriques représentées graphiquement), modifiez les valeurs applicables pour afficher les métriques au format de votre choix.

   Dans le champ Statistiques, sélectionnez Somme ou SampleCount; ces statistiques affichent toutes deux la même valeur.

Obtenir des métriques de requêtes DNS à l'aide du AWS CLI

Pour obtenir les métriques des requêtes DNS à l'aide de AWS CLI, vous devez utiliser la get-metric-datacommande. Remarques :

- Vous spécifiez la plupart des valeurs pour la commande dans un fichier JSON distinct. Pour de plus amples informations, veuillez consulter get-metric-data.
- La commande renvoie une valeur pour chaque intervalle que vous spécifiez pour `Period` dans le fichier JSON. `Period` est en secondes. Par conséquent, si vous spécifiez une période de cinq minutes et que vous indiquez `60` pour `Period`, vous obtenez cinq valeurs. Si vous spécifiez une période de cinq minutes et que vous indiquez `300` pour `Period`, vous obtenez une valeur.
- Dans le fichier JSON, vous pouvez spécifier n'importe quelle valeur pour `Id`.
- Laissez la AWS région non spécifiée ou spécifiez-la `us-east-1` comme région. Les métriques Route 53 ne sont pas disponibles si vous choisissez une autre région. Pour plus d'informations, consultez la section Configuration de la AWS CLI dans le guide de AWS Command Line Interface l'utilisateur.

Voici la AWS CLI commande que vous utilisez pour obtenir les métriques des requêtes DNS pour la période de cinq minutes comprise entre 4 h 01 et 4 h 07 le 1er mai 2019. Le paramètre `metric-data-queries` fait référence à l'exemple de fichier JSON qui suit la commande.

```
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
```

Voici l'exemple de fichier JSON :

```
[
    {
        "Id": "my_dns_queries_id",
        "MetricStat": {
            "Metric": {
                "Namespace": "AWS/Route53",
                "MetricName": "DNSQueries",
                "Dimensions": [
                    {
                        "Name": "HostedZoneId",
                        "Value": "Z1D633PJN98FT9"
                    }
                ]
            },
            "Period": 60,
            "Stat": "Sum"
        },
        "ReturnData": true
    }
]
```

Voici le résultat de cette commande. Remarques :

- L'heure de début et l'heure de fin de la commande couvrent une période de sept minutes, de `2019-05-01T04:01:00Z` à `2019-05-01T04:07:00Z`.
- Il n'y a que six valeurs renvoyées. Il n'y a pas de valeur pour `2019-05-01T04:05:00Z`, car il n'y a eu aucune requête DNS pendant cette minute.
- La valeur de `Period` spécifiée dans le fichier JSON est `60` (secondes). Les valeurs sont donc présentées par intervalles d'une minute.

```
{
```

```
    "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"
            ]
        }
    ]
}
```

Suppression d'une zone hébergée publique

Cette section explique comment supprimer une zone hébergée publique à l'aide de la console Amazon Route 53.

Vous pouvez supprimer une zone hébergée uniquement s'il n'existe aucun autre enregistrement que les enregistrements SOA et NS par défaut. Si votre zone hébergée contient d'autres enregistrements, vous devez les supprimer avant de pouvoir supprimer votre zone hébergée. Cela vous empêche de supprimer accidentellement une zone hébergée qui contient encore des enregistrements.

Rubriques

- Empêcher le routage du trafic vers votre domaine
- Suppression des zones hébergées publiques qui étaient créées par un autre service
- Utilisation de la console Route 53 pour supprimer une zone hébergée publique

Empêcher le routage du trafic vers votre domaine

Si vous souhaitez conserver l'enregistrement de votre domaine, mais que vous souhaitez arrêter d'acheminer le trafic Internet vers votre site web ou votre application web, nous vous recommandons de supprimer les enregistrements dans la zone hébergée au lieu de supprimer la zone hébergée.

> **Important**
>
> Si vous supprimez une zone hébergée, vous ne pourrez pas annuler cette suppression. Vous devez créer une nouvelle zone hébergée et mettre à jour les serveurs de noms pour l'enregistrement de votre domaine, ce qui peut nécessiter jusqu'à 48 heures pour prendre effet. En outre, si vous supprimez une zone hébergée, quelqu'un peut pirater le domaine et acheminer le trafic vers ses propres ressources à l'aide de votre nom de domaine.
> Si vous avez délégué la responsabilité d'un sous-domaine à une zone hébergée et que vous souhaitez supprimer la zone hébergée enfant, vous devez également mettre à jour la zone hébergée parent en supprimant l'enregistrement NS portant le même nom que la zone hébergée enfant. Par exemple, si vous souhaitez supprimer la zone hébergée acme.example.com, vous devez également supprimer l'enregistrement NS acme.example.com dans la zone hébergée example.com. Nous vous recommandons de supprimer d'abord l'enregistrement NS et d'attendre pendant la durée de vie (TTL) sur l'enregistrement NS avant de supprimer la zone hébergée enfant. Vous êtes ainsi assuré que personne ne peut pirater la zone hébergée enfant lors de la période pendant laquelle les résolveurs DNS ont encore les serveurs de noms pour la zone hébergée enfant mis en cache.

Si vous souhaitez éviter les frais mensuels pour la zone hébergée, vous pouvez transférer le service DNS pour le domaine vers un service DNS gratuit. Lorsque vous transférez le service DNS, vous devez mettre à jour les serveurs de noms pour l'enregistrement du domaine. Si le domain est enregistré auprès de Route 53, consultez Ajout ou modification de serveurs de noms et d'enregistrements de type glue pour un domaine pour savoir comment remplacer des serveurs de noms Route 53 par des serveurs de noms pour le nouveau service DNS. Si le domaine est enregistré auprès d'un autre bureau d'enregistrement, utilisez la méthode fournie par le bureau d'enregistrement pour mettre à jour les serveurs de noms pour l'enregistrement du domaine. Pour en savoir plus, effectuez une recherche Internet sur « service DNS gratuit. »

Suppression des zones hébergées publiques qui étaient créées par un autre service

Si une zone hébergée a été créée par un autre service, vous ne pouvez pas la supprimer à l'aide de la console Route 53. Au lieu de cela, vous devez utiliser le processus de l'autre service :

- AWS Cloud Map— Pour supprimer une zone hébergée AWS Cloud Map créée lorsque vous avez créé un espace de noms DNS public, supprimez l'espace de noms. AWS Cloud Map supprime automatiquement la zone hébergée. Pour plus d'informations, consultez Suppression des espaces de noms dans le Guide du développeur AWS Cloud Map .
- Découverte du service Amazon Elastic Container Service (Amazon ECS) – Pour supprimer une zone hébergée publique créée par Amazon ECS lorsque vous avez créé un service à l'aide de la découverte de service, supprimez les services Amazon ECS qui utilisent l'espace de noms et supprimez l'espace de noms. Pour plus d'informations, consultez Suppression d'un service dans le Guide du développeur Amazon Elastic Container Service.

Utilisation de la console Route 53 pour supprimer une zone hébergée publique

Pour utiliser la console Route 53 afin de supprimer une zone hébergée publique, exécutez la procédure suivante.

Pour supprimer une zone hébergée publique à l'aide de la console Route 53

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le panneau de navigation, choisissez Hosted zones (Zones hébergées), et choisissez le lien surligné de la zone hébergée que vous souhaitez supprimer.
3. Vérifiez que la zone hébergée que vous souhaitez supprimer contient uniquement un enregistrement NS et un enregistrement SOA. Si elle contient d'autres registres, supprimez-les : Vous devrez également désactiver la signature DNSSEC :

   - Sur la page de détails de la zone hébergée, dans la liste des Records (Enregistrements), si la liste des enregistrements inclut des enregistrements pour lesquels la valeur de la colonne Type n'est ni NS ni SOA, choisissez la ligne, et choisissez Delete (Supprimer).

     Pour sélectionner plusieurs enregistrements consécutifs, appuyez sur la touche MAJ et maintenez-la enfoncée, puis sélectionnez la dernière ligne. Pour sélectionner plusieurs enregistrements non consécutifs, appuyez sur la touche Ctrl et maintenez-la enfoncée, puis sélectionnez les autres lignes.

> **Note**
>
> Si vous avez créé des enregistrements NS pour des sous-domaines dans la zone hébergée, supprimez également ces enregistrements.

4. Retournez à la page Hosted Zones (Zones hébergées), et choisissez la ligne de la zone hébergée que vous souhaitez supprimer.
5. Sélectionnez Delete (Supprimer).
6. Saisissez la clé de confirmation et choisissez Delete (Supprimer).
7. Si vous ne voulez pas que le domaine soit disponible sur Internet, nous vous recommandons de transférer le service DNS vers un service DNS gratuit, puis de supprimer la zone hébergée Route 53. Cela évitera les requêtes DNS futures d'être mal acheminées.

   Si le domain est enregistré auprès de Route 53, consultez Ajout ou modification de serveurs de noms et d'enregistrements de type glue pour un domaine pour savoir comment remplacer des serveurs de noms Route 53 par des serveurs de noms pour le nouveau service DNS. Si le domaine est enregistré auprès d'un autre bureau d'enregistrement, utilisez la méthode fournie par le bureau d'enregistrement pour changer les serveurs de noms du domaine.

   > **Note**
   >
   > Si vous supprimez une zone hébergée pour un sous-domaine (acme.example.com), vous n'avez pas besoin de changer les serveurs de noms du domaine (example.com).

Vérification des réponses DNS à partir de Route 53

Si vous avez créé une zone hébergée Amazon Route 53 pour votre domaine, vous pouvez utiliser l'outil de vérification DNS dans la console pour voir de quelle manière Route 53 répond aux requêtes DNS si vous configurez votre domaine pour qu'il utilise Route 53 en tant que service DNS. Pour les enregistrements de géolocalisation, de géoproximité et de latence, vous pouvez également simuler des requêtes à partir d'un résolveur DNS et/ou d'une adresse IP de client particuliers pour déterminer la réponse que Route 53 renverrait.

> **Important**
>
> L'outil ne soumet pas de requêtes au système de noms de domaine. Il répond uniquement en fonction des paramètres des enregistrements de la zone hébergée. L'outil renvoie les mêmes informations, même si la zone hébergée est actuellement utilisée pour acheminer le trafic pour le domaine.

L'outil de vérification DNS fonctionne pour les zones hébergées publiques uniquement.

> **Note**
>
> L'outil de vérification DNS renvoie des informations similaires à celles que vous attendez de la section de réponse de la commande `dig`. Par conséquent, si vous recherchez les serveurs de noms d'un sous-domaine qui pointent vers les serveurs de noms parents, ceux-ci ne seront pas renvoyés.

Rubriques

- Utilisation de l'outil de vérification pour voir comment Amazon Route 53 répond aux requêtes DNS
- Utilisation de l'outil de vérification pour simuler des requêtes d'adresses IP spécifiques (enregistrements de géolocalisation et de latence uniquement)

Utilisation de l'outil de vérification pour voir comment Amazon Route 53 répond aux requêtes DNS

Vous pouvez utiliser l'outil pour voir quelle réponse Amazon Route 53 renvoie en réponse à une requête DNS pour un registre.

Pour utiliser l'outil de vérification pour voir comment Route 53 répond aux requêtes DNS

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation, choisissez Hosted Zones (Zones hébergées).
3. Sur la page Hosted Zones (Zones hébergées), choisissez le nom d'une zone hébergée. La console affiche la liste des enregistrements pour cette zone hébergée.
4. Pour accéder directement à la page Check response from Route 53 (Vérifier la réponse depuis Route 53), choisissez Test record (Tester le registre).

5. Indiquez l'une des valeurs suivantes :
   - Nom de l'enregistrement, à l'exclusion du nom de la zone hébergée. Par exemple, pour vérifier www.example.com, entrez www. Pour vérifier example.com, laissez le champ Record name (Nom de l'enregistrement) vide.
   - Type de l'enregistrement à vérifier, comme A ou CNAME.
6. Choisissez Get Response.
7. La section Response returned by Route 53 inclut les valeurs suivantes :

   DNS response code

   Code qui indique si la requête était valide ou non. Le code de réponse le plus courant est NOERROR, ce qui signifie que la requête était valide. Si la réponse n'est pas valide, Route 53 renvoie un code de réponse qui en explique la raison. Pour une liste des codes de réponse possibles, consultez DNS RCODES sur le site web IANA.

   Protocole

   Protocole utilisé par Amazon Route 53 pour répondre à la requête, UDP ou TCP.

   Response returned by Route 53

   La valeur que Route 53 renverrait à une application web. La valeur est l'une des suivantes :
   - Pour les enregistrements sans alias, la réponse contient la ou les valeurs dans l'enregistrement.
   - Pour plusieurs enregistrements qui ont les mêmes nom et type, qui inclut pondéré, latence, géolocalisation et basculement, la réponse contient la valeur de l'enregistrement approprié, basée sur la demande.
   - Pour les enregistrements d'alias qui font référence à AWS des ressources autres qu'un autre enregistrement, la réponse contient une adresse IP ou un nom de domaine pour la AWS ressource, selon le type de ressource.
   - Pour les enregistrements d'alias qui font référence à d'autres enregistrements, la réponse contient la ou les valeurs de l'enregistrement référencé.

Utilisation de l'outil de vérification pour simuler des requêtes d'adresses IP spécifiques (enregistrements de géolocalisation et de latence uniquement)

Si vous avez créé des enregistrements de latence ou géolocalisation, vous pouvez utiliser l'outil de vérification pour simuler des requêtes à partir de l'adresse IP pour un résolveur DNS et un client.

Pour utiliser l'outil de vérification afin de simuler des requêtes à partir des adresses IP spécifiées

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation, choisissez Hosted Zones (Zones hébergées).
3. Sur la page Hosted Zones (Zones hébergées), choisissez le nom d'une zone hébergée. La console affiche la liste des enregistrements pour cette zone hébergée.
4. Pour accéder directement à la page Check response from Route 53, choisissez Test record set.

   Pour accéder à la page Check response from Route 53 relative à un enregistrement spécifique, cochez la case correspondant à cet enregistrement et choisissez Test record set.
5. Si vous avez choisi Test record set (Tester le jeu d'enregistrements) sans avoir choisi un enregistrement au préalable, spécifiez les valeurs suivantes :

   - Nom de l'enregistrement, à l'exclusion du nom de la zone hébergée. Par exemple, pour vérifier www.example.com, entrez www. Pour vérifier example.com, laissez le champ Record name (Nom de l'enregistrement) vide.
   - Type de l'enregistrement à vérifier, comme A ou CNAME.
6. Spécifiez les valeurs applicables :

   Resolver IP address (Adresse IP du résolveur)

   Spécifiez une IPv6 adresse IPv4 OR pour simuler l'emplacement du résolveur DNS utilisé par un client pour effectuer des demandes. C'est utile pour tester les enregistrements de latence et de géolocalisation. Si vous omettez cette valeur, l'outil utilise l'adresse IP d'un résolveur DNS dans la région AWS USA Est (Virginie du Nord) (us-east-1).

   EDNS0 client subnet IP

   Si le résolveur prend en charge EDNS0, entrez l'IP du sous-réseau client pour une adresse IP dans l'emplacement géographique approprié, par exemple, 192.0.2.0 ou 2001:db8:85a3::8a2e:370:7334.

Masque de sous-réseau

Si vous spécifiez une adresse IP pour EDNS0 client subnet IP, vous pouvez spécifier le nombre de bits de l'adresse IP que vous voulez que l'outil de vérification inclue dans la requête DNS. Par exemple, si vous spécifiez 192.0.2.44 pour EDNS0 client subnet IP et 24 pour Subnet mask, l'outil de vérification simulera une requête à partir de 192.0.2.0/24. La valeur par défaut est de 24 bits pour les IPv4 adresses et de 64 bits pour les IPv6 adresses.

7. Choisissez Get Response.
8. La section Response returned by Route 53 inclut les valeurs suivantes :

DNS query sent to Route 53

La requête, au format BIND, que l'outil de vérification a envoyé à Route 53. C'est le même format que celui qu'une application web utilise pour envoyer une requête. Les trois valeurs sont généralement le nom de l'enregistrement, IN (pour Internet) et le type de l'enregistrement.

DNS response code

Code qui indique si la requête était valide ou non. Le code de réponse le plus courant est NOERROR, ce qui signifie que la requête était valide. Si la réponse n'est pas valide, Route 53 renvoie un code de réponse qui en explique la raison. Pour une liste des codes de réponse possibles, consultez DNS RCODES sur le site web IANA.

Protocole

Protocole utilisé par Amazon Route 53 pour répondre à la requête, UDP ou TCP.

Response returned by Route 53

La valeur que Route 53 renverrait à une application web. La valeur est l'une des suivantes :

- Pour les enregistrements sans alias, la réponse contient la ou les valeurs dans l'enregistrement.
- Pour plusieurs enregistrements qui ont les mêmes nom et type, qui inclut pondéré, latence, géolocalisation et basculement, la réponse contient la valeur de l'enregistrement approprié, basée sur la demande.
- Pour les enregistrements d'alias qui font référence à AWS des ressources autres qu'un autre enregistrement, la réponse contient une adresse IP ou un nom de domaine pour la AWS ressource, selon le type de ressource.

- Pour les enregistrements d'alias qui font référence à d'autres enregistrements, la réponse contient la ou les valeurs de l'enregistrement référencé.

Configuration de serveurs de noms en marque blanche

Chaque zone hébergée Amazon Route 53 est associée à quatre serveurs de noms, appelés collectivement « ensemble de délégations ». Par défaut, les noms des serveurs de noms ressemblent à ns-2048.awsdns-64.com. Si vous souhaitez que le nom de domaine de vos serveurs de noms soit le même que celui de votre zone hébergée, par exemple, ns1.example.com, vous pouvez configurer des serveurs de noms en marque blanche, également appelés « serveurs de noms personnels » ou « serveurs de noms privés ».

Les étapes suivantes expliquent comment configurer un ensemble de quatre serveurs de noms en marque blanche réutilisables pour plusieurs domaines. Supposons par exemple que vous possédez les domaines example.com, example.org et example.net. Avec ces étapes, vous pouvez configurer des serveurs de noms en marque blanche pour example.com et les réutiliser pour example.org et example.net.

Rubriques

- Étape 1 : créer un ensemble de délégations réutilisables Route 53
- Étape 2 : créer ou recréer des zones hébergées Amazon Route 53 et modifier la TTL des registres NS et SOA
- Étape 3 : Recréer des enregistrements pour vos zones hébergées
- Étape 4 : Obtenir des adresses IP
- Étape 5 : Créer des enregistrements pour les serveurs de noms en marque blanche
- Étape 6 : Mettre à jour les enregistrements NS et SOA
- Étape 7 : Créer des enregistrements de type glue et changer les serveurs de noms du bureau d'enregistrement
- Étape 8 : Surveiller le trafic du site web ou de l'application
- Étape 9 : TTLs Revenez à leurs valeurs d'origine
- Étape 10 : (Facultatif) Contacter les services DNS récursifs

Étape 1 : créer un ensemble de délégations réutilisables Route 53

Les serveurs de noms en marque blanche sont associés à un ensemble de délégations réutilisables Route 53. Vous pouvez utiliser des serveurs de noms en marque blanche pour une zone hébergée uniquement si la zone hébergée et le jeu de délégation réutilisable ont été créés par le même AWS compte.

Pour créer un ensemble de délégation réutilisable, vous pouvez utiliser l'API Route 53, la AWS CLI ou l'une des AWS SDKs. Pour plus d'informations, consultez la documentation de suivante :

- API Route 53 — Voir CreateReusableDelegationSetla référence de l'API Amazon Route 53
- AWS CLI — Voir create-reusable-delegation-setdans la référence des AWS CLI commandes
- AWS SDKsConsultez la documentation du SDK applicable sur la page de AWS documentation

Étape 2 : créer ou recréer des zones hébergées Amazon Route 53 et modifier la TTL des registres NS et SOA

Créez ou recréez des zones hébergées Amazon Route 53 :

- Si vous n'utilisez pas actuellement Route 53 en tant que service DNS pour les domaines pour lesquels vous souhaitez utiliser des serveurs de noms en marque blanche – Créez les zones hébergées et spécifiez l'ensemble de délégations réutilisables que vous avez créé lors de l'étape précédente avec chaque zone hébergée. Pour plus d'informations, consultez CreateHostedZonele manuel Amazon Route 53 API Reference.
- Si vous utilisez Route 53 en tant que service DNS pour les domaines pour lesquels vous souhaitez utiliser des serveurs de noms en marque blanche – Vous devez recréer les zones hébergées pour lesquelles vous souhaitez utiliser des serveurs de noms en marque blanche et spécifier l'ensemble de délégations réutilisables que vous avez créé lors de l'étape précédente pour chaque zone hébergée.

> **Important**
>
> Vous ne pouvez pas modifier les serveurs de noms qui sont associés à une zone hébergée existante. Vous pouvez associer un ensemble de délégations réutilisables à une zone hébergée uniquement lorsque vous créez la zone hébergée.

Lorsque vous créez les zones hébergées, et avant d'essayer d'accéder aux ressources pour les domaines correspondants, modifiez les valeurs suivantes relatives à la durée de vie pour chaque zone hébergée :

- Définissez la durée de vie pour l'enregistrement NS pour la zone hébergée sur 60 secondes maximum.
- Définissez la durée de vie minimale pour l'enregistrement SOA pour la zone hébergée sur 60 secondes maximum. Il s'agit de la dernière valeur de l'enregistrement SOA.

Si vous attribuez accidentellement à votre bureau d'enregistrement des adresses IP incorrectes pour vos serveurs de noms en marque blanche, votre site web devient indisponible et reste indisponible pendant la durée de vie après la résolution du problème. En définissant une durée de vie courte, vous réduisez le temps d'indisponibilité de votre site web.

Pour plus d'informations sur la création de zones hébergées et la spécification d'un ensemble de délégation réutilisable pour les serveurs de noms des zones hébergées, consultez CreateHostedZonele manuel Amazon Route 53 API Reference.

Étape 3 : Recréer des enregistrements pour vos zones hébergées

Créez des enregistrements dans les zones hébergées que vous avez créées à l'étape 2 :

- Si vous migrez un service DNS pour vos domaines vers Amazon Route 53 – Vous pouvez créer des registres en important des informations concernant vos registres existants. Pour de plus amples informations, veuillez consulter Création d'enregistrements par importation d'un fichier de zone.
- Si vous remplacez des zones hébergées existantes pour pouvoir utiliser des serveurs de noms en marque blanche – Dans les nouvelles zones hébergées, recréez les registres qui apparaissent dans vos zones hébergées actuelles. Route 53 ne permet pas d'exporter des registres depuis une zone hébergée, mais certains fournisseurs tiers le permettent. Vous pouvez ensuite utiliser la fonction d'importation Route 53 pour importer des registres sans alias, pour lesquels la politique de routage est simple. Il n'existe aucun moyen d'exporter et de réimporter des enregistrements d'alias ou des enregistrements pour lesquels la stratégie de routage n'est pas simple.

  Pour plus d'informations sur la création d'enregistrements à l'aide de l'API Route 53, consultez CreateHostedZonele manuel Amazon Route 53 API Reference. Pour plus d'informations sur la création de registres à l'aide de la console Route 53, consultez Utilisation des enregistrements.

Étape 4 : Obtenir des adresses IP

Obtenez les IPv6 adresses IPv4 et des serveurs de noms du jeu de délégation réutilisable, puis complétez le tableau suivant.

Nom d'un serveur de noms dans votre ensemble de délégations réutilisables (exemple : Ns-2048.awsdns-64.com)	IPv4 et IPv6 adresses	Le nom que vous souhaitez attribuer au serveur de noms en marque blanche (exemple : ns1.example.com)
	IPv4: IPv6:	
	IPv4: IPv6:	
	IPv4: IPv6:	
	IPv4: IPv6:	

Supposons par exemple que les quatre serveurs de noms de votre ensemble de délégations réutilisables sont :

- ns-2048.awsdns-64.com
- ns-2049.awsdns-65.net
- ns-2050.awsdns-66.org
- ns-2051.awsdns-67.co.uk

Voici les commandes Linux et Windows à exécuter pour obtenir les adresses IP pour le premier de vos quatre serveurs de noms :

Commandes dig pour Linux

```
% 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
```

commande nslookup pour Windows

```
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
```

Étape 5 : Créer des enregistrements pour les serveurs de noms en marque blanche

Dans la zone hébergée portant le même nom (par exemple, example.com) que le nom de domaine des serveurs de noms en marque blanche (par exemple, ns1.example.com), créez huit enregistrements :

- Un enregistrement A pour chaque serveur de noms en marque blanche
- Un enregistrement AAAA pour chaque serveur de noms en marque blanche

> **Important**
>
> Si vous utilisez les mêmes serveurs de noms en marque blanche pour plusieurs zones hébergées, n'effectuez pas cette opération pour les autres zones hébergées.

Pour chaque enregistrement, spécifiez les valeurs suivantes. Reportez-vous au tableau que vous avez rempli à l'étape précédente :

Stratégie de routage

Spécifiez Simple routing (Routage simple).

Nom de l'enregistrement

Le nom que vous souhaitez attribuer à l'un de vos serveurs de noms en marque blanche, par exemple, ns1.example.com. Pour le préfixe (ns1 dans cet exemple), vous pouvez utiliser n'importe quelle valeur valide dans un nom de domaine.

Valeur/acheminer le trafic vers

IPv6 Adresse IPv4 ou de l'un des serveurs de noms Route 53 de votre ensemble de délégations réutilisable.

> **Important**
>
> Si vous spécifiez des adresses IP incorrectes lors de la création d'enregistrements pour vos serveurs de noms en marque blanche, votre site web ou votre application web devient indisponible sur Internet lorsque vous effectuez les étapes suivantes. Même si vous corrigez immédiatement les adresses IP, votre site web ou votre application web reste inaccessible pendant la durée de vie définie.

Type de registre

Spécifiez A lorsque vous créez des enregistrements pour les IPv4 adresses.

Spécifiez AAAA lorsque vous créez des enregistrements pour les IPv6 adresses.

TTL (secondes)

Cette valeur correspond à la durée pendant laquelle les résolveurs DNS mettent en cache les informations contenues dans ce registre avant de transférer une autre requête DNS à Route 53. Nous vous recommandons de spécifier une valeur initiale de 60 secondes maximum, afin de pouvoir procéder à une récupération rapide si vous spécifiez accidentellement des valeurs incorrectes dans ces enregistrements.

Étape 6 : Mettre à jour les enregistrements NS et SOA

Mettez à jour les enregistrements SOA et NS dans les zones hébergées pour lesquelles vous souhaitez utiliser des serveurs de noms en marque blanche. Effectuez les étapes 6 à 8 pour une zone hébergée et le domaine correspondant en même temps, puis répétez l'opération pour une autre zone hébergée et le domaine correspondant.

> **Important**
>
> Commencez par la zone hébergée Amazon Route 53 portant le même nom de domaine (par exemple, example.com) que les serveurs de noms en marque blanche (par exemple, ns1.example.com).

1. Mettez à jour le registre SOA en remplaçant le nom du serveur de noms Route 53 par le nom de l'un de vos serveurs de noms en marque blanche.

   Exemple

   Remplacez le nom du serveur de noms Route 53 :

   ```
   ns-2048.awsdns-64.net. hostmaster.example.com. 1 7200 900 1209600 60
   ```

   par le nom de l'un de vos serveurs de noms en marque blanche :

   ```
   ns1.example.com. hostmaster.example.com. 1 7200 900 1209600 60
   ```

   > **Note**
   >
   > Vous avez modifié la dernière valeur, la durée de vie (TTL), dans Étape 2 : créer ou recréer des zones hébergées Amazon Route 53 et modifier la TTL des registres NS et SOA.

   Pour plus d'informations sur la mise à jour de registres à l'aide de la console Route 53, consultez Modification des enregistrements.

2. Dans l'enregistrement NS, notez les noms des serveurs de noms actuels pour le domaine, afin de pouvoir les rétablir si nécessaire.
3. Mettez à jour l'enregistrement NS. Remplacez les noms des serveurs de noms Route 53 par les noms de vos quatre serveurs de noms en marque blanche, par exemple, `ns1.example.com`, `ns2.example.com`, `ns3.example.com` et `ns4.example.com`.

Étape 7 : Créer des enregistrements de type glue et changer les serveurs de noms du bureau d'enregistrement

Utilisez la méthode fournie par le bureau d'enregistrement pour créer des enregistrements de type glue et changer les serveurs de noms du bureau d'enregistrement :

1. Ajoutez des enregistrements de type glue :

   - Si vous mettez à jour le domaine portant le même nom de domaine que les serveurs de noms en marque blanche – Créez quatre registres Glue pour lesquels les noms et les adresses IP correspondent aux valeurs obtenues à l'étape 4. Incluez à la fois l' IPv6 adresse IPv4 et l'adresse d'un serveur de noms en marque blanche dans l'enregistrement Glue correspondant, par exemple :

     ns1.example.com – Adresses IP = 192.0.2.117 et 2001:db8:85a3::8a2e:370:7334

     Les bureaux d'enregistrement utilisent une terminologie riche pour les enregistrements de type glue. Cette opération est également qualifiée d'enregistrement de nouveaux serveurs de noms.
   - Si vous mettez à jour un autre domaine – Si Route 53 est votre service DNS, vous devez d'abord terminer l'étape de la puce précédente et créer les glue records correspondants au nom de domaine. Ensuite, passez directement à l'étape 2 de cette procédure.
2. Modifiez les serveurs de noms du domaine par les noms de vos serveurs de noms en marque blanche.

Si vous utilisez Amazon Route 53 en tant que service DNS, consultez Ajout ou modification de serveurs de noms et d'enregistrements de type glue pour un domaine.

Étape 8 : Surveiller le trafic du site web ou de l'application

Surveillez le trafic du site web ou de l'application pour lequel vous avez créé des enregistrements de type glue et modifié les serveurs de noms à l'étape 7 :

- Si le trafic s'interrompt – Utilisez la méthode fournie par le bureau d'enregistrement pour modifier les serveurs de noms pour le domaine pour rétablir les serveurs de noms Route 53 précédents. Il s'agit des serveurs de noms que vous avez notés à l'étape 6b. Déterminez ce qui s'est mal passé.
- Si le trafic n'est pas affecté – Répétez les étapes 6 à 8 pour les autres zones hébergées pour lesquelles vous souhaitez utiliser les mêmes serveurs de noms en marque blanche.

Étape 9 : TTLs Revenez à leurs valeurs d'origine

Pour toutes les zones hébergées qui utilisent désormais des serveurs de noms en marque blanche, modifiez les valeurs suivantes :

- Modifiez la durée de vie de l'enregistrement NS pour la zone hébergée par une valeur plus courante, par exemple, 172 800 secondes (deux jours).
- Remplacez la durée de vie minimale pour l'enregistrement SOA de la zone hébergée par une valeur plus courante, par exemple 900 secondes. Il s'agit de la dernière valeur de l'enregistrement SOA.

Étape 10 : (Facultatif) Contacter les services DNS récursifs

Facultatif Si vous utilisez le routage de géolocalisation Amazon Route 53, contactez les services DNS récursifs qui prennent en charge l' edns-client-subnetextension EDNS0 et donnez-leur les noms de vos serveurs de noms en marque blanche. Cela permet de garantir que ces services DNS continueront à acheminer les requêtes DNS vers l'emplacement Route 53 optimal en fonction de l'emplacement géographique approximatif duquel provient la requête.

Registres NS et SOA créés par Amazon Route 53 pour une zone hébergée publique

Pour chaque zone hébergée publique que vous créez, Amazon Route 53 crée automatiquement un registre de serveur de noms (NS) et un registre de source de noms (SOA). Vous avez rarement besoin de modifier ces enregistrements.

Rubriques

- Enregistrement de serveur de noms (NS)
- Enregistrement de source de noms (SOA)

Enregistrement de serveur de noms (NS)

Amazon Route 53 crée automatiquement un registre de serveur de noms (NS) portant le même nom que votre zone hébergée. Il répertorie les quatre serveurs de noms qui sont les serveurs de noms faisant autorité pour votre zone hébergée. Sauf dans de rares cas, nous vous recommandons de ne pas ajouter, modifier ou supprimer des serveurs de noms dans cet enregistrement.

Les exemples suivants illustrent le format des noms des serveurs de noms Route 53 (il s'agit d'exemples ; ne les utilisez pas lorsque vous mettez à jour les registres des serveurs de noms de votre bureau d'enregistrement) :

- ns-2048.awsdns-64.com
- ns-2049.awsdns-65.net
- ns-2050.awsdns-66.org
- ns-2051.awsdns-67.co.uk

Pour obtenir la liste des serveurs de noms pour votre zone hébergée :

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le panneau de navigation, choisissez Hosted zones (Zones hébergées).
3. Sur la page Hosted zones (Zones hébergées), choisissez la case d'option (pas le nom) de la zone hébergée, puis View details (Afficher les détails).
4. Sur la page des détails de la zone hébergée, choisissez Hosted zone details (Détails de la zone hébergée).
5. Notez les quatre serveurs répertoriés dans Name servers (Serveurs de noms).

Pour plus d'informations sur la migration d'un service DNS d'un autre fournisseur de services DNS vers Route 53, consultez Configuration d'Amazon Route 53 en tant que service DNS d'un domaine existant.

Enregistrement de source de noms (SOA)

L'enregistrement de source de noms (SOA) identifie les informations DNS de base relatives au domaine, par exemple :

```
ns-2048.awsdns-64.net. hostmaster.example.com. 1 7200 900 1209600 86400
```

Un enregistrement SOA inclut les éléments suivants :

- Le serveur de noms Route 53 ayant créé le registre SOA, par exemple, `ns-2048.awsdns-64.net`.
- L'adresse e-mail de l'administrateur. Le symbole `@` est remplacé par une période, par exemple, `hostmaster.example.com`. La valeur par défaut est une adresse e-mail amazon.com qui n'est pas contrôlée.
- Un numéro de série que vous pouvez facultativement augmenter chaque fois que vous mettez à jour un registre dans la zone hébergée. Route 53 n'augmente pas automatiquement le numéro. (Le

numéro de série est utilisé par les services DNS prenant en charge les serveurs DNS secondaires.) Dans l'exemple, cette valeur est `1`.

- Un temps d'actualisation, en secondes, pendant lequel les serveurs DNS secondaires patientent avant d'interroger l'enregistrement SOA du serveur DNS principal pour vérifier les modifications. Dans l'exemple, cette valeur est `7200`.
- L'intervalle de nouvelle tentative, en secondes, pendant lequel un serveur secondaire patiente avant de réessayer le transfert d'une zone ayant échoué. En général, l'intervalle de nouvelle tentative est inférieur au temps d'actualisation. Dans l'exemple, cette valeur est `900` (15 minutes).
- Le délai, en secondes, pendant lequel un serveur secondaire continue d'essayer de finaliser un transfert de zone. Si ce délai expire avant la réussite d'un transfert de zone, le serveur secondaire ne répondra plus aux requêtes, car il considère que les données sont trop anciennes pour être fiables. Dans l'exemple, cette valeur est `1209600` (deux semaines).
- La durée de vie minimale (TTL). Cette valeur permet de définir la durée pendant laquelle les résolveurs récursifs doivent mettre en cache les réponses suivantes provenant de Route 53 :

  NXDOMAIN

  Il n'existe aucun enregistrement de quelque type que ce soit avec le nom spécifié dans la requête DNS, comme example.com. Il n'existe pas non plus d'enregistrements qui sont des enfants du nom spécifié dans la requête DNS, comme zenith.example.com.

  NODATA

  Il existe au moins un enregistrement portant le nom spécifié dans la requête DNS, mais aucun de ces enregistrements n'a le type (A par exemple) spécifié dans la requête DNS.

  Lorsqu'un résolveur DNS met en cache une réponse NXDOMAIN ou NODATA, ce résultat est appelé mise en cache négative.

  La durée de mise en cache négative est la plus courte des valeurs suivantes :

  - Cette valeur est la TTL minimale dans le registre SOA. Dans cet exemple, la valeur est `86400` (un jour)
  - Valeur de la durée de vie (TTL) pour l'enregistrement SOA. La valeur par défaut est de 900 secondes. Pour plus d'informations sur la modification de cette valeur, consultez Modification des enregistrements.

  Lorsque Route 53 répond à des requêtes DNS avec une réponse NXDOMAIN ou NODATA (réponse négative), le tarif pour les requêtes standard vous est facturé. (Consultez « Requêtes »

dans Tarifications Amazon Route 53). Si vous vous inquiétez du coût des réponses négatives, vous pouvez modifier la TTL du registre SOA, la TTL minimale dans le registre SOA (cette valeur), ou les deux. Notez que leur augmentation TTLs, qui s'applique aux réponses négatives pour l'ensemble de la zone hébergée, peut avoir des effets à la fois positifs et négatifs :

- Les résolveurs DNS sur Internet mettent en cache l'inexistence de registres pendant des périodes plus longues, ce qui réduit le nombre de requêtes transférées vers Route 53. Cela réduit les frais Route 53 des requêtes DNS.
- Toutefois, si vous supprimez par erreur un enregistrement valide et que vous le recréez ultérieurement, les résolveurs DNS mettront en cache la réponse négative (cet enregistrement n'existe pas) pendant une période plus longue. Cela allonge le temps pendant lequel vos clients ou utilisateurs ne peuvent pas accéder à la ressource correspondante, comme un serveur web pour acme.example.com.

Pour trouver vos enregistrements SOA dans Route 53

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le panneau de navigation, choisissez Zones hébergées.
3. Sélectionnez le nom lié du domaine pour lequel vous souhaitez afficher les enregistrements.
4. Sur la page Records (Enregistrements), vous pouvez voir tous les enregistrements répertoriés et filtrer les enregistrements pour trouver votre valeur SOA.

Utilisation des zones hébergées privées

Une zone hébergée privée est un conteneur qui contient des informations sur la manière dont vous souhaitez qu'Amazon Route 53 réponde aux requêtes DNS pour un domaine et ses sous-domaines au sein d'un ou de plusieurs domaines VPCs que vous créez avec le service Amazon VPC. Voici comment fonctionnent les zones hébergées privées :

1. Vous créez une zone hébergée privée, comme exemple.com, et spécifiez le VPC que vous souhaitez associer à la zone hébergée. Après avoir créé la zone hébergée, vous pouvez en VPCs associer d'autres.
2. Vous créez des enregistrements dans la zone hébergée qui déterminent la manière dont Route 53 répond aux requêtes DNS pour votre domaine et les sous-domaines au sein de votre et entre vous VPCs. Supposons, par exemple, que vous disposiez d'un serveur de base de données

qui s'exécute sur une EC2 instance du VPC que vous avez associée à votre zone hébergée privée. Vous créez un enregistrement A ou AAAA, par exemple db.exemple.com, et vous indiquez l'adresse IP du serveur de base de données.

Pour plus d'informations sur les enregistrements , consultez la section Utilisation des enregistrements. Pour plus d'informations sur les exigences Amazon VPC inhérentes à l'utilisation de zones hébergées privées, consultez Utilisation des zones hébergées privées dans le Guide de l'utilisateur Amazon VPC.

3. Lorsqu'une application envoie une requête DNS pour db.exemple.com, Route 53 renvoie l'adresse IP correspondante. Pour obtenir une réponse depuis une zone hébergée privée, vous devez également exécuter une EC2 instance dans l'une des zones associées VPCs (ou disposer d'un point de terminaison entrant issu d'une configuration hybride). Si vous essayez d'interroger une zone hébergée privée en dehors de votre configuration hybride VPCs ou de votre configuration hybride, la requête sera résolue de manière récursive sur Internet.
4. L'application utilise l'adresse IP obtenue depuis Route 53 pour établir une connexion avec le serveur de base de données.

Lorsque vous créez une zone hébergée privée, les serveurs de noms suivants sont utilisés :

- ns-0.awsdns-00.com
- ns-512.awsdns-00.net
- ns-1024.awsdns-00.org
- ns-1536.awsdns-00.co.uk

Ces serveurs de noms sont utilisés parce que le protocole DNS exige que chaque zone hébergée possède un ensemble d'enregistrements NS. Ces serveurs de noms sont réservés et ne sont jamais utilisés par les zones hébergées publiques Route 53. Vous pouvez uniquement interroger ces zones via Route 53 Resolver dans un VPC associé à la zone hébergée en utilisant un point de terminaison entrant connecté au point spécifié dans VPCs la zone hébergée privée.

Bien que les serveurs de noms soient visibles sur Internet, Route 53 Resolver ne se connecte pas aux adresses des serveurs de noms. De plus, les informations relatives à la zone hébergée privée ne sont pas renvoyées si vous interrogez directement les serveurs de noms sur Internet. Au lieu de cela, Route 53 Resolver détecte que les requêtes se trouvent dans un espace de noms privé basé sur le VPC et les associations de zones hébergées et utilise une connectivité privée directe pour atteindre les serveurs DNS privés.

> **Note**
>
> Vous pouvez modifier l'enregistrement NS défini dans une zone hébergée privée si vous le souhaitez et la résolution DNS privée fonctionnera toujours. Nous vous déconseillons de le faire, mais si vous le souhaitez, vous devez utiliser des noms de domaine réservés qui ne sont pas utilisés par les serveurs DNS publics.

Vous pouvez utiliser une zone hébergée publique Route 53 pour acheminer le trafic de votre domaine sur Internet. Pour de plus amples informations, veuillez consulter Utilisation de zones hébergées publiques.

Rubriques

- Remarques sur l'utilisation des zones hébergées privées
- Création d'une zone hébergée privée
- Affichage des zones hébergées privées
- Associer davantage VPCs à une zone hébergée privée
- Associer un Amazon VPC et une zone hébergée privée que vous avez créée avec différents comptes AWS
- Dissociation VPCs d'une zone hébergée privée
- Suppression d'une zone hébergée privée
- Autorisations VPC

Remarques sur l'utilisation des zones hébergées privées

Lorsque vous utilisez des zones hébergées privées, notez les informations suivantes.

- Amazon VPC settings
- Route 53 health checks
- Supported routing policies for records in a private hosted zone
- Split-view DNS
- Public and private hosted zones that have overlapping namespaces
- Private hosted zones that have overlapping namespaces
- Private hosted zones and Route 53 Resolver rules

- Delegating responsibility for a subdomain
- Custom DNS servers
- Required IAM permissions

Paramètres Amazon VPC

Pour utiliser les zones hébergées privées, vous devez définir les paramètres Amazon VPC suivants sur `true` :

- `enableDnsHostnames`
- `enableDnsSupport`

Pour plus d'informations, consultez Afficher et mettre à jour les attributs DNS de votre VPC dans le guide de l'utilisateur Amazon VPC.

Surveillances d'états Route 53

Dans une zone hébergée privée, vous pouvez associer les vérifications de santé de Route 53 uniquement aux enregistrements relatifs au basculement, aux réponses à valeurs multiples, à la pondération, à la latence, à la géolocalisation et aux enregistrements de géoproximité. Pour plus d'informations sur l'association de vérifications de l'état à des enregistrements de basculement, consultez Configuration du basculement dans une zone hébergée privée.

Politiques de routage des registres dans une zone hébergée privée prises en charge

Vous pouvez utiliser les stratégies de routage suivantes lors de la création d'enregistrements dans une zone hébergée privée :

- Routage simple
- Routage par basculement
- Multivalue answer routing (Routage de réponse multivaleur)
- Weighted routing (Routage pondéré)
- Routage basé sur la latence
- Routage de géolocalisation
- Routage par géoproximité

La création d'enregistrements dans une zone hébergée privée à l'aide d'autres stratégies de routage de géolocalisation ou de latence n'est pas prise en charge.

DNS vue divisée

Vous pouvez utiliser Route 53 pour configurer un DNS en mode d'affichage fractionné, également connu sous le nom « DNS à horizon fractionné ». Dans le DNS en vue divisée, vous utilisez le même nom de domaine (example.com) pour des utilisations internes (accounting.example.com) et externes, notamment votre site web public (www.example.com). Vous pouvez également vouloir utiliser le même nom de sous-domaine en interne et en externe, mais proposer un contenu différent ou exiger une authentification différente pour les utilisateurs internes et externes.

Pour configurer le DNS en vue divisée, effectuez les opérations suivantes :

1. Créez des zones hébergées publiques et privées ayant le même nom (Le DNS en vue divisée continue à fonctionner si vous utilisez un autre service DNS pour la zone hébergée publique.)
2. Associez un ou plusieurs Amazon VPCs à la zone hébergée privée. Route 53 Resolver utilise la zone hébergée privée pour acheminer les requêtes DNS dans la zone spécifiée VPCs.
3. Créez des enregistrements dans chaque zone hébergée. Les enregistrements de la zone hébergée publique contrôlent la manière dont le trafic Internet est acheminé, tandis que les enregistrements de la zone hébergée privée contrôlent la manière dont le trafic est acheminé sur votre Amazon. VPCs

Si vous devez effectuer la résolution de nom de votre VPC et de vos charges de travail sur site, vous pouvez utiliser Route 53 Resolver. Pour de plus amples informations, veuillez consulter Qu'est-ce que c'est Amazon Route 53 Resolver ?.

Zones hébergées publiques et privées dont les espaces de noms se chevauchent

Si vous disposez de zones hébergées privées et publiques dont les espaces de noms se chevauchent, comme example.com et accounting.example.com, Resolver achemine le trafic en fonction de la correspondance la plus spécifique. Lorsque les utilisateurs sont connectés à une EC2 instance d'un Amazon VPC que vous avez associée à la zone hébergée privée, voici comment Route 53 Resolver gère les requêtes DNS :

1. Resolver évalue si le nom de la zone hébergée privée correspond au nom de domaine de la demande, par exemple, accounting.example.com. Une correspondance se définit de l'une des façons suivantes :
   - Une correspondance identique
   - Le nom de la zone hébergée privée est un parent du nom de domaine de la demande. Supposons par exemple que le nom de domaine de la demande soit :

     seattle.accounting.example.com

Les zones hébergées suivantes correspondent, car elles sont parents de seattle.accounting.example.com :

- accounting.example.com
- example.com

S'il n'existe aucune zone hébergée privée correspondante, Resolver transmet la demande à un résolveur DNS public et votre demande est résolue en tant que requête DNS normale.

2. Si le nom d'une zone hébergée privée correspond au nom de domaine de la demande, une recherche est lancée dans la zone hébergée afin de trouver un enregistrement correspondant au nom de domaine et au type DNS de la demande, par exemple un enregistrement A pour accounting.example.com.

> **Note**
>
> S'il existe une zone hébergée privée correspondante, mais qu'aucun registre ne correspond au nom de domaine ni au type de domaine de la demande, Resolver ne transfère pas la demande à un résolveur DNS public. Au lieu de cela, elle renvoie une réponse NXDOMAIN (domaine non existant) au client.

Zones hébergées privées dont les espaces de noms se chevauchent

Si vous disposez de deux zones hébergées privées ou plus dont les espaces de noms se chevauchent, comme example.com et accounting.example.com, Resolver achemine le trafic en fonction de la correspondance la plus spécifique.

> **Note**
>
> Si vous disposez d'une zone hébergée privée (example.com) et d'une règle Route 53 Resolver qui achemine le trafic vers votre réseau pour le même nom de domaine, la règle Resolver est prioritaire. Consultez Private hosted zones and Route 53 Resolver rules.

Lorsque les utilisateurs sont connectés à une EC2 instance d'un Amazon VPC que vous avez associée à toutes les zones hébergées privées, voici comment Resolver gère les requêtes DNS :

1. Resolver évalue si nom de domaine de la demande, par exemple, accounting.example.com, correspond au nom de l'une des zones hébergées privées.

2. Si aucune zone hébergée ne correspond exactement au nom de domaine dans la demande, Resolver recherche une zone hébergée dont le nom est le parent du nom de domaine dans la demande. Supposons par exemple que le nom de domaine de la demande soit :

   `seattle.accounting.example.com`

   Les zones hébergées suivantes correspondent, car elles sont parents de `seattle.accounting.example.com` :

   - `accounting.example.com`
   - `example.com`

   Resolver choisit `accounting.example.com` car il est plus spécifique que `example.com`.

3. Resolver recherche, dans la zone hébergée `accounting.example.com`, un registre correspondant au nom de domaine et au type DNS de la demande, par exemple, un registre A pour `seattle.accounting.example.com`.

   Si aucun enregistrement ne correspond au nom de domaine et au type dans la demande, Resolver renvoie NXDOMAIN (domaine inexistant) au client.

Zones hébergées privées et règles Route 53 Resolver

Si vous disposez d'une zone hébergée privée (example.com) et d'une règle Resolver qui achemine le trafic vers votre réseau pour le même nom de domaine, la règle Resolver est prioritaire.

Par exemple, supposons que vous ayez la configuration suivante :

- Vous disposez d'une zone hébergée privée appelée example.com et vous l'associez à un VPC.
- Vous créez une règle Route 53 Resolver qui transfère le trafic pour example.com vers votre réseau, et vous associez la règle au même VPC.

Dans cette configuration, la règle Resolver a priorité sur la zone hébergée privée. Les requêtes DNS sont transférées à votre réseau au lieu d'être résolues en fonction des enregistrements de la zone hébergée privée.

Délégation de responsabilité pour un sous-domaine

Vous pouvez désormais créer des enregistrements NS dans une zone hébergée privée pour déléguer la responsabilité d'un sous-domaine. Pour de plus amples informations, veuillez consulter Tutoriel sur les règles de délégation Resolver.

Serveurs DNS personnalisés

Si vous avez configuré des serveurs DNS personnalisés sur des EC2 instances Amazon de votre VPC, vous devez configurer ces serveurs DNS pour acheminer vos requêtes DNS privées vers l'adresse IP des serveurs DNS fournis par Amazon pour votre VPC. Cette adresse IP est l'adresse IP à la base de votre plage réseau VPC, plus le chiffre deux. Par exemple, si la plage d'adresses CIDR pour votre VPC est 10.0.0.0/16, l'adresse IP du serveur DNS est 10.0.0.2.

Si vous souhaitez acheminer des requêtes DNS entre VPCs et votre réseau, vous pouvez utiliser Resolver. Pour de plus amples informations, veuillez consulter Qu'est-ce que c'est Amazon Route 53 Resolver ?.

Autorisations IAM requises

Pour créer des zones hébergées privées, vous devez accorder des autorisations IAM pour les EC2 actions Amazon en plus des autorisations pour les actions Route 53. Pour plus d'informations, consultez la rubrique Actions, ressources et clés de condition pour Route 53 dans la section Référence de l'autorisation de service.

Création d'une zone hébergée privée

Une zone hébergée privée est un conteneur pour les enregistrements d'un domaine que vous hébergez dans un ou plusieurs clouds privés virtuels Amazon (VPCs). Vous créez une zone hébergée pour un domaine (tel que exemple.com), puis vous créez des enregistrements pour indiquer à Amazon Route 53 comment vous souhaitez que le trafic soit acheminé pour ce domaine au sein de votre et entre vous. VPCs

> **Important**
>
> Lorsque vous créez une zone hébergée privée, vous devez lui associer un VPC, et le VPC que vous spécifiez doit avoir été créé en utilisant le même compte que celui que vous utilisez pour créer la zone hébergée. Après avoir créé la zone hébergée, vous pouvez y associer d'autres VPCs zones, notamment celles VPCs que vous avez créées à l'aide d'un autre AWS compte.
> Pour associer VPCs ce que vous avez créé à l'aide d'un compte à une zone hébergée privée que vous avez créée à l'aide d'un autre compte, vous devez autoriser l'association, puis l'établir par programmation. Pour de plus amples informations, veuillez consulter Associer

un Amazon VPC et une zone hébergée privée que vous avez créée avec différents comptes AWS.

Pour plus d'informations sur la création d'une zone hébergée privée à l'aide de l'API Route 53, consultez le document Référence de l'API Amazon Route 53.

Pour créer une zone hébergée privée à l'aide de la console Route 53

1. Pour chaque VPC que vous souhaitez associer à la zone hébergée Route 53, définissez les paramètres VPC suivants sur `true` :

   - `enableDnsHostnames`
   - `enableDnsSupport`

   Pour plus d'informations, consultez Mise à jour du support DNS pour votre VPC dans le Guide de l'utilisateur Amazon VPC.
2. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
3. Si vous débutez avec Route 53, choisissez Get started (Mise en route).

   Si vous utilisez déjà Route 53, choisissez Hosted Zones (Zones hébergées) dans le panneau de navigation.
4. Choisissez Create hosted zone (Créer une zone hébergée).
5. Dans le volet Create private hosted zone (Créer une zone hébergée privée), saisissez un nom de domaine et, éventuellement, un commentaire.

   Pour plus d'informations sur la spécification d'autres caractères que a-z, 0-9 et - (trait d'union), et de noms de domaine internationaux, consultez Format de nom de domaine DNS.
6. Dans la liste Type, choisissez Private hosted zone (Zone hébergée privée).
7. Dans la liste VPC ID, sélectionnez le VPC que vous voulez associer à la zone hébergée.

   > **Note**
   >
   > Si la console affiche le message suivant, vous essayez d'associer une zone hébergée qui utilise le même espace de noms que celui d'une autre zone hébergée au sein du même VPC :

« A conflicting domain is already associated with the given VPC or Delegation Set. » Par exemple, si la zone hébergée A et la zone hébergée B ont le même nom de domaine, comme `example.com`, vous ne pouvez pas associer les deux zones hébergées au même VPC.

8. Choisissez Create hosted zone (Créer une zone hébergée).

Affichage des zones hébergées privées

Vous pouvez utiliser la console Amazon Route 53 pour répertorier toutes les zones hébergées que vous avez créées avec le AWS compte actuel. Pour plus d'informations sur la façon de répertorier les zones hébergées à l'aide de l'API Route 53, consultez ListHostedZonesle manuel Amazon Route 53 API Reference.

Pour répertorier les zones hébergées associées à un AWS compte

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le panneau de navigation, choisissez Zones hébergées.

   La page Zones hébergées affiche automatiquement la liste de toutes les zones hébergées créées à l'aide du AWS compte actuel. La colonne Type indique si une zone hébergée est privée ou publique. Sélectionnez l'en-tête de colonne pour regrouper toutes les zones hébergées privées et toutes les zones hébergées publiques.

Associer davantage VPCs à une zone hébergée privée

Vous pouvez utiliser la console Amazon Route 53 pour en VPCs associer davantage à une zone hébergée privée si vous avez créé la zone hébergée et en VPCs utilisant le même AWS compte.

Important

Si vous souhaitez associer VPCs ce que vous avez créé en utilisant un compte à une zone hébergée privée que vous avez créée à l'aide d'un autre compte, vous devez d'abord autoriser l'association. En outre, vous ne pouvez pas utiliser la AWS console pour autoriser l'association ou pour l' VPCs associer à la zone hébergée. Pour de plus amples informations,

veuillez consulter Associer un Amazon VPC et une zone hébergée privée que vous avez créée avec différents comptes AWS.

Pour plus d'informations sur la manière d' VPCs associer davantage à une zone hébergée privée à l'aide de l'API Route 53, consultez Associer VPCWith HostedZone dans le manuel Amazon Route 53 API Reference.

Pour VPCs associer des zones supplémentaires à une zone hébergée privée à l'aide de la console Route 53

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le panneau de navigation, choisissez Zones hébergées.
3. Cliquez sur le bouton radio correspondant à la zone hébergée privée à laquelle vous souhaitez VPCs associer davantage.
4. Choisissez Modifier.
5. Choisissez Add VPC (Ajouter un VPC).
6. Choisissez la région et l'ID du VPC que vous souhaitez associer à cette zone hébergée.
7. Pour en VPCs associer davantage à cette zone hébergée, répétez les étapes 5 et 6.
8. Sélectionnez Enregistrer les modifications.

Associer un Amazon VPC et une zone hébergée privée que vous avez créée avec différents comptes AWS

Si vous souhaitez associer un VPC que vous avez créé avec un AWS compte à une zone hébergée privée que vous avez créée avec un autre compte, effectuez la procédure suivante :

Pour associer un Amazon VPC et une zone hébergée privée que vous avez créée à différents comptes AWS

1. A l'aide du compte qui a créé la zone hébergée, autorisez l'association du VPC à la zone hébergée privée en utilisant l'une des méthodes suivantes :
   - AWS CLI— Voir create-vpc-association-authorizationdans la référence des AWS CLI commandes

- AWS SDK ou AWS Tools for Windows PowerShell— Consultez la documentation applicable sur la page de AWS documentation
- API Amazon Route 53 — Voir Créer une VPCAssociation autorisation dans le manuel de référence de l'API Amazon Route 53

Remarques :

- Si vous souhaitez associer plusieurs sites VPCs que vous avez créés à un compte à une zone hébergée créée avec un compte différent, vous devez soumettre une demande d'autorisation pour chaque VPC.
- Lorsque vous autorisez l'association, vous devez spécifier l'ID de la zone hébergée, par conséquent, la zone hébergée privée doit déjà exister.
- Vous ne pouvez pas utiliser la console Route 53 pour autoriser l'association d'un VPC à une zone hébergée privée, ni pour effectuer l'association.

2. A l'aide du compte qui a créé le VPC, associez ce VPC à la zone hébergée. Comme pour autoriser l'association, vous pouvez utiliser le AWS SDK, Tools for Windows PowerShell AWS CLI, ou l'API Route 53. Si vous utilisez l'API, utilisez l'VPCWithHostedZoneaction Associer.
3. Recommandé – Supprimez l'autorisation d'associer le VPC à la zone hébergée. La suppression de l'autorisation n'affecte pas l'association, elle vous empêche seulement de réassocier le VPC à la zone hébergée par la suite. Si vous souhaitez réassocier le VPC à la zone hébergée, vous devrez répéter les étapes 1 et 2 de cette procédure.

> **Important**
>
> `ListHostedZonesByVPC`Renvoie les zones hébergées à partir d'un VPC et `GetHostedZone` l'API renvoie les zones VPCs associées à la zone hébergée. Ils APIs ne prennent en compte que l'association entre la zone hébergée et le VPC créée par l'`AssociateVPCWithHostedZone`API ou lors de la création de la zone hébergée privée. Si vous souhaitez obtenir la liste complète des associations de zones hébergées à un VPC, appelez également. ListProfileResourceAssociations

> **Note**
>
> Pour connaître le nombre maximal d'autorisations que vous pouvez créer, consultez Quotas applicables aux entités.

Dissociation VPCs d'une zone hébergée privée

Vous pouvez utiliser la console Amazon Route 53 pour vous VPCs dissocier d'une zone hébergée privée. Ce faisant, Route 53 cesse d'acheminer le trafic à l'aide de registres dans la zone hébergée pour les requêtes DNS qui proviennent du VPC. Par exemple, si la zone hébergée example.com est associée à un VPC et que vous dissociez la zone hébergée de ce VPC, Route 53 cesse de résoudre les requêtes DNS pour example.com ou tout autre registre de la zone hébergée example.com.

> **Note**
>
> Vous ne pouvez pas dissocier le dernier VPC d'une zone hébergée privée. Si vous souhaitez dissocier ce VPC, vous devez d'abord associer un autre VPC à la zone hébergée.

Pour se dissocier VPCs d'une zone hébergée privée

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le panneau de navigation, choisissez Zones hébergées.
3. Cliquez sur le bouton radio correspondant à la zone hébergée privée dont vous souhaitez dissocier une ou plusieurs VPCs zones.
4. Choisissez Modifier.
5. Choisissez Remove VPC (Supprimer le VPC) en regard du VPC que vous souhaitez dissocier de cette zone hébergée.
6. Sélectionnez Enregistrer les modifications.

Suppression d'une zone hébergée privée

Cette section explique comment supprimer une zone hébergée privée à l'aide de la console Amazon Route 53.

Vous pouvez supprimer une zone hébergée privée uniquement s'il n'existe aucun autre enregistrement que les enregistrements SOA et NS par défaut. Si votre zone hébergée contient d'autres enregistrements, vous devez les supprimer avant de pouvoir supprimer votre zone hébergée. Cela vous empêche de supprimer accidentellement une zone hébergée qui contient encore des enregistrements.

Rubriques

- Suppression des zones hébergées privées qui étaient créées par un autre service
- Utilisation de la console Route 53 pour supprimer une zone hébergée privée

Suppression des zones hébergées privées qui étaient créées par un autre service

Si une zone hébergée privée a été créée par un autre service, vous ne pouvez pas la supprimer à l'aide de la console Route 53. Au lieu de cela, vous devez utiliser le processus de l'autre service :

- AWS Cloud Map— Pour supprimer une zone hébergée AWS Cloud Map créée lorsque vous avez créé un espace de noms DNS privé, supprimez l'espace de noms. AWS Cloud Map supprime automatiquement la zone hébergée. Pour plus d'informations, consultez Suppression des espaces de noms dans le Guide du développeur AWS Cloud Map .
- Découverte du service Amazon Elastic Container Service (Amazon ECS) – Pour supprimer une zone hébergée privée créée par Amazon ECS lorsque vous avez créé un service à l'aide de la découverte de service, supprimez les services Amazon ECS qui utilisent l'espace de noms, et supprimez l'espace de noms. Pour plus d'informations, consultez Suppression d'un service dans le Guide du développeur Amazon Elastic Container Service.

Utilisation de la console Route 53 pour supprimer une zone hébergée privée

Pour utiliser la console Route 53 afin de supprimer une zone hébergée privée, exécutez la procédure suivante.

Pour supprimer une zone hébergée privée à l'aide de la console Route 53

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Vérifiez que la zone hébergée que vous souhaitez supprimer contient uniquement un enregistrement NS et un enregistrement SOA. Si elle contient d'autres enregistrements, supprimez-les :

   a. Choisissez le nom de la zone hébergée que vous souhaitez supprimer.

   b. Sur la page Record (Registre), si la liste des registres inclut des registres pour lesquels la valeur de la colonne Type n'est ni NS ni SOA, choisissez la ligne et choisissez Delete (Supprimer).

      Pour sélectionner plusieurs enregistrements consécutifs, appuyez sur la touche MAJ et maintenez-la enfoncée, puis sélectionnez la dernière ligne. Pour sélectionner plusieurs enregistrements non consécutifs, appuyez sur la touche Ctrl et maintenez-la enfoncée, puis sélectionnez les autres lignes.
3. Sur la page Hosted Zones, choisissez la ligne de la zone hébergée que vous souhaitez supprimer.
4. Sélectionnez Delete (Supprimer).
5. Saisissez la clé de confirmation et choisissez Delete (Supprimer).

Autorisations VPC

Les autorisations VPC utilisent les conditions de politique de gestion des identités et des accès (IAM) qui vous permettent de définir des autorisations granulaires VPCs lorsque vous utilisez Associer VPCWithHostedZone, Disassocier, Créer une VPCAssociation autorisation VPCFrom HostedZone VPCAssociation, Supprimer une autorisation et VPC. CreateHostedZoneListHostedZonesBy APIs

Avec la condition de politique IAM`route53:VPCs`, vous pouvez accorder des droits administratifs granulaires à d'autres AWS utilisateurs. Cela vous permet d'accorder à quelqu'un l'autorisation d'associer une zone hébergée à, de dissocier une zone hébergée de, de créer une autorisation d'association VPC pour, de supprimer l'autorisation d'association VPC pour, de créer une zone hébergée avec ou de répertorier des zones hébergées pour :

- Un seul VPC.
- N'importe VPCs lequel au sein de la même région.

- Multiple VPCs.

Pour plus d'informations sur les autorisations VPC, consultez. Utilisation de conditions de politique IAM pour un contrôle d'accès précis

Pour savoir comment authentifier AWS les utilisateurs, consultez Authentification par des identités et pour savoir comment contrôler l'accès aux ressources Route 53, voirContrôle d'accès.

Migration d'une zone hébergée vers un autre compte AWS

Lors de la migration d'une zone hébergée vers une autre Compte AWS, suivez ces étapes recommandées.

Ces étapes sont particulièrement adaptées aux zones hébergées dont les enregistrements ne sont pas fréquemment modifiés. Pour les zones hébergées avec des mises à jour fréquentes des enregistrements, tenez compte des points suivants :

- Ne mettez à jour aucun enregistrement de ressource pendant la migration.
- Publiez les modifications des enregistrements de ressources dans les anciennes et les nouvelles zones hébergées après le transfert de la délégation.

Prérequis

Installez ou mettez à niveau AWS CLI :

Pour plus d'informations sur le téléchargement, l'installation et la configuration du AWS CLI, consultez le guide de AWS Command Line Interface l'utilisateur.

> **Note**
>
> Configurez l'interface de ligne de commande afin de pouvoir l'utiliser lorsque vous utilisez à la fois le compte qui a créé la zone hébergée et le compte vers lequel vous migrez la zone hébergée. Pour plus d'informations, consultez Configure (Configuration) dans le Guide de l'utilisateur AWS Command Line Interface .

Si vous utilisez déjà le AWS CLI, nous vous recommandons de passer à la dernière version de la CLI afin que les commandes de la CLI prennent en charge les dernières fonctionnalités de Route 53.

Rubriques

- Étape 1 : Préparation à la migration
- Étape 2 : Créer la nouvelle zone hébergée
- Étape 3 : (Facultatif) Migrer les bilans de santé
- Étape 4 : Migrer les enregistrements de l'ancienne zone hébergée vers la nouvelle zone hébergée
- Étape 5 : Comparez les enregistrements de l'ancienne et de la nouvelle zone hébergée
- Étape 6 : Mettre à jour l'enregistrement du domaine pour utiliser des serveurs de noms pour la nouvelle zone hébergée
- Étape 7 : Remettez le TTL de l'enregistrement NS à une valeur plus élevée
- Étape 8 : réactivez la signature DNSSEC et établissez la chaîne de confiance (si nécessaire)
- Étape 9 : (Facultatif) supprimer l'ancienne zone hébergée

Étape 1 : Préparation à la migration

Les étapes de préparation vous aident à minimiser les risques associés à la migration d'une zone hébergée.

1. Surveillez la disponibilité des zones

Vous pouvez contrôler la zone de disponibilité des noms de domaine. Cela peut vous aider à résoudre les problèmes susceptibles d'entraîner l'annulation de la migration. Vous pouvez surveiller les noms de domaine qui génèrent le plus de trafic en utilisant CloudWatch ou en enregistrant les requêtes. Pour plus d'informations sur la configuration de la journalisation des requêtes, consultez Surveillance d'Amazon Route 53.

Vous pouvez effectuer la surveillance via un script shell ou via un service tiers. Cela ne devrait toutefois pas être le seul signal permettant de déterminer si une annulation est nécessaire, car vous pourriez également obtenir des commentaires de la part de vos clients si un domaine n'est pas disponible.

2. Réduisez le paramètre TTL

Le paramètre de durée de vie d'un enregistrement spécifie la durée pendant laquelle vous voulez que les résolveurs DNS mettent en cache l'enregistrement et utilisent les informations mises en cache. À la date d'expiration, un résolveur envoie une autre requête au fournisseur de services DNS d'un domaine afin d'obtenir les informations les plus récentes.

Le paramètre de durée de vie d'un enregistrement NS est de 172 800 secondes, soit deux jours. L'enregistrement NS répertorie les serveurs de noms que le système de noms de domaine (DNS) peut utiliser pour obtenir des informations sur la manière d'acheminer le trafic pour votre domaine. La réduction du TTL pour l'enregistrement NS, à la fois avec votre fournisseur de services DNS actuel et avec Route 53, réduit le temps d'arrêt de votre domaine si vous découvrez un problème lors de la migration du DNS vers Route 53. Si vous ne réduisez pas la durée de vie, votre domaine risque d'être indisponible sur Internet pendant deux jours en cas de problème.

Pour abaisser le TTL

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Choisissez Zones hébergées dans le volet de navigation.
3. Choisissez le nom de la zone hébergée.
4. Choisissez l'enregistrement NS, puis dans le volet Détails de l'enregistrement, sélectionnez Modifier l'enregistrement.
5. Modifiez la valeur du champ TTL (Seconds) (Durée de vie (secondes)). Nous vous recommandons de spécifier une valeur comprise entre 60 secondes et 900 secondes (15 minutes).
6. Choisissez Enregistrer.

3. Supprimer l'enregistrement DS de la zone parent (si le protocole DNSSEC est configuré)

Si vous avez configuré DNSSEC pour votre domaine, supprimez le registre Delegation Signer (DS) de la zone parent avant de migrer votre domaine vers Route 53.

Si la zone parent est hébergée via Route 53, consultez Suppression de clés publiques pour un domaine pour plus d'informations. Si la zone parent est hébergée sur un autre bureau d'enregistrement, contactez-le pour supprimer l'enregistrement DS.

Route 53 ne prend actuellement pas en charge la migration du paramètre DNSSEC. Vous devez donc désactiver la validation DNSSEC effectuée sur votre domaine avant la migration en supprimant l'enregistrement DS de la zone parent. Après la migration, vous pouvez réactiver la validation DNSSEC en configurant le DNSSEC sur la nouvelle zone hébergée et en ajoutant l'enregistrement DS correspondant à la zone parent.

4. Assurez-vous qu'aucune autre opération n'est en cours basée sur la zone hébergée en cours de migration

Certaines opérations s'appuieront sur la résolution DNS dans la zone hébergée en cours de migration. Par exemple, le processus de renouvellement du certificat TLS/SSL peut nécessiter des modifications d'enregistrement DNS et le fournisseur essaiera de résoudre l'enregistrement DNS comme méthode de validation. Avant la migration, vous devez vous assurer qu'aucune autre opération n'est en cours, afin d'éviter tout impact inattendu lié à la migration de la zone hébergée.

Étape 2 : Créer la nouvelle zone hébergée

Créez la nouvelle zone hébergée dans le compte vers lequel vous souhaitez migrer la zone hébergée.

Choisissez l'onglet pour les instructions relatives à la console AWS CLI ou à la console.

- INTERFACE DE LIGNE DE COMMANDE (CLI)
- Console

CLI

Entrez la commande suivante :

```
aws route53 create-hosted-zone \
            --name $hosted_zone_name \
            --caller-reference $unique_string
```

Pour de plus amples informations, veuillez consulter create-hosted-zone.

Console

Pour créer une nouvelle zone hébergée à l'aide d'un autre compte

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.

   Connectez-vous avec les informations d'identification du compte vers lequel vous souhaitez migrer la zone hébergée.
2. Créez une zone hébergée. Pour de plus amples informations, veuillez consulter Création d'une zone hébergée publique.
3. Notez l'ID de la zone hébergée. Dans certains cas, vous en aurez besoin ultérieurement dans le processus.

4. Déconnectez-vous de la console Route 53.

Réduisez également le TTL NS dans la nouvelle zone, comme dans le cas du paramètre TTL inférieur lors de la préparation, étape 1, abaissez le paramètre TTL.

Étape 3 : (Facultatif) Migrer les bilans de santé

Vous pouvez associer les enregistrements DNS du nouveau compte aux contrôles de santé de Route 53 effectués à partir du compte à partir duquel vous effectuez la migration. Pour migrer un bilan de santé Route 53, vous devez créer de nouveaux bilans de santé dans votre nouveau compte avec la même configuration que les bilans existants. Pour de plus amples informations, veuillez consulter Création de bilans de santé pour Amazon Route 53 .

Étape 4 : Migrer les enregistrements de l'ancienne zone hébergée vers la nouvelle zone hébergée

Vous pouvez migrer des enregistrements d'un document Compte AWS à un autre à l'aide de la console ou du AWS CLI

Console

Si votre zone ne contient que quelques enregistrements, vous pouvez envisager d'utiliser la console Route 53 pour répertorier les enregistrements de votre ancienne zone, les noter et les créer dans la nouvelle zone. Si vous avez migré le bilan de santéÉtape 3 : (Facultatif) Migrer les bilans de santé, lorsque vous créez les enregistrements dans la nouvelle zone hébergée, vous devez spécifier le nouvel identifiant du bilan de santé. Pour plus d’informations, consultez les rubriques suivantes :

- Liste des enregistrements
- Création d'enregistrements à l'aide de la console Amazon Route 53
- Configuration du basculement DNS

Vous devez également baisser le TTL NS dans la nouvelle zone, de la même manière que le paramètre Lower TTL défini à l'étape 1.

Migrer les enregistrements par programmation

Si votre zone contient un grand nombre d'enregistrements, vous pouvez envisager d'exporter les enregistrements que vous souhaitez migrer vers un fichier, de modifier le fichier, puis d'utiliser

le fichier modifié pour créer des enregistrements dans la nouvelle zone hébergée. La procédure suivante utilisera AWS CLI les commandes comme référence, il existe également des outils tiers à cet effet.

1. Exécutez la commande suivante :

```
aws route53 list-resource-record-sets --hosted-zone-id hosted-zone-id > path-to-output-file
```

   Remarques :

   - Pour*hosted-zone-id*, spécifiez l'ID de la zone hébergée que vous avez obtenu à l'étape 2 de cette procédure.
   - Pour*path-to-output-file*, spécifiez le chemin du répertoire et le nom de fichier dans lesquels vous souhaitez enregistrer la sortie.
   - Le caractère > envoie la sortie dans le fichier spécifié.
   - Gère AWS CLI automatiquement la pagination pour les zones hébergées contenant plus de 100 enregistrements. Pour plus d'informations, consultez la section Utilisation des options de pagination de l'interface de ligne de AWS commande dans le Guide de l'AWS Command Line Interface utilisateur.

     Si vous utilisez une autre méthode programmatique pour répertorier les enregistrements, comme l'un des AWS SDKs, vous pouvez obtenir un maximum de 100 enregistrements par page de résultats. Si la zone hébergée contient plus de 100 enregistrements, vous devez soumettre plusieurs demandes pour répertorier tous les enregistrements.

   Faites une copie de cette sortie. Après avoir créé des enregistrements dans la nouvelle zone hébergée, nous vous recommandons d'exécuter la AWS CLI `list-resource-record-sets` commande sur la nouvelle zone hébergée et de comparer les deux sorties pour vous assurer que tous les enregistrements ont été créés.

2. Modifiez les enregistrements que vous souhaitez migrer.

   Le format du fichier que vous avez créé dans la procédure précédente est proche du format requis par la AWS CLI `change-resource-record-sets` commande que vous utilisez pour créer des enregistrements dans la nouvelle zone hébergée. Toutefois, le fichier nécessite certaines modifications. Vous devez appliquer certaines des modifications à chaque

enregistrement. Vous pouvez effectuer ces modifications à l'aide de la fonction de recherche et de remplacement dans un éditeur de texte.

Ouvrez une copie du fichier que vous avez créé à l'étape 1 de cette procédure qui contient les enregistrements que vous souhaitez migrer, et apportez les modifications suivantes :

- Remplacez l' ResourceRecordSets élément en haut du fichier par un `Changes` élément.
- Facultatif : ajoutez un `Comment` élément.
- Supprimez les lignes relatives aux enregistrements NS et SOA du nom de la zone hébergée. La nouvelle zone hébergée possède déjà ces enregistrements.
- Pour chaque enregistrement, ajoutez un élément `Action` et un `ResourceRecordSets` élément, ajoutez des crochets ouvrants et fermants (`{ }`) selon les besoins pour que le code JSON soit valide.

  > **Note**
  >
  > Vous pouvez utiliser un validateur JSON pour vérifier que toutes les accolades et tous les crochets sont correctement placés. Pour trouver un validateur JSON en ligne, recherchez « validateur JSON » dans votre navigateur.

- Si la zone hébergée contient tous les alias qui font référence à d'autres enregistrements dans la même zone hébergée, apportez les modifications suivantes :
  - Remplacez l'ID de la zone hébergée par l'ID de la nouvelle zone hébergée.

    > **Important**
    >
    > Si l'enregistrement d'alias pointe vers une autre ressource, par exemple un équilibreur de charge, ne remplacez pas l'ID de zone hébergée par l'ID de zone hébergée du domaine. Si vous modifiez accidentellement l'ID de zone hébergée, rétablissez l'ID de zone hébergée en identifiant de zone hébergée de la ressource elle-même, et non en identifiant de zone hébergée du domaine. L'ID de zone hébergée par la ressource se trouve dans la AWS console où la ressource a été créée.

  - Déplacez les registres d'alias au bas du fichier. Route 53 doit créer le registre auquel un registre d'alias fait référence avant de pouvoir créer le registre d'alias.

> **Important**
>
> Si un ou plusieurs enregistrements d'alias font référence à d'autres enregistrements d'alias, les enregistrements qui sont la cible de l'alias doivent apparaître dans le fichier avant les enregistrements d'alias qui font référence. Par exemple, si `alias.example.com` est la cible de l'alias pour `alias.alias.example.com`, `alias.example.com` doit apparaître en premier dans le fichier.

- Supprimez les enregistrements d'alias qui acheminent le trafic vers une instance de stratégie de trafic. Notez les enregistrements afin de pouvoir les recréer ultérieurement.

- Si vous avez migré les bilans de santéÉtape 3 : (Facultatif) Migrer les bilans de santé, modifiez les enregistrements pour les associer au nouveau bilan de santé. IDs

L'exemple suivant montre la version modifiée d'enregistrements pour une zone hébergée pour example.com. Le texte en rouge et en italique est nouveau :

```
{
    "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. Divisez les gros fichiers en fichiers plus petits

   Si vous avez un grand nombre d'enregistrements ou si vous avez des enregistrements comportant de nombreuses valeurs (par exemple, un grand nombre d'adresses IP), vous pouvez avoir besoin de fractionner le fichier en fichiers plus petits. Les valeurs maximales sont les suivantes :

   - Chaque fichier peut contenir 1 000 enregistrements maximum.
   - La longueur combinée maximale des valeurs de tous les éléments `Value` est de 32 000 octets.

4. Créez des enregistrements dans la nouvelle zone hébergée

   Entrez la CLI suivante :

```
aws route53 change-resource-record-sets \
            --hosted-zone-id new-hosted-zone-id \
            --change-batch file://path-to-file-that-contains-records
```

   Indiquez l'une des valeurs suivantes :

   - Pour*new-hosted-zone-id*, spécifiez l'ID de la nouvelle zone hébergée.
   - Pour*path-to-file-that-contains-records*, spécifiez le chemin du répertoire et le nom de fichier que vous avez modifiés au cours des étapes précédentes.

Si vous avez supprimé des registres d'alias qui acheminent le trafic vers une instance de politique de trafic, recréez-les à l'aide de la console Route 53. Pour de plus amples informations, veuillez consulter Création d'enregistrements à l'aide de la console Amazon Route 53.

Étape 5 : Comparez les enregistrements de l'ancienne et de la nouvelle zone hébergée

Pour confirmer que vous avez bien créé tous vos enregistrements dans la nouvelle zone hébergée, entrez la commande CLI suivante pour répertorier les enregistrements de la nouvelle zone hébergée et comparez le résultat avec la liste des enregistrements de l'ancienne zone hébergée.

```
aws route53 list-resource-record-sets \
            --hosted-zone-id new-hosted-zone-id \
            --output json > path-to-output-file
```

Indiquez l'une des valeurs suivantes :

- Pour*new-hosted-zone-id*, spécifiez l'ID de la nouvelle zone hébergée.
- Pour*path-to-output-file*, spécifiez le chemin du répertoire et le nom de fichier dans lesquels vous souhaitez enregistrer la sortie. Utilisez un nom de fichier différent de celui que vous avez utilisé à l'étape 4.

  Le caractère > envoie la sortie dans le fichier spécifié.

Comparez le résultat avec le résultat de l'étape 4. Hormis les valeurs des enregistrements NS et SOA et les modifications que vous avez apportées à l'étape 4 (telles que des zones hébergées IDs ou des noms de domaine différents), les deux sorties doivent être identiques.

Si les enregistrements de la nouvelle zone hébergée ne correspondent pas à ceux de l'ancienne zone hébergée, effectuez l'une des opérations suivantes :

- Apportez des corrections mineures à l'aide de la console Route 53. Pour de plus amples informations, veuillez consulter Modification des enregistrements.
- Supprimez tous les enregistrements sauf les enregistrements NS et SOA de la nouvelle zone hébergée et répétez la procédure de l'étape 4.

Étape 6 : Mettre à jour l'enregistrement du domaine pour utiliser des serveurs de noms pour la nouvelle zone hébergée

Lorsque vous avez terminé de migrer les enregistrements vers la nouvelle zone hébergée, modifiez les serveurs de noms pour l'enregistrement du domaine afin qu'ils utilisent les serveurs de noms de la nouvelle zone hébergée. Pour plus d'informations, consultez Faire d'Amazon Route 53 le service DNS d'un domaine existant.

Si votre zone hébergée est utilisée, par exemple, si vos utilisateurs utilisent le nom de domaine pour accéder à un site Web ou à une application Web, vous devez continuer à surveiller le trafic et la disponibilité de la zone hébergée, y compris le trafic du site Web ou des applications, le courrier électronique, etc.

- Si le trafic ralentit ou s'arrête, remplacez le service de noms pour l'enregistrement du domaine par les anciens serveurs de noms de l'ancienne zone hébergée. Déterminez ce qui s'est mal passé.
- Si le trafic n'est pas affecté, passez à l'étape suivante.

Étape 7 : Remettez le TTL de l'enregistrement NS à une valeur plus élevée

Dans la nouvelle zone hébergée, remplacez le TTL de l'enregistrement NS par une valeur plus classique, par exemple 172 800 secondes (deux jours). Cette étape permet d'améliorer la latence pour vos utilisateurs car ils n'auront plus besoin d'attendre aussi souvent que les résolveurs DNS envoient une requête pour les serveurs de noms de votre domaine.

Pour modifier le TTL

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Choisissez Zones hébergées dans le volet de navigation.
3. Choisissez le nom de la zone hébergée.
4. Choisissez l'enregistrement NS, puis dans le volet Détails de l'enregistrement, sélectionnez Modifier l'enregistrement.
5. Modifiez la valeur du TTL (secondes) par le nombre de secondes pendant lesquelles vous souhaitez que les résolveurs DNS mettent en cache les noms des serveurs de noms de votre domaine. Nous vous recommandons une valeur de 172 800 secondes.
6. Choisissez Enregistrer.

Étape 8 : réactivez la signature DNSSEC et établissez la chaîne de confiance (si nécessaire)

Vous pouvez réactiver la signature DNSSEC en deux étapes :

1. Activez la signature DNSSEC pour Route 53 et demandez à Route 53 de créer une clé de signature (KSK) basée sur une clé d'entrée gérée par le client. AWS Key Management Service
2. Créez une chaîne de confiance pour la zone hébergée en ajoutant un enregistrement de signature de délégation (DS) à la zone parent, afin que les réponses DNS puissent être authentifiées à l'aide de signatures cryptographiques fiables.

Pour obtenir des instructions, veuillez consulter Activation de la signature DNSSEC et établissement d'une chaîne d'approbation.

Étape 9 : (Facultatif) supprimer l'ancienne zone hébergée

Lorsque vous êtes sûr de ne plus avoir besoin de l'ancienne zone hébergée, vous pouvez éventuellement la supprimer. Pour obtenir des instructions, veuillez consulter Suppression d'une zone hébergée publique.

> **Important**
>
> Ne supprimez pas l'ancienne zone hébergée ou tous les enregistrements de cette zone hébergée pendant au moins 48 heures après avoir mis à jour l'enregistrement de domaine pour utiliser les serveurs de noms de la nouvelle zone hébergée. Si vous supprimez l'ancienne zone hébergée avant que les résolveurs DNS ne cessent d'utiliser les enregistrements dans cette zone hébergée, votre domaine peut être indisponible sur Internet jusqu'à ce que les résolveurs commencent à utiliser la nouvelle zone hébergée.

Utilisation des enregistrements

Une fois que vous avez créé une zone hébergée pour votre domaine, par exemple, example.com, vous créez des enregistrements pour indiquer au système de noms de domaine (DNS) la façon dont le trafic doit être acheminé pour ce domaine.

Par exemple, vous pouvez créer des enregistrements entraînant le comportement DNS suivant :

- Achemine le trafic Internet d'example.com vers l'adresse IP d'un hôte de votre centre de données.

- Achemine l'e-mail de ce domaine (ichiro@example.com) vers un serveur de messagerie (mail.example.com).
- Achemine le trafic d'un sous-domaine appelé operations.tokyo.example.com vers l'adresse IP d'un autre hôte.

Chaque enregistrement inclut le nom d'un domaine ou d'un sous-domaine, un type d'enregistrement (par exemple, un enregistrement avec un type d'e-mail de routage MX) et d'autres informations applicables au type de l'enregistrement (pour les enregistrements MX, le nom d'hôte d'un ou de plusieurs serveurs de messagerie et une priorité pour chaque serveur). Pour plus d'informations sur les différents types d'enregistrement, consultez Types d'enregistrements DNS pris en charge.

Le nom de chaque enregistrement dans une zone hébergée doit se terminer par le nom de la zone hébergée. Par exemple, la zone hébergée example.com peut contenir des enregistrements pour les sous-domaines www.example.com et accounting.tokyo.example.com, mais ne peut pas contenir d'enregistrements pour un sous-domaine www.example.ca.

> **Note**
>
> Pour créer des enregistrements pour des configurations de routage complexes, vous pouvez également utiliser l'éditeur visuel Traffic Flow et enregistrer la configuration en tant que politique de trafic. Vous pouvez ensuite associer la stratégie de trafic à un ou plusieurs noms de domaine (par exemple, example.com) ou noms de sous-domaine (par exemple, www.example.com), dans la même zone hébergée ou dans plusieurs zones hébergées. En outre, vous pouvez restaurer les mises à jour si la nouvelle configuration ne fonctionne pas comme vous l'aviez prévu. Pour de plus amples informations, veuillez consulter Utiliser Traffic Flow pour acheminer le trafic DNS.

Amazon Route 53 ne facture pas les enregistrements que vous ajoutez à une zone hébergée. Pour plus d'informations sur le nombre maximum d'enregistrements que vous pouvez créer dans une zone hébergée, consultez Quotas.

Rubriques

- Sélection d'une stratégie de routage
- Choix entre des enregistrements avec ou sans alias
- Types d'enregistrements DNS pris en charge
- Création d'enregistrements à l'aide de la console Amazon Route 53

- Autorisations relatives aux ensembles d'enregistrements
- Valeurs à spécifier lorsque vous créez ou modifiez des enregistrements Amazon Route 53
- Création d'enregistrements par importation d'un fichier de zone
- Modification des enregistrements
- Suppression d'enregistrements
- Liste des enregistrements

Sélection d'une stratégie de routage

Lorsque vous créez un enregistrement, vous choisissez une stratégie de routage, qui détermine la façon dont Amazon Route 53 répond aux requêtes :

- Simple routing policy (Stratégie de routage simple) : utilisez une stratégie de routage simple quand vous disposez d'une seule ressource qui exécute une fonction donnée pour votre domaine, comme, par exemple, un serveur web qui diffuse le contenu du site web example.com. Vous pouvez utiliser le routage simple pour créer des enregistrements dans une zone hébergée privée.
- Failover routing policy (Stratégie de routage par basculement) : utilisez une stratégie de routage par basculement pour configurer le basculement actif-passif. Vous pouvez utiliser le routage par basculement pour créer des enregistrements dans une zone hébergée privée.
- Stratégie de routage de géolocalisation : utilisez la stratégie de routage de géolocalisation lorsque vous souhaitez acheminer le trafic en fonction de l'emplacement de vos utilisateurs. Vous pouvez utiliser le routage de géolocalisation pour créer des enregistrements dans une zone hébergée privée.
- Stratégie de routage par proximité géographique : utilisez cette stratégie lorsque vous souhaitez acheminer du trafic en fonction de l'emplacement de vos ressources et, éventuellement, détourner le trafic de vos ressources à un emplacement donné vers les ressources d'un autre emplacement. Vous pouvez utiliser le routage de géoproximité pour créer des enregistrements dans une zone hébergée privée.
- Politique de routage en cas de latence : à utiliser lorsque vous disposez de plusieurs ressources Régions AWS et que vous souhaitez acheminer le trafic vers la région offrant la meilleure latence. Vous pouvez utiliser le routage avec latence pour créer des enregistrements dans une zone hébergée privée.
- IP-based routing policy (Politique de routage basée sur IP) – utilisez la politique de routage basée sur IP lorsque vous voulez acheminer le trafic en fonction de l'emplacement de vos utilisateurs, et que vous disposez des adresses IP d'où provient le trafic.

- Multivalue answer routing policy (Stratégie de routage de réponse multivaleur) : utilisez la stratégie de routage de réponse multivaleur lorsque vous souhaitez que Route 53 réponde aux requêtes DNS avec jusqu'à huit enregistrements sains sélectionnés de manière aléatoire. Vous pouvez utiliser le routage de réponses à plusieurs valeurs pour créer des enregistrements dans une zone hébergée privée.
- Weighted routing policy (Stratégie de routage pondéré) : utilisez la stratégie de routage pondéré pour acheminer le trafic vers plusieurs ressources selon les proportions que vous spécifiez. Vous pouvez utiliser le routage pondéré pour créer des enregistrements dans une zone hébergée privée.

Rubriques

- Routage simple
- Routage par basculement
- Routage de géolocalisation
- Routage par géoproximité
- Routage basé sur la latence
- Routage basé sur IP
- Multivalue answer routing (Routage de réponse multivaleur)
- Weighted routing (Routage pondéré)
- Comment Amazon Route 53 utilise EDNS0 pour estimer l'emplacement d'un utilisateur

Routage simple

Le routage simple vous permet de configurer des enregistrements DNS standard sans routage Route 53 spécial, comme un routage pondéré ou de latence. Avec le routage simple, vous acheminez généralement le trafic vers une seule ressource, par exemple, un serveur web pour votre site web.

Vous pouvez utiliser la stratégie de routage simple pour créer des enregistrements dans une zone hébergée privée.

Si vous choisissez la stratégie de routage simple dans la console Route 53, vous ne pouvez pas créer plusieurs enregistrements ayant le même nom et le même type, mais vous pouvez spécifier plusieurs valeurs dans le même enregistrement, par exemple plusieurs adresses IP. (Si vous choisissez la politique de routage simple pour un enregistrement d'alias, vous ne pouvez spécifier qu'une seule AWS ressource ou un seul enregistrement dans la zone hébergée actuelle.) Si vous

spécifiez plusieurs valeurs dans un enregistrement, Route 53 renvoie toutes les valeurs au résolveur récursif dans un ordre aléatoire, puis le résolveur renvoie les valeurs au client (comme un navigateur web) qui a envoyé la requête DNS. Le client sélectionne ensuite une valeur et renvoie la requête. Avec une politique de routage simple, même si vous pouvez spécifier plusieurs adresses IP, aucune surveillance de l'état n'a lieu pour ces adresses IP.

Pour plus d'informations sur les valeurs que vous spécifiez lorsque vous utilisez la stratégie de routage simple pour créer des enregistrements, consultez les rubriques suivantes :

- Valeurs spécifiques aux enregistrements simples
- Valeurs spécifiques aux enregistrements d'alias simples
- Valeurs communes à toutes les politiques de routage
- Valeurs communes aux enregistrements d'alias pour toutes les politiques de routage

Routage par basculement

Le routage par basculement vous permet d'acheminer le trafic vers une ressource lorsqu'elle est saine ou vers une autre ressource si la première ressource n'est pas saine. L'enregistrement principal et l'enregistrement secondaire peuvent acheminer le trafic de différents types d'éléments, d'un compartiment Amazon S3 configuré comme site web à une arborescence complexe d'enregistrements. Pour de plus amples informations, veuillez consulter Basculement actif-passif.

Vous pouvez utiliser la stratégie de routage de basculement pour créer des enregistrements dans une zone hébergée privée.

Pour plus d'informations sur les valeurs que vous spécifiez lorsque vous utilisez la stratégie de routage de basculement pour créer des enregistrements, consultez les rubriques suivantes :

- Valeurs spécifiques aux enregistrements de basculement
- Valeurs spécifiques aux enregistrements d'alias de basculement
- Valeurs communes à toutes les politiques de routage
- Valeurs communes aux enregistrements d'alias pour toutes les politiques de routage

Routage de géolocalisation

Le routage de géolocalisation vous permet de choisir les ressources qui servent le trafic en fonction de la localisation géographique de vos utilisateurs, c'est-à-dire de l'emplacement d'où proviennent

les requêtes DNS. Par exemple, vous souhaitez peut-être que toutes les requêtes d'Europe soient acheminées vers l'équilibreur de charge Elastic Load Balancing dans la région de Francfort.

Quand vous utilisez le routage de géolocalisation, vous pouvez localiser votre contenu et présenter tout ou partie de votre site web dans la langue de vos utilisateurs. Vous pouvez aussi utiliser le routage de géolocalisation pour limiter la distribution de contenu aux seuls emplacements dans lesquels vous avez des droits de distribution. Une autre utilisation possible consiste à équilibrer la charge entre les points de terminaison de easy-to-manage manière prévisible, afin que chaque emplacement utilisateur soit systématiquement acheminé vers le même point de terminaison.

Vous pouvez spécifier des emplacements géographiques par continent, par pays ou par état des États-Unis. Si vous créez des enregistrements distincts pour des régions géographiques qui se chevauchent (par exemple, un pour l'Amérique du Nord et un autre pour le Canada), la région géographique la plus petite est prioritaire. Cela vous permet d'acheminer des requêtes concernant un continent vers une ressource et celles concernant des pays sélectionnés sur ce continent vers une autre ressource. (Pour obtenir la liste des pays de chaque continent, consultez Emplacement.)

La géolocalisation se base sur le mappage d'adresses IP à des emplacements. Cependant, certaines adresses IP ne sont pas mappées à des emplacements géographiques. Ainsi, même si vous créez des enregistrements de géolocalisation couvrant les sept continents, Amazon Route 53 recevra des requêtes DNS à partir d'emplacements qu'il n'est pas en mesure d'identifier. Vous pouvez créer un enregistrement par défaut pour gérer les requêtes provenant d'adresses IP qui ne sont mappées à aucun emplacement et les requêtes issues d'emplacements pour lesquels vous n'avez pas créé d'enregistrements de géolocalisation. Si vous ne créez pas d'enregistrement par défaut, Route 53 renvoie un message « aucune réponse » pour les requêtes provenant de ces emplacements.

Vous pouvez utiliser le routage de géolocalisation pour des enregistrements dans les zones hébergées publiques et privées.

Pour de plus amples informations, veuillez consulter Comment Amazon Route 53 utilise EDNS0 pour estimer l'emplacement d'un utilisateur.

Pour plus d'informations sur les valeurs que vous spécifiez lorsque vous utilisez la stratégie de routage de géolocalisation pour créer des enregistrements, consultez les rubriques suivantes :

- Valeurs spécifiques aux enregistrements de géolocalisation
- Valeurs spécifiques aux enregistrements d'alias de géolocalisation
- Valeurs communes à toutes les politiques de routage

- Valeurs communes aux enregistrements d'alias pour toutes les politiques de routage

Routage de géolocalisation dans des zones hébergées privées

Pour les zones hébergées privées, Route 53 répond aux requêtes DNS en fonction Région AWS du VPC d'où provient la requête. Pour en obtenir la liste Régions AWS, voir Régions et zones dans le guide de l' EC2 utilisateur d'Amazon.

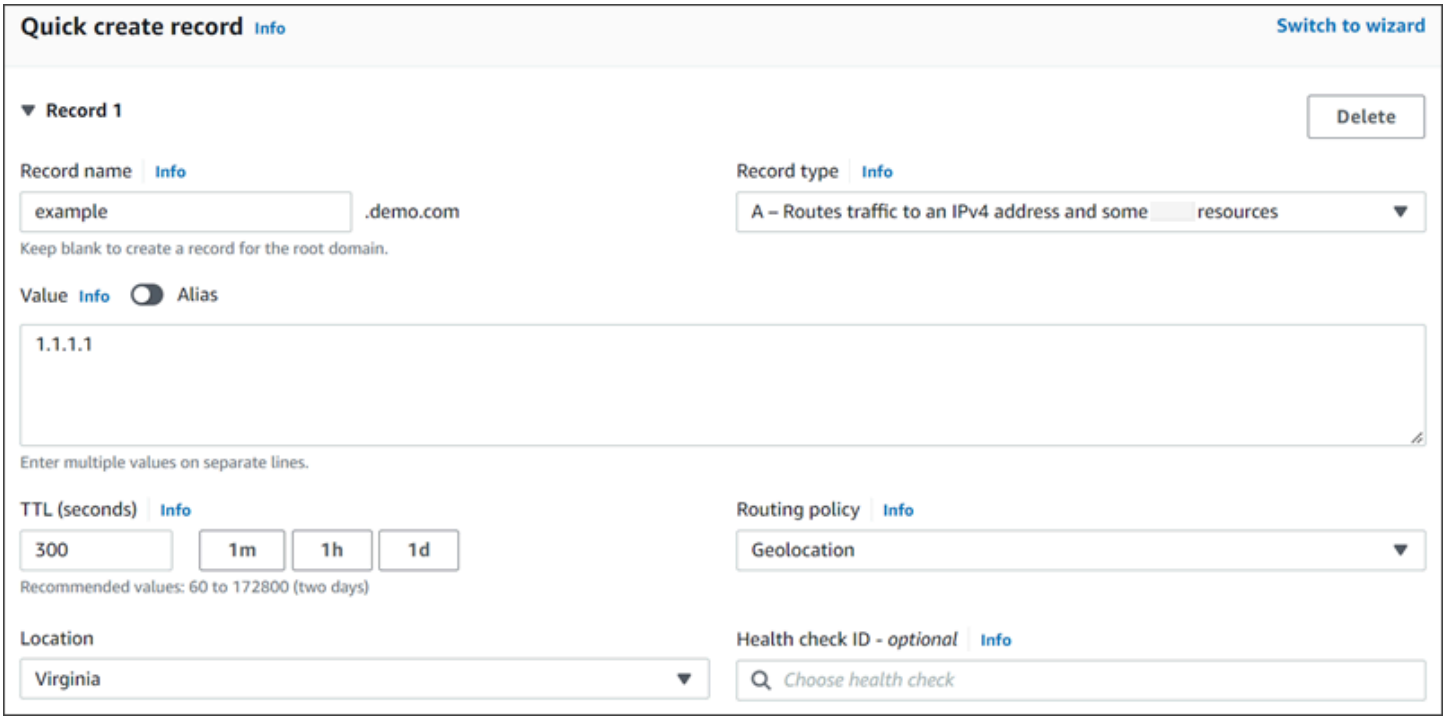
Si la requête DNS provient d'une partie sur site d'un réseau hybride, elle sera considérée comme provenant de la Région AWS dans laquelle se trouve le VPC.

Si vous incluez des surveillances de l'état, vous pouvez créer des enregistrements par défaut pour :

- Les adresses IP qui ne sont pas mappées à des emplacements géographiques.
- Les requêtes DNS qui proviennent d'emplacements pour lesquels vous n'avez pas créé d'enregistrement de géolocalisation.

Si l'enregistrement de géolocalisation pour la région de la requête DNS est défectueux, l'enregistrement par défaut sera renvoyé (s'il est sain).

Dans l'exemple de configuration illustré dans la figure suivante, les requêtes DNS provenant d'un Région AWS us-east-1 (Virginie) seront acheminées vers le point de terminaison 1.1.1.1.



Routage par géoproximité

Avec le routage par proximité géographique, Amazon Route 53 achemine le trafic vers vos ressources en fonction de l'emplacement géographique de vos utilisateurs et ressources. Il achemine le trafic vers la ressource disponible la plus proche. Vous pouvez également, si vous le souhaitez, choisir d'acheminer davantage ou moins de trafic vers une ressource donnée en spécifiant une valeur, appelée écart. Un écart augmente ou réduit la taille de la région géographique à partir de laquelle le trafic est acheminé vers une ressource.

Vous créez des règles de proximité géographique pour vos ressources et spécifiez l'une des valeurs suivantes pour chaque règle :

- Si vous utilisez AWS des ressources, spécifiez le Région AWS ou le groupe de zones local dans lequel vous avez créé la ressource.
- Si vous n'utilisez pas de AWS ressources, spécifiez la latitude et la longitude de la ressource.

Pour utiliser AWS les Zones Locales, vous devez d'abord les activer. Pour plus d'informations, consultez Premiers pas avec les zones locales dans le Guide de l'utilisateur des zones locales AWS .

Pour en savoir plus sur la différence entre les zones Régions AWS et les zones locales, consultez Régions et zones dans le guide de EC2 l'utilisateur Amazon.

(Facultatif) Pour modifier la taille de la région géographique à partir de laquelle Route 53 achemine le trafic vers une ressource, spécifiez la valeur d'écart applicable :

- Pour étendre la taille de la région géographique à partir de laquelle Route 53 achemine le trafic vers une ressource, spécifiez un nombre entier positif compris entre 1 et 99 en tant que valeur d'écart. Route 53 diminue la taille des régions adjacentes.
- Pour réduire la taille de la région géographique à partir de laquelle Route 53 achemine le trafic vers une ressource, spécifiez une valeur d'écart négative comprise entre -1 et -99. Route 53 étend la taille des régions adjacentes.

> **Note**
>
> Nous mettons à jour la console Traffic Flow pour Route 53. Pendant la période de transition, vous pouvez continuer à utiliser l'ancienne console.

Choisissez l'onglet correspondant à la console que vous utilisez.

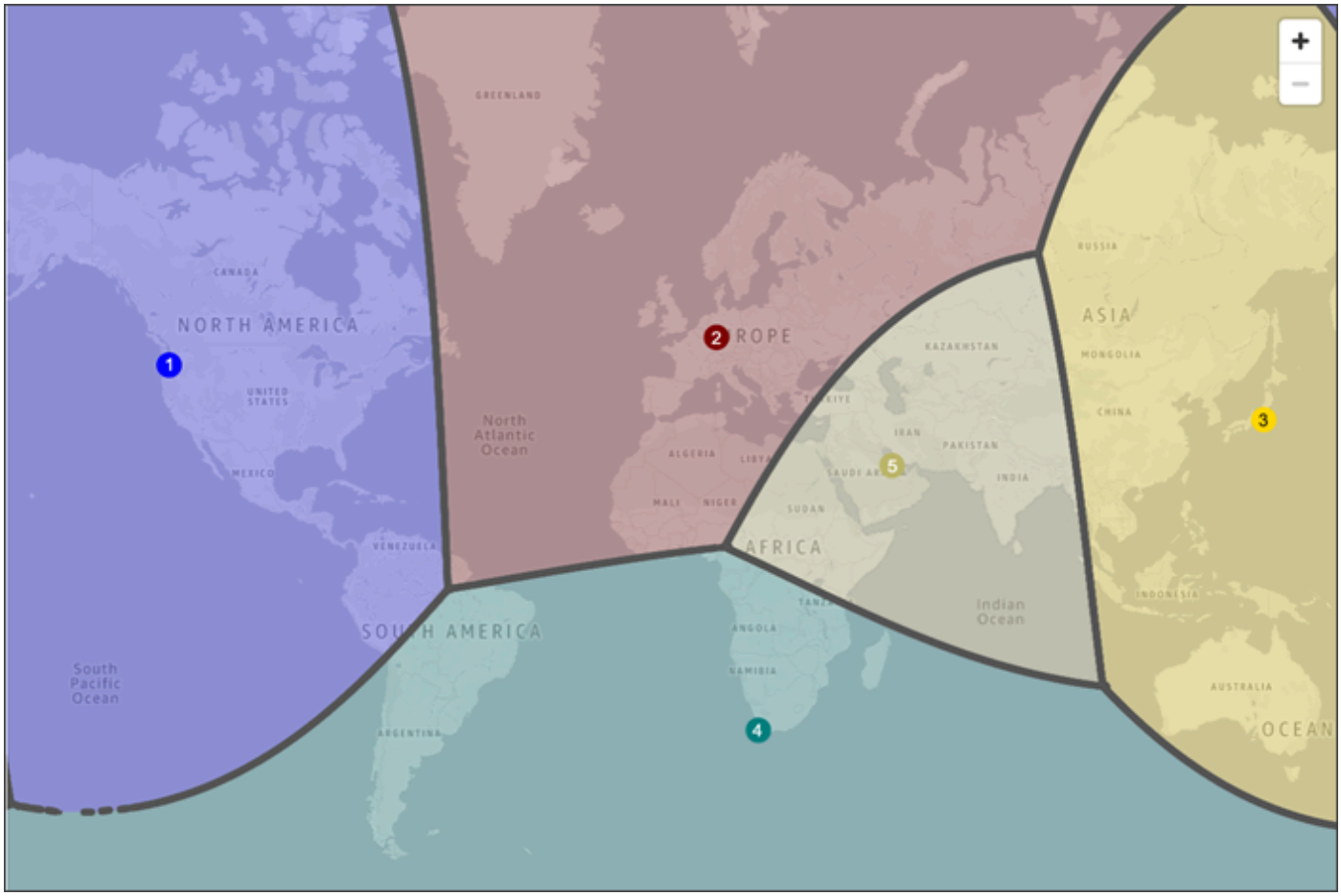
- Nouvelle console
- Ancienne console

New console

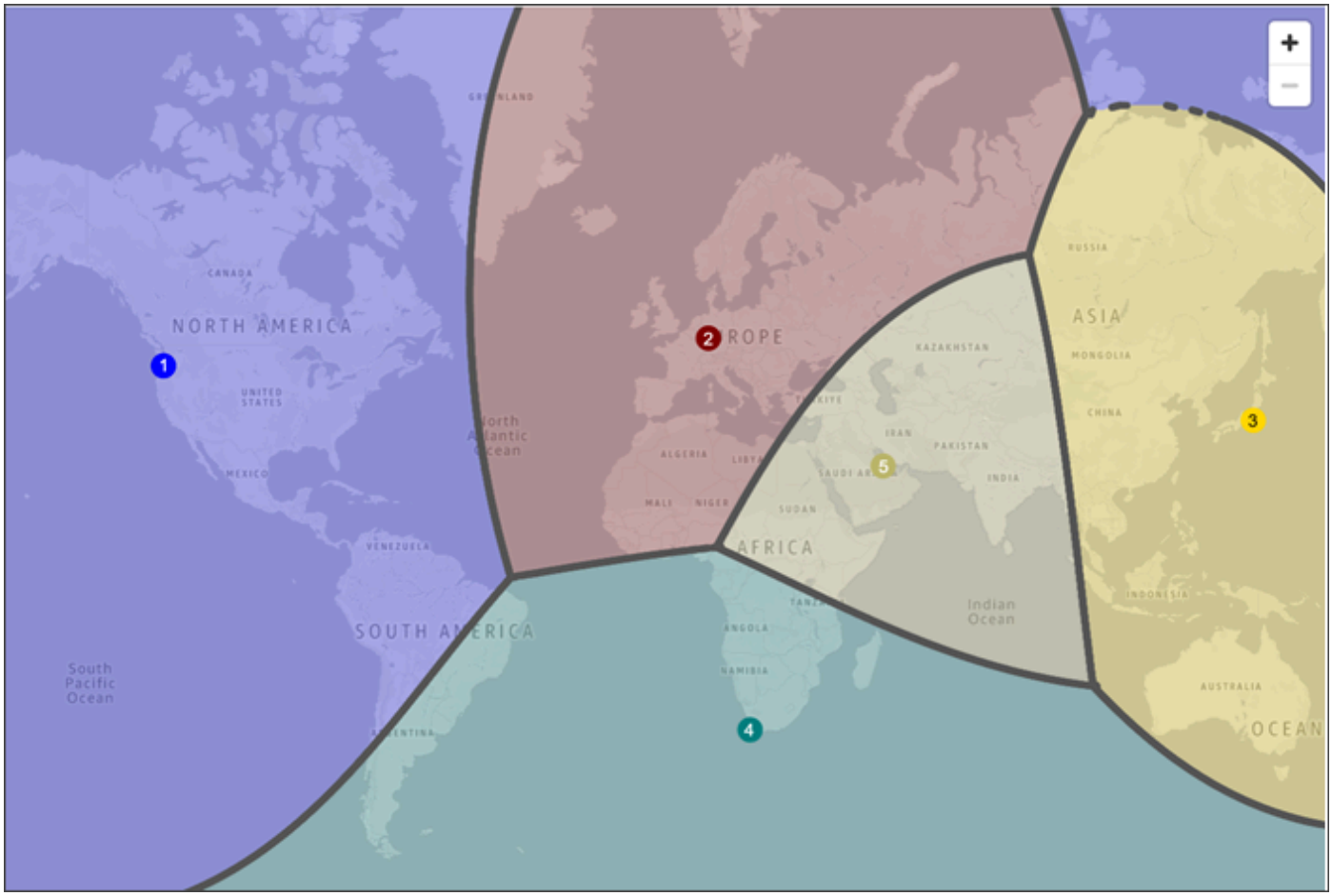
La carte suivante en montre quatre Régions AWS (numérotées de 1 à 5) :

1. USA Ouest (Oregon)
2. Europe (Francfort)
3. Asie-Pacifique (Tokyo)
4. Afrique (Le Cap)
5. Moyen-Orient (Bahreïn)

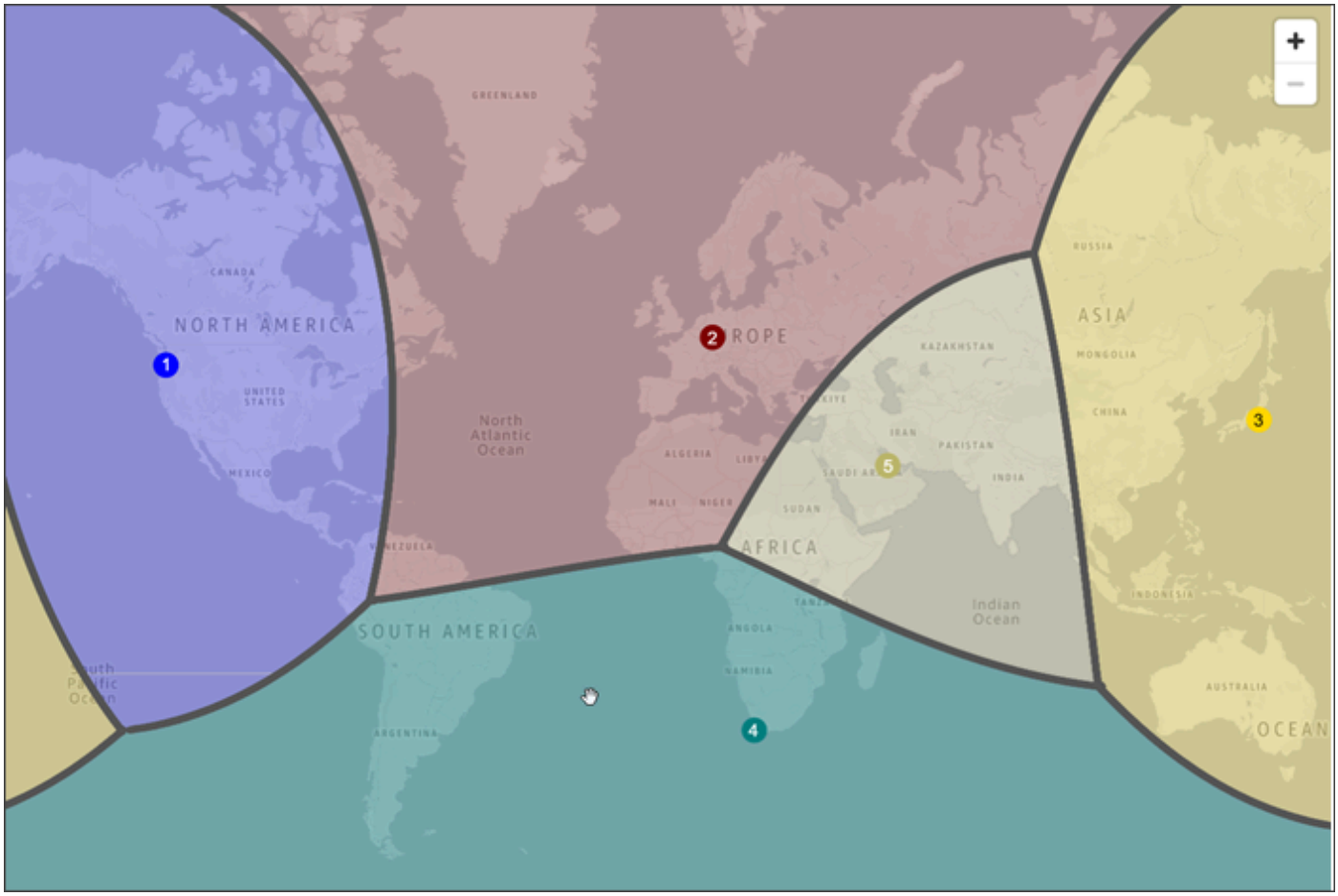
> **Note**
>
> Les cartes ne sont disponibles qu'avec Traffic Flow.



La carte suivante montre ce qui se passe si vous ajoutez un biais de +25 pour la région USA Ouest (Oregon) (numéro 1 sur la carte). Le trafic est acheminé vers la ressource dans cette région à partir d'une plus grande partie de l'Amérique du Nord et de toute l'Amérique du Sud qu'auparavant.



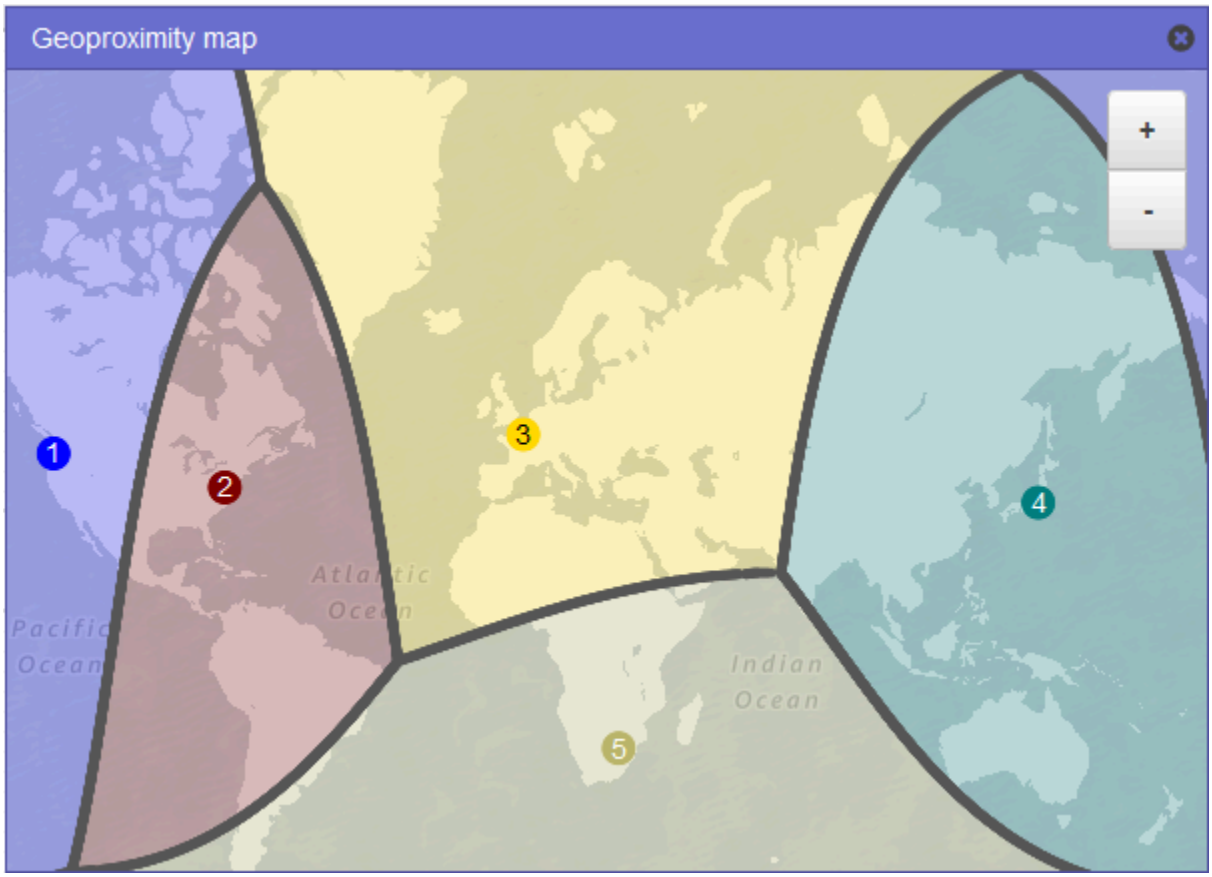
La carte suivante montre ce qui se passe si vous modifiez le biais à -25 pour la région de l'ouest des États-Unis (Oregon). Le trafic est acheminé vers la ressource de cette région depuis de plus petites parties de l'Amérique du Nord et du Sud qu'auparavant, et une plus grande partie du trafic est acheminée vers les ressources des régions adjacentes 2, 3 et 4.



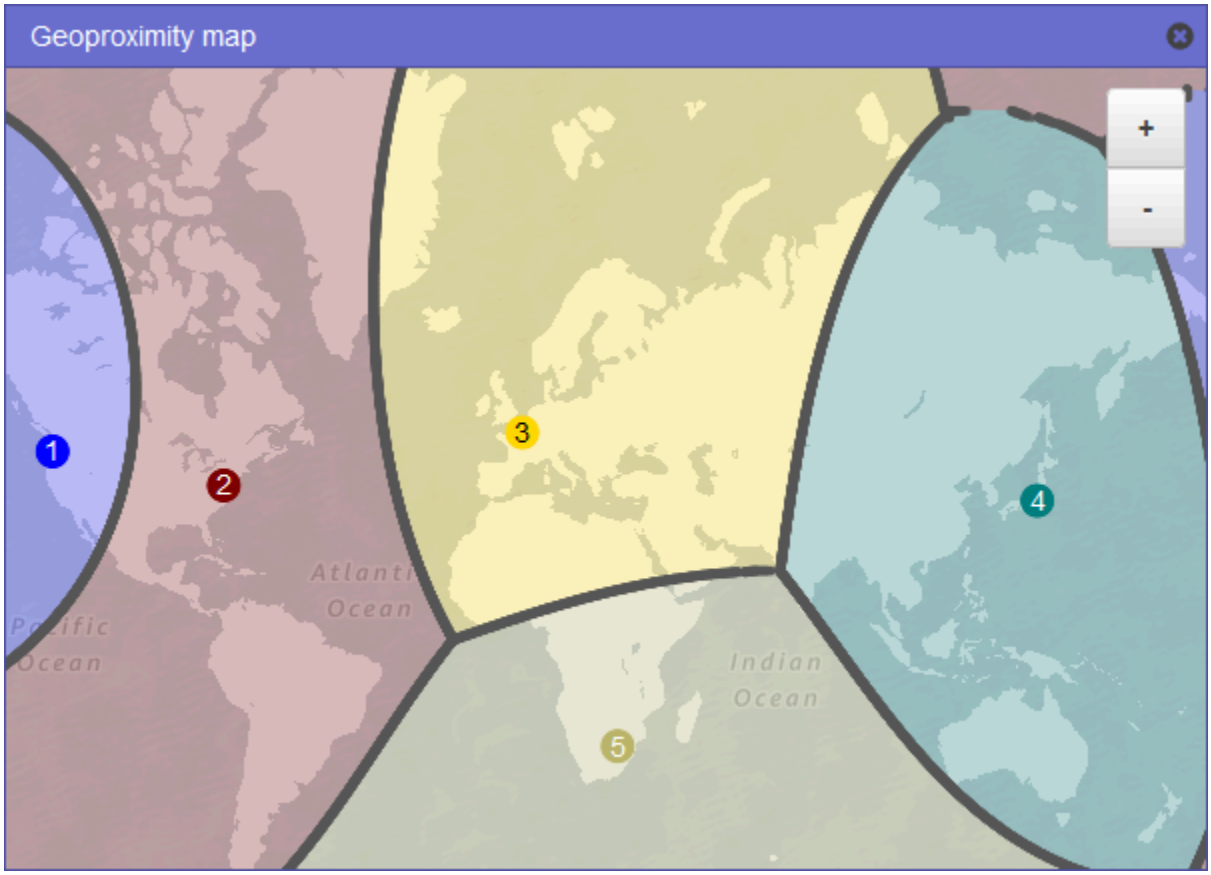
Old console

La carte suivante en montre quatre Régions AWS (numérotées de 1 à 4) et un emplacement à Johannesburg, en Afrique du Sud, indiqué par la latitude et la longitude (5).

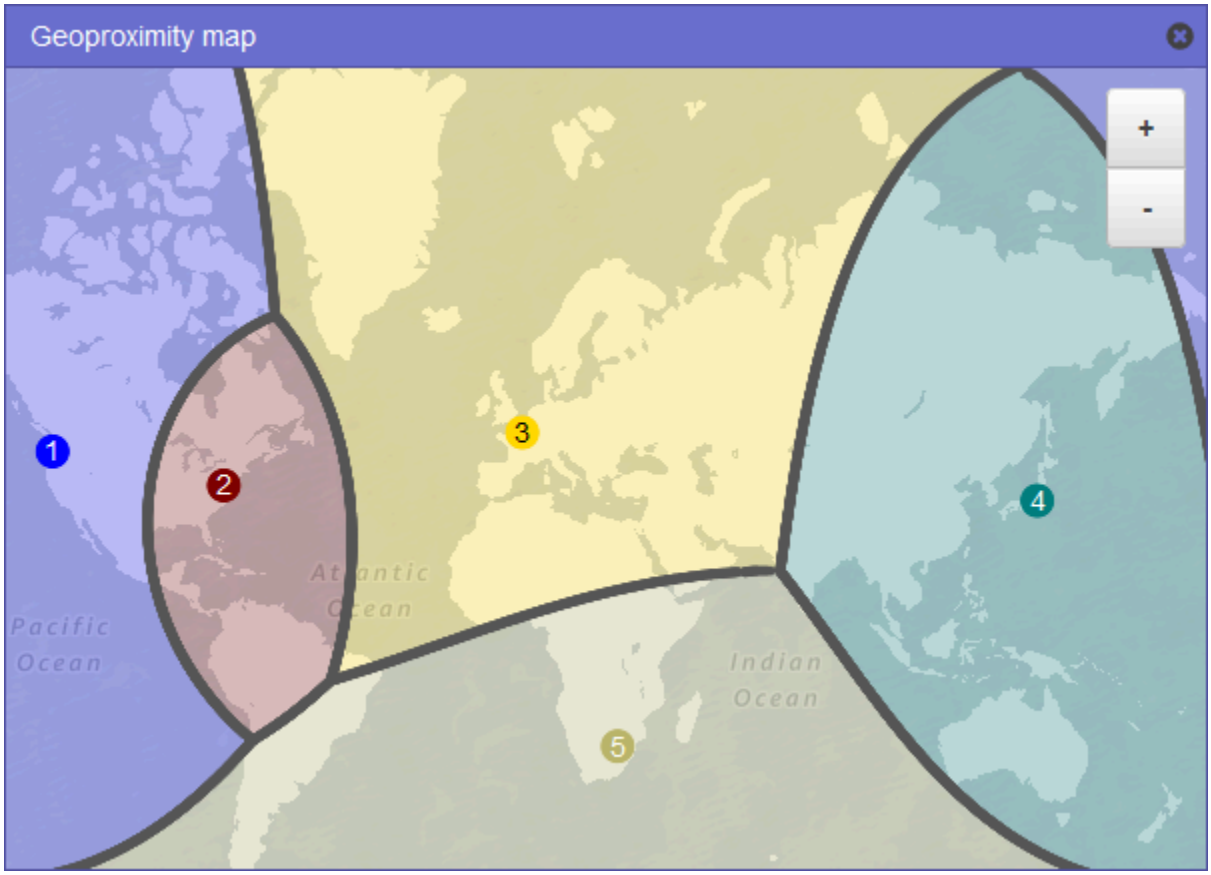
> **Note**
>
> Les cartes ne sont disponibles qu'avec Traffic Flow.



La carte suivante montre ce qui se produit si vous ajoutez un écart de +25 pour la région USA Est (Virginie du Nord) (numéro 2 sur la carte). Le trafic est acheminé vers la ressource dans cette région à partir d'une plus grande partie de l'Amérique du Nord que précédemment, et à partir de l'ensemble de l'Amérique du Sud.



La carte suivante montre ce qui se produit si vous modifiez l'écart à -25 pour la région USA Est (Virginie du Nord). Le trafic est acheminé vers la ressource dans cette région à partir de plus petites parties d'Amérique du Nord et du Sud que précédemment, et davantage de trafic est acheminé vers les ressources dans les régions adjacentes 1, 3 et 5.



L'impact de la valeur d'écart de vos ressources dépend d'un certain nombre de facteurs, dont les éléments suivants :

- Le nombre de ressources dont vous disposez.
- La proximité des ressources les unes par rapport aux autres.
- Le nombre de vos utilisateurs se trouvant à proximité de la zone frontalière entre les régions géographiques. Supposons, par exemple, que vous disposiez de ressources dans l'est des Régions AWS États-Unis (Virginie du Nord) et dans l'ouest des États-Unis (Oregon), et que vous ayez de nombreux utilisateurs à Dallas, Austin et San Antonio, au Texas, aux États-Unis. Ces villes étant approximativement à égale distance entre vos ressources, un léger changement de biais pourrait entraîner une importante variation du trafic entre les ressources. Région AWS

Nous vous recommandons de modifier la valeur d'écart par petits incréments afin d'éviter de surcharger vos ressources en raison d'un basculement inattendu du trafic.

Pour de plus amples informations, veuillez consulter Comment Amazon Route 53 utilise EDNS0 pour estimer l'emplacement d'un utilisateur.

Comment Amazon Route 53 utilise une valeur d'écart pour acheminer le trafic

Voici la formule utilisée par Amazon Route 53 pour déterminer la manière d'acheminer le trafic :

Écart

```
Biased distance = actual distance * [1 - (bias/100)]
```

Lorsque la valeur du biais est positive, Route 53 traite la source d'une requête DNS et la ressource que vous spécifiez dans un enregistrement de géoproximité (telle qu'une EC2 instance dans un Région AWS) comme si elles étaient plus proches l'une de l'autre qu'elles ne le sont réellement. Supposons par exemple que vous disposez des enregistrements de proximité géographique suivants :

- Un enregistrement pour un serveur Web A, qui possède une valeur d'écart positive de 50
- Un enregistrement pour un serveur Web B qui ne possède aucune valeur d'écart

Lorsqu'un enregistrement de proximité géographique possède une valeur d'écart positive de 50, Route 53 divise par deux la distance entre la source d'une requête et la ressource correspondant à cet enregistrement. Route 53 détermine ensuite par des calculs la ressource la plus proche de la source de la requête. Supposons qu'un serveur Web A se trouve à 150 kilomètres de la source d'une requête et que le serveur Web B se trouve à 100 kilomètres de la source de la requête. Si aucun enregistrement n'avait eu de valeur d'écart, Route 53 aurait acheminé la requête vers le serveur Web B, en raison de sa proximité. Cependant, puisque l'enregistrement pour le serveur Web A s'accompagne d'une valeur d'écart positive de 50, Route 53 considère que le serveur Web A se trouve à 75 kilomètres de la source de la requête. Route 53 va donc acheminer la requête vers le serveur Web A.

Voici le calcul pour une valeur d'écart positive de 50 :

```
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
```

Routage basé sur la latence

Si votre application est hébergée sur plusieurs sites Régions AWS, vous pouvez améliorer les performances de vos utilisateurs en traitant leurs demandes à partir de la solution Région AWS offrant la latence la plus faible.

> **Note**
>
> Les données relatives à la latence entre les utilisateurs et vos ressources sont entièrement basées sur le trafic entre les utilisateurs et les centres de données AWS . Si vous n'utilisez pas de ressources dans un Région AWS, la latence réelle entre vos utilisateurs et vos ressources peut varier considérablement en fonction des données de AWS latence. Cela est vrai même si vos ressources sont situées dans la même ville qu'une Région AWS.

Pour utiliser le routage basé sur la latence, vous créez des enregistrements pour vos ressources dans plusieurs Régions AWS. Lorsque Route 53 reçoit une requête DNS pour votre domaine ou un sous-domaine (exemple.com ou acme.exemple.com), il détermine les Régions AWS pour lesquelles vous avez créé des enregistrements de latence, les régions offrant aux utilisateurs la latence la plus faible, puis sélectionne un enregistrement de latence pour cette région. Route 53 répond avec la valeur de l'enregistrement sélectionné, telle que l'adresse IP d'un serveur Web.

Par exemple, si vous disposez d'équilibreurs de charge Elastic Load Balancing dans la région USA Ouest (Oregon) et la région Asie-Pacifique (Singapour). Vous avez créé un enregistrement de latence pour chaque équilibreur de charge. Voici ce qui se produit quand un utilisateur basé à Londres entre le nom de votre domaine dans un navigateur :

1. DNS achemine la requête vers un serveur de noms Route 53.
2. Route 53 se réfère à ses données relatives à la latence entre Londres et la région Singapour, et entre Londres et la région Oregon.
3. Si la latence est inférieure entre les régions de Londres et de l'Oregon, Route 53 répond à la requête avec l'adresse IP de l'équilibreur de charge de l'Oregon. Si la latence est inférieure entre les régions de Londres et de Singapour, Route 53 répond avec l'adresse IP de l'équilibreur de charge de Singapour.

La latence entre les hôtes sur Internet peut évoluer au fil du temps, suite à des modifications de connectivité réseau et de routage. Le routage basé sur la latence s'appuie sur des mesures de

latence réalisées sur une période donnée. Ces mesures reflètent ces évolutions. Une demande acheminée vers la région de l'Oregon une semaine peut être acheminée vers la région de Singapour la semaine suivante.

> **Note**
>
> Lorsqu'un navigateur ou un autre utilisateur utilise un résolveur DNS qui prend en charge l' edns-client-subnetextension EDNS0, le résolveur DNS envoie à Route 53 une version tronquée de l'adresse IP de l'utilisateur. Si vous configurez le routage en fonction de la latence, Route 53 tient compte de cette valeur lors de l'acheminement du trafic vers vos ressources. Pour de plus amples informations, veuillez consulter Comment Amazon Route 53 utilise EDNS0 pour estimer l'emplacement d'un utilisateur.

Vous pouvez utiliser la stratégie de routage de latence pour des enregistrements dans une zone hébergée privée.

Pour plus d'informations sur les valeurs que vous spécifiez lorsque vous utilisez la stratégie de routage de latence pour créer des enregistrements, consultez les rubriques suivantes :

- Valeurs spécifiques aux enregistrements de latence
- Valeurs spécifiques aux enregistrements d'alias de latence
- Valeurs communes à toutes les politiques de routage
- Valeurs communes aux enregistrements d'alias pour toutes les politiques de routage

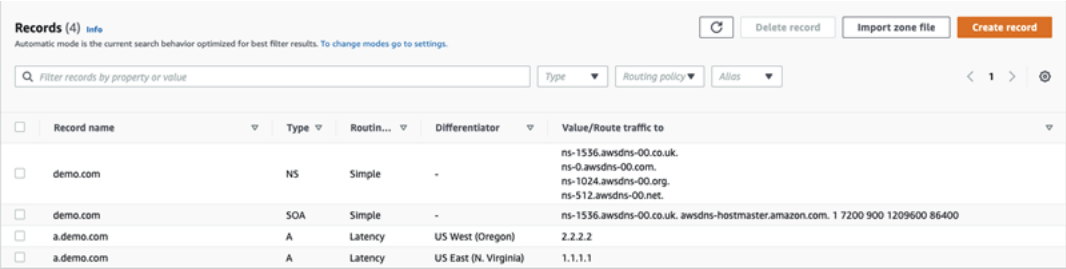
Routage basé sur la latence dans les zones hébergées privées

Pour les zones hébergées privées, Route 53 répond aux requêtes DNS avec un point de terminaison Région AWS situé au même endroit ou le plus proche Région AWS du VPC d'où provient la requête.

> **Note**
>
> Si un point de terminaison sortant est transféré vers un point de terminaison entrant, l'enregistrement sera résolu en fonction de l'emplacement du point de terminaison entrant, et non du point de terminaison sortant.

Si vous incluez des surveillances de l'état et que l'enregistrement avec la latence la plus faible par rapport à l'origine de la requête est défectueux, un point de terminaison sain avec la latence la plus faible est renvoyé.

Dans l'exemple de configuration illustré dans la figure suivante, les requêtes DNS provenant d'un Région AWS us-east-1, ou du plus proche de celui-ci, seront acheminées vers le point de terminaison 1.1.1.1. Les requêtes DNS provenant de la région us-west-2, ou la plus proche de celle-ci, seront acheminées vers le point de terminaison 2.2.2.2.



Routage basé sur IP

Avec le routage basé sur IP dans Amazon Route 53, vous pouvez affiner votre routage DNS en utilisant votre compréhension de votre réseau, de vos applications, et de vos clients pour prendre les meilleures décisions de routage DNS pour vos utilisateurs finaux. Le routage basé sur IP vous donne un contrôle granulaire pour optimiser les performances ou réduire les coûts du réseau en téléchargeant vos données sur Route 53 sous forme de mappages. user-IP-to-endpoint

Le routage basé sur la géolocalisation et la latence s'appuie sur les données que Route 53 collecte et tient à jour. Cette approche fonctionne bien pour la majorité des clients, mais le routage basé sur IP vous offre la possibilité supplémentaire d'optimiser le routage en fonction de la connaissance spécifique de votre clientèle. Par exemple, un fournisseur mondial de contenu vidéo peut vouloir acheminer les utilisateurs finaux à partir d'un fournisseur de services Internet (FSI) particulier.

Voici quelques cas d'utilisation courants du routage basé sur IP :

- Vous souhaitez acheminer les utilisateurs finaux de certains points de terminaison ISPs vers des points de terminaison spécifiques afin d'optimiser les coûts ou les performances du réseau.
- Vous voulez ajouter des surcharges aux types de routage Route 53 existants, comme le routage de géolocalisation, en fonction de votre connaissance des emplacements physiques de vos clients.

Gérer les plages d'adresses IP et les associer à un ensemble d'enregistrements de ressources (RRSet)

Pour IPv4, vous pouvez utiliser des blocs d'adresse CIDR d'une longueur comprise entre 1 et 24 bits inclus, tandis que pourIPv6, vous pouvez utiliser des blocs d'adresse CIDR d'une longueur comprise entre 1 et 48 bits inclus. Pour définir un bloc d'adresse CIDR zéro bit (0.0.0.0/0 or ::/0), utilisez l'emplacement par défaut (« * »).

Pour les requêtes DNS dont le CIDR est plus long que celui spécifié dans la collection d'adresses CIDR, Route 53 les met en correspondance avec le CIDR le plus court. Par exemple, si vous spécifiez 2001:0 DB8 : :/32 comme bloc CIDR dans votre collection CIDR et qu'une requête provient de 2001:0 DB8 : 0000:1234 : :/48, elle correspondra. Si, par contre, vous spécifiez 2001:0 DB8 : 0000:1234 : :/48 dans votre collection CIDR et qu'une requête provient de 2001:0 DB8 : :/32, cela ne correspondra pas et Route 53 répondra avec l'enregistrement correspondant à l'emplacement par défaut (« * »).

Vous pouvez regrouper des jeux de blocs CIDR (ou plages IP) en emplacements CIDR, qui sont à leur tour regroupés en entités réutilisables appelées collections CIDR :

Bloc d'adresse CIDR

Une plage d'adresses IP en notation CIDR, par exemple 192.0.2.0/24 ou 2001 : : :/32. DB8

Emplacement CIDR

Une liste nommée de blocs CIDR. Par exemple, example-isp-seattle = [192.0.2.0/24, 203.0.113.0/22, 198.51.100.0/24, 2001 : : :/32]. DB8 Les blocs d'une liste d'emplacements CIDR ne doivent pas nécessairement être adjacents ou appartenir à la même plage.

Un même emplacement peut avoir les deux IPv6 blocs IPv4 et cet emplacement peut être associé à la fois aux ensembles d'enregistrements A et AAAA, respectivement.

Le nom de l'emplacement est souvent un emplacement par convention, mais peut être n'importe quelle chaîne, par exemple Entreprise-A.

Collection CIDR

Une collection d'emplacements nommée. Par exemple, mycollection = [example-isp-seattle, example-isp-tokyo].

Les jeux d'enregistrements de ressources de routage basé sur IP font référence à un emplacement dans une collection, et tous les jeux d'enregistrements de ressources pour le même nom et type de jeu d'enregistrements doivent faire référence à la même collection. Par exemple, si vous créez des sites Web dans deux régions et que vous voulez diriger les requêtes DNS de deux

emplacements CIDR différents vers un site Web spécifique en fonction des adresses IP d'origine, ces deux emplacements doivent être répertoriés dans la même collection CIDR.

Vous ne pouvez pas utiliser la politique de routage basée sur IP pour les enregistrements dans une zone hébergée privée.

Pour plus d'informations sur les valeurs que vous spécifiez lorsque vous utilisez la politique de routage basée sur IP pour créer des enregistrements, consultez les rubriques suivantes :

- Valeurs spécifiques aux enregistrements basés sur IP
- Valeurs spécifiques aux enregistrements d'alias basés sur IP
- Valeurs communes à toutes les politiques de routage
- Valeurs communes aux enregistrements d'alias pour toutes les politiques de routage

Rubriques

- Création d'une collection CIDR avec des emplacements et des blocs CIDR
- Utilisation des emplacements et des blocs CIDR
- Suppression d'une collection CIDR
- Déplacement d'un routage par géolocalisation vers un routage basé sur IP

Création d'une collection CIDR avec des emplacements et des blocs CIDR

Pour commencer, créez une collection CIDR et ajoutez-y des blocs et des emplacements CIDR.

Pour créer une collection CIDR à l'aide de la console Route 53

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le panneau de navigation, choisissez IP-based routing (Routage basé sur IP), puis CIDR collections (Collections CIDR).
3. Sélectionnez Create CIDR collection (Créer une collection CIDR).
4. Dans le panneau Create CIDR collection (Créer une collection CIDR), sous Details (Détails), saisissez un nom pour la collection.
5. Choisissez Create collection (Créer une collection) pour créer une collection vide.

- ou -

Dans la section Créer des emplacements CIDR, saisissez le nom de l'emplacement CIDR dans le champ Emplacement CIDR. Le nom de l'emplacement peut être n'importe quelle chaîne d'identification, par exemple **`company 1`** ou **`Seattle`**. Il ne doit pas nécessairement s'agir d'un emplacement géographique réel.

> **Important**
>
> Le nom de l'emplacement CIDR a une longueur maximale de 16 caractères.

Saisissez les blocs d'adresse CIDR dans le champ Blocs CIDR, un par ligne. Il peut s'agir IPv4 d' IPv6 adresses comprises entre /0 et /24 pour IPv4 et /0 à /48 pour. IPv6

6. Après avoir saisi les blocs CIDR, choisissez Create CIDR collection (Créer une collection CIDR), ou Add another location (Ajouter un autre emplacement) pour continuer à saisir des emplacements et un bloc CIDR. Vous pouvez saisir plusieurs emplacements CIDR par collection.
7. Après avoir saisi les emplacements CIDR, choisissez Create CIDR collection (Créer une collection CIDR).

Utilisation des emplacements et des blocs CIDR

Pour travailler avec des emplacements CIDR en utilisant la console Route 53

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le panneau de navigation, choisissez IP-based routing (Routage basé sur IP), CIDR collections (Collections CIDR), puis, dans la section CIDR collections (Collections CIDR), cliquez sur un lien vers une collection CIDR dans la liste Collection name (Nom de la collection).

   Sur la page CIDR locations (Emplacements CIDR), vous pouvez créer un emplacement CIDR, le supprimer ou modifier un emplacement et ses blocs.

   - Pour créer un emplacement, choisissez Create CIDR location (Créer un emplacement CIDR).
   - Dans le panneau Create CIDR location (Créer un emplacement CIDR), saisissez un nom pour l'emplacement, les blocs CIDR associés à l'emplacement, puis cliquez sur Create (Créer).

- Pour afficher un emplacement CIDR et les blocs qu'il contient, choisissez la case d'option en regard d'un emplacement pour afficher son nom et ses blocs CIDR dans le panneau d'emplacement.

  Dans ce panneau, vous pouvez également choisir Modifier pour mettre à jour le nom de l'emplacement ou de ses blocs CIDR. Choisissez Save (Enregistrer) lorsque vous avez terminé la modification.
- Pour supprimer un emplacement CIDR et les blocs qu'il contient, sélectionnez la case d'option en regard de l'emplacement que vous voulez supprimer, puis cliquez sur Delete (Supprimer). Pour confirmer la suppression, saisissez le nom de l'emplacement dans la zone de saisie de texte et sélectionnez à nouveau Delete (Supprimer).

> **Important**
>
> La suppression d'un emplacement CIDR ne peut pas être annulée. Si vous avez des enregistrements DNS associés à l'emplacement, votre domaine peut devenir inaccessible.

Suppression d'une collection CIDR

Pour supprimer une collection CIDR, ses emplacements et blocs en utilisant la console Route 53

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le panneau de navigation, choisissez IP-based routing (Routage basé sur IP), puis CIDR collections (Collections CIDR).
3. Dans la section CIDR collections (Collections CIDR), cliquez sur le nom lié de la collection que vous voulez supprimer.
4. Sur la page CIDR locations (Emplacements CIDR), sélectionnez chaque emplacement un par un, choisissez Delete (Supprimer), saisissez son nom dans la boîte de dialogue, puis choisissez Delete (Supprimer). Vous devez supprimer chaque emplacement associé à une collection CIDR avant de pouvoir supprimer la collection.
5. Une fois la suppression de chaque emplacement CIDR terminée, sur la page CIDR locations (Emplacements CIDR), choisissez le bouton radio en regard de la collection que vous voulez supprimer, puis choisissez Delete (Supprimer).

Déplacement d'un routage par géolocalisation vers un routage basé sur IP

Si vous utilisez des politiques de routage par géolocalisation ou par géoproximité et que vous constatez régulièrement que des clients spécifiques sont acheminés vers un point de terminaison qui n'est pas optimal en fonction de leur emplacement physique ou de la topologie du réseau, vous pouvez mieux cibler les plages IP publiques de ces clients en utilisant le routage par IP.

Le tableau suivant contient un exemple de configuration de géolocalisation pour un routage de géolocalisation existant que nous allons acheminer avec précision pour les plages IP de Californie.

Nom du jeu d'enregistrements	Politique et origine du routage	Adresse IP du point de terminaison de l'application
example.com	Routage par géolocalisation (US)	`198.51.100.1`
example.com	Routage par géolocalisation (UE)	`198.51.100.2`

Pour remplacer les plages IP de Californie par un nouveau point de terminaison d'application, recréez d'abord le routage de géolocalisation sous un nouveau nom de jeu d'enregistrements.

Nom du jeu d'enregistrements	Politique et origine du routage	Adresse IP du point de terminaison de l'application
geo.example.com	Routage par géolocalisation (US)	`198.51.100.1`
geo.example.com	Routage par géolocalisation (UE)	`198.51.100.2`

Créez ensuite des enregistrements de routage basés sur IP et un enregistrement par défaut qui pointe vers votre jeu d'enregistrements de routage de géolocalisation récemment recréé.

Nom du jeu d'enregistrements	Politique et origine du routage	Adresse IP du point de terminaison de l'application
example.com	Routage basé sur IP (par défaut)	Enregistrement d'alias vers le point de terminaison de l'application geo.example.com que vous voulez être le point par défaut. Par exemple, `198.51.100.1` .
example.com	Routage basé sur IP (plages IP de Californie)	`198.51.100.3`

Multivalue answer routing (Routage de réponse multivaleur)

Le routage de réponse multivaleur vous permet de configurer Amazon Route 53 pour renvoyer plusieurs valeurs, comme des adresses IP pour vos serveurs web, en réponse aux requêtes DNS. Vous pouvez spécifier plusieurs valeurs pour la plupart des enregistrements, mais le routage de réponse multivaleur vous permet également de vérifier l'intégrité de chaque ressource. Route 53 renvoie donc uniquement les valeurs des ressources saines. Il ne constitue pas de substitut pour un équilibreur de charge, mais la capacité de retourner plusieurs adresses IP dont l'intégrité est vérifiable permet d'utiliser DNS pour améliorer la disponibilité et l'équilibrage de charge.

Pour acheminer le trafic approximativement de manière aléatoire vers plusieurs ressources, comme des serveurs web, vous créez un enregistrement de réponse multivaleur pour chaque ressource et, facultativement, vous associez une surveillance de l'état Route 53 à chaque enregistrement. Route 53 répond aux requêtes DNS par jusqu'à huit enregistrements et fournit des réponses distinctes aux différents résolveurs DNS. Si un serveur web devient indisponible après qu'un résolveur met une réponse en cache, le logiciel client peut essayer une autre adresse IP dans la réponse.

Remarques :

- Si vous associez une surveillance de l'état à un enregistrement de réponse multivaleur, Route 53 répond aux requêtes DNS avec l'adresse IP correspondante uniquement lorsque la surveillance de l'état est saine.

- Si vous n'associez pas de surveillance de l'état à un enregistrement de réponse multivaleur, Route 53 considère toujours l'enregistrement comme sain.
- Si vous disposez de huit enregistrements sains ou moins, Route 53 répond à toutes les requêtes DNS par tous les enregistrements sains.
- Lorsque tous les registres sont non sains, Route 53 répond à toutes les requêtes DNS par jusqu'à huit registres non sains.

Vous pouvez utiliser la stratégie de routage de réponse multivaleur pour des enregistrements dans une zone hébergée privée.

Pour plus d'informations sur les valeurs que vous spécifiez lorsque vous utilisez la politique de routage de réponse multivaleur pour créer des enregistrements, veuillez consulter Valeurs spécifiques pour les enregistrements de réponses multivaleur et Valeurs communes à toutes les politiques de routage.

Weighted routing (Routage pondéré)

Le routage pondéré vous permet d'associer plusieurs ressources à un nom de domaine unique (par exemple, example.com) ou à un nom de sous-domaine (par exemple, acme.example.com) et de choisir le volume de trafic acheminé vers chaque ressource. Cela peut vous être utile pour de nombreuses actions, notamment l'équilibrage de charge et le test de nouvelles versions de logiciels.

Pour configurer un acheminement pondéré, créez des enregistrements avec les mêmes valeurs pour les champs Nom et Type que celles de vos ressources. Vous attribuez à chaque enregistrement une pondération relative correspondant au volume de trafic à envoyer à chaque ressource. Amazon Route 53 retourne le trafic vers une ressource en fonction de la pondération attribuée à l'enregistrement par rapport au poids total des enregistrements dans le groupe :

$$\frac{\text{Weight for a specified record}}{\text{Sum of the weights for all records}}$$

Par exemple, si vous souhaitez envoyer une petite partie de votre trafic vers une ressource et que le reste soit acheminé vers une autre ressource, vous pouvez spécifier des pondérations de 1 à 255. La ressource ayant une pondération de 1 obtient 1/256e du trafic (1/(1+255)) et l'autre ressource obtient 255/256e (255/(1+255)). Vous pouvez progressivement modifier l'équilibre en changeant les pondérations. Si vous arrêtez d'envoyer du trafic vers une ressource, vous pouvez passer la pondération de cette ressource à 0.

Pour plus d'informations sur les valeurs que vous spécifiez lorsque vous utilisez la stratégie de routage pondéré pour créer des enregistrements, consultez les rubriques suivantes :

- Valeurs spécifiques aux enregistrements pondérés
- Valeurs spécifiques aux enregistrements d'alias pondérés
- Valeurs communes à toutes les politiques de routage
- Valeurs communes aux enregistrements d'alias pour toutes les politiques de routage

Vous pouvez utiliser la stratégie de routage pondéré pour des enregistrements dans une zone hébergée privée.

Surveillance de l'état et routage pondéré

Si vous ajoutez les surveillances de l'état à tous les enregistrements d'un groupe d'enregistrements pondérés, mais que vous attribuez des pondérations différentes de zéro à certains enregistrements et des pondérations égales à zéro pour d'autres, les surveillances de l'état fonctionnent de la même manière que lorsque tous les enregistrements ont des pondérations différentes de zéro, avec les exceptions suivantes :

- Initialement, Route 53 prend uniquement en compte les enregistrements pondérés dont la pondération est différente de zéro, s'il y en a.
- Si tous les enregistrements ayant une pondération supérieure à 0 ne sont pas sains, Route 53 prend en compte les enregistrements dont la pondération est égale à zéro.

Le tableau suivant détaille le comportement lorsque l'enregistrement à pondération nulle inclut une surveillance de l'état :

	Enregistrement 1	Enregistrement 2	Enregistrement 3
Weight	1	1	0
Comprend la surveillance de l'état ?	Oui	Oui	Oui
	Non sain	Non sain	Sain

	Enregistrement 1	Enregistrement 2	Enregistrement 3
Statut de la surveillance de l'état			
Requête DNS répondue ?	Non	Non	Oui
Statut de la surveillance de l'état	Non sain	Non sain	Non sain
Requête DNS répondue ?	Oui	Oui	Non
Statut de la surveillance de l'état	Non sain	Sain	Non sain
Requête DNS répondue ?	Non	Oui	Non
Statut de la surveillance de l'état	Sain	Sain	Non sain
Requête DNS répondue ?	Oui	Oui	Non
Statut de la surveillance de l'état	Sain	Sain	Sain
Requête DNS répondue ?	Oui	Oui	Non

Le tableau suivant détaille le comportement lorsque l'enregistrement à pondération nulle n'inclut pas une surveillance de l'état :

	Enregistrement 1	Enregistrement 2	Enregistrement 3
Weight	1	1	0
Comprend la surveillance de l'état ?	Oui	Oui	Non
Statut de la surveillance de l'état	Sain	Sain	N/A
Requête DNS répondue ?	Oui	Oui	Non
Statut de la surveillance de l'état	Non sain	Non sain	N/A
Requête DNS répondue ?	Non	Non	Oui
Statut de la surveillance de l'état	Non sain	Sain	N/A
Requête DNS répondue ?	Non	Oui	Non

Comment Amazon Route 53 utilise EDNS0 pour estimer l'emplacement d'un utilisateur

Pour améliorer la précision de la géolocalisation, de la géoproximité, du routage basé sur IP et du routage par latence, Amazon Route 53 prend en charge l' edns-client-subnetextension d'EDNS0.

(EDNS0 ajoute plusieurs extensions facultatives au protocole DNS.) Route 53 ne peut être utilisée edns-client-subnet que lorsque les résolveurs DNS la prennent en charge :

- Lorsqu'un navigateur ou un autre lecteur utilise un résolveur DNS qui ne le prend pas en charge edns-client-subnet, Route 53 utilise l'adresse IP source du résolveur DNS pour localiser approximativement l'utilisateur et répond aux requêtes de géolocalisation avec l'enregistrement DNS correspondant à l'emplacement du résolveur.
- Lorsqu'un navigateur ou un autre utilisateur utilise un résolveur DNS compatible edns-client-subnet, le résolveur DNS envoie à Route 53 une version tronquée de l'adresse IP de l'utilisateur. Route 53 détermine l'emplacement de l'utilisateur en fonction de l'adresse IP tronquée plutôt que de l'adresse IP source du résolveur DNS ; cela fournit généralement une estimation plus précise de l'emplacement de l'utilisateur. Route 53 répond ensuite aux requêtes de géolocalisation avec l'enregistrement DNS correspondant à l'emplacement de l'utilisateur.
- EDNS0 n'est pas applicable aux zones hébergées privées. Pour les zones hébergées privées, Route 53 utilise les données des résolveurs Route 53 dans lesquelles se trouve la Région AWS zone hébergée privée pour prendre des décisions de géolocalisation et de routage avec latence.

Pour plus d'informations edns-client-subnet, consultez la RFC relative au sous-réseau du client EDNS, sous-réseau client dans les demandes DNS.

Choix entre des enregistrements avec ou sans alias

Les enregistrements d'alias Amazon Route 53 fournissent une extension spécifique à Route 53 à la fonctionnalité DNS. Les enregistrements d'alias vous permettent d'acheminer le trafic vers AWS des ressources sélectionnées, y compris, mais sans s'y limiter, les CloudFront distributions et les compartiments Amazon S3. Elles vous permettent également d'acheminer le trafic d'un enregistrement dans une zone hébergée vers un autre enregistrement.

Contrairement à l'enregistrement CNAME, vous pouvez créer un enregistrement d'alias pour le nœud supérieur d'un espace de nom DNS, également appelé zone apex. Par exemple, si vous enregistrez le nom DNS example.com, la zone apex est example.com. Vous ne pouvez pas créer un enregistrement CNAME pour exemple.com, mais vous pouvez créer un enregistrement d'alias pour exemple.com qui achemine le trafic vers www.exemple.com (tant que le type d'enregistrement pour www.exemple.com n'est pas CNAME).

Quand Route 53 reçoit une requête DNS pour un enregistrement d'alias, Route 53 répond avec la valeur applicable pour cette ressource :

- Une API régionale Amazon API Gateway personnalisée ou une API optimisée pour les périphériques : Route 53 répond avec une ou plusieurs adresses IP pour votre API.
- Un point de terminaison d'interface d'un VPC Amazon : Route 53 répond avec une ou plusieurs adresses IP pour votre point de terminaison d'interface.
- Une CloudFront distribution — Route 53 répond avec une ou plusieurs adresses IP pour les serveurs de CloudFront périphérie qui peuvent diffuser votre contenu.
- Service App Runner — Route 53 répond avec une ou plusieurs adresses IP.
- Un environnement Elastic Beanstalk : Route 53 répond avec une ou plusieurs adresses IP pour l'environnement.
- Un équilibreur de charge Elastic Load Balancing : Route 53 répond avec une ou plusieurs adresses IP pour l'équilibreur de charge. Cela inclut Application Load Balancer, Classic Load Balancer et Network Load Balancer.
- Un AWS Global Accelerator accélérateur — Route 53 répond avec les adresses IP de l'accélérateur.
- Un OpenSearch service — Route 53 répond avec une ou plusieurs adresses IP pour le domaine personnalisé du OpenSearch service.
- Un compartiment Amazon S3 configuré comme un site web statique : Route 53 répond avec une seule adresse IP pour le compartiment Amazon S3.
- Un autre enregistrement Route 53 du même type dans la même zone hébergée – Route 53 répond comme si la requête était destinée à l'enregistrement référencé par l'enregistrement d'alias (voir Comparaison d'enregistrements d'alias et CNAME).
- AWS AppSync nom de domaine — Route 53 répond avec une ou plusieurs adresses IP pour le point de terminaison de votre interface.

Pour de plus amples informations, veuillez consulter Acheminement du trafic Internet vers vos AWS ressources.

Lorsque vous utilisez un enregistrement d'alias pour acheminer le trafic vers une AWS ressource, Route 53 reconnaît automatiquement les modifications apportées à la ressource. Imaginez par exemple qu'un enregistrement d'alias pour example.com pointe vers un équilibreur de charge Elastic Load Balancing à l'adresse lb1-1234.us-east-2.elb.amazonaws.com. Si l'adresse IP de l'équilibreur de charge change, Route 53 commence automatiquement à répondre aux requêtes DNS à l'aide de la nouvelle adresse IP.

Si un enregistrement d'alias pointe vers une AWS ressource, vous ne pouvez pas définir la durée de vie (TTL) ; Route 53 utilise le TTL par défaut pour la ressource. Si un enregistrement d'alias pointe vers un autre enregistrement de la même zone hébergée, Route 53 utilise la durée de vie de l'enregistrement vers lequel l'enregistrement d'alias pointe. Pour de plus amples informations sur la valeur de la durée de vie actuelle pour Elastic Load Balancing, consultez Demande de routage dans le Guide de l'utilisateur Elastic Load Balancing et recherchez « ttl ».

Pour plus d'informations sur la création d'enregistrements à l'aide de la console Route 53, consultez Création d'enregistrements à l'aide de la console Amazon Route 53. Pour plus d'informations sur les valeurs que vous spécifiez dans les enregistrements d'alias, consultez la rubrique correspondante dans Valeurs à spécifier lorsque vous créez ou modifiez des enregistrements Amazon Route 53 :

- Valeurs spécifiques aux enregistrements d'alias simples
- Valeurs spécifiques aux enregistrements d'alias pondérés
- Valeurs spécifiques aux enregistrements d'alias de latence
- Valeurs spécifiques aux enregistrements d'alias de basculement
- Valeurs spécifiques aux enregistrements d'alias de géolocalisation
- Valeurs spécifiques aux enregistrements d'alias de géoproximité
- Valeurs communes aux enregistrements d'alias pour toutes les politiques de routage

Comparaison d'enregistrements d'alias et CNAME

Les enregistrements d'alias sont similaires aux enregistrements CNAME, mais présentent néanmoins des différences importantes : La liste suivante compare les enregistrements d'alias et les enregistrements CNAME.

Ressources vers lesquelles vous pouvez rediriger des requêtes

Enregistrements d'alias

Un enregistrement d'alias peut uniquement rediriger les requêtes vers AWS des ressources sélectionnées, y compris, mais sans s'y limiter, les suivantes :

- Compartiments Amazon S3
- CloudFront distributions
- Autre enregistrement dans la même zone hébergée Route 53

Par exemple, vous pouvez créer un enregistrement d'alias nommé acme.exemple.com qui redirige les requêtes vers un compartiment Amazon S3 qui est également

nommée acme.exemple.com. Vous pouvez également créer un enregistrement d'alias acme.exemple.com qui redirige les requêtes vers un enregistrement nommé zenith.exemple.com dans la zone hébergée exemple.com.

Enregistrements CNAME

Un enregistrement CNAME peut rediriger les requêtes DNS vers tout enregistrement DNS. Par exemple, vous pouvez créer un enregistrement CNAME qui redirige les requêtes depuis acme.exemple.com vers zenith.exemple.com ou acme.exemple.org. Vous n'avez pas besoin d'utiliser Route 53 comme service DNS pour le domaine vers lequel vous redirigez les requêtes.

Création d'enregistrements portant le même nom que le domaine (enregistrements dans la zone apex)

Enregistrements d'alias

Dans la plupart des configurations, vous pouvez créer un enregistrement d'alias portant le même nom que la zone hébergée (la zone apex). La seule exception survient lorsque vous souhaitez rediriger les requêtes depuis la zone apex (comme exemple.com) vers un enregistrement de la zone hébergée qui est de type CNAME (comme zenith.exemple.com). L'enregistrement d'alias doit être du même type que l'enregistrement vers lequel vous acheminez le trafic et que la création d'un enregistrement CNAME pour la zone apex n'est pas prise en charge, même pour un enregistrement d'alias.

Enregistrements CNAME

Vous ne pouvez pas créer un enregistrement CNAME portant le même nom que la zone hébergée (la zone apex). Cela est vrai pour les zones hébergées pour les noms de domaine (exemple.com) et pour les zones hébergées pour les sous-domaines (zenith.exemple.com).

Tarification des requêtes DNS

Enregistrements d'alias

Route 53 ne facture pas les requêtes d'alias vers les AWS ressources. Pour plus d’informations, consultez Tarification Amazon Route 53.

Enregistrements CNAME

Route 53 applique des frais pour les requêtes CNAME.

> **Note**
>
> Si vous créez un enregistrement CNAME qui procède à une redirection vers le nom d'un autre enregistrement dans une zone hébergée Route 53 (la même zone hébergée ou une autre zone hébergée), chaque requête DNS est facturée sur la base de deux requêtes :
>
> - Route 53 répond à la première requête DNS avec le nom de l'enregistrement vers lequel vous souhaitez procéder à la redirection.
> - Ensuite, le résolveur DNS doit soumettre une autre requête pour l'enregistrement dans la première réponse afin d'obtenir des informations sur l'endroit vers lequel diriger le trafic, par exemple, l'adresse IP d'un serveur Web.
>
> Si l'enregistrement CNAME procède à la redirection vers le nom d'un enregistrement hébergé avec un autre service DNS, Route 53 facture une requête. L'autre service DNS peut facturer la deuxième requête.

Type d'enregistrement spécifié dans la requête DNS

Enregistrements d'alias

Route 53 répond à une requête DNS uniquement lorsque le nom de l'enregistrement d'alias (par exemple, acme.exemple.com) et le type de l'enregistrement d'alias (par exemple, A ou AAAA) correspondent au nom et au type dans la requête DNS.

Enregistrements CNAME

Un enregistrement CNAME redirige les requêtes DNS pour un nom d'enregistrement, quel que soit le type d'enregistrement spécifié dans la requête DNS (A ou AAAA, par exemple).

Comment les enregistrements sont répertoriés dans des requêtes dig ou nslookup

Enregistrements d'alias

Dans la réponse à une requête dig ou nslookup, un enregistrement d'alias est répertorié selon le type d'enregistrement que vous avez spécifié lors de la création de l'enregistrement (A ou AAAA, par exemple). (Le type d'enregistrement que vous spécifiez pour un enregistrement d'alias dépend de la ressource vers laquelle vous acheminez le trafic. Par exemple, pour acheminer le trafic vers un compartiment S3, vous spécifiez le type A.) La propriété alias n'est visible que dans la console Route 53 ou dans la réponse à une demande programmatique, telle qu'une `list-resource-record-sets` commande AWS CLI.

Enregistrements CNAME

Un enregistrement CNAME est répertorié en tant qu'enregistrement CNAME en réponse à des requêtes dig ou nslookup.

Types d'enregistrements DNS pris en charge

Amazon Route 53 prend en charge les types d'enregistrement DNS qui sont répertoriés dans cette section. Chaque type d'enregistrement inclut également un exemple illustrant la façon de formater l'élément `Value` lorsque vous accédez à Route 53 à l'aide de l'API.

> **Note**
>
> Pour les types d'enregistrement qui incluent un nom de domaine, entrez un nom de domaine complet, par exemple, www.example.com. Le point final est facultatif ; Route 53 suppose que le nom de domaine est complet. Cela signifie que Route 53 traite www.example.com (sans point final) et www.example.com. (avec un point final) de la même façon.

Route 53 fournit une extension à la fonctionnalité DNS connue sous le nom d'enregistrement d'alias. À l'instar des enregistrements CNAME, les enregistrements d'alias vous permettent d'acheminer le trafic vers AWS des ressources sélectionnées, telles que les CloudFront distributions et les compartiments Amazon S3. Pour plus d'informations, notamment une comparaison des enregistrements d'alias et CNAME, consultez Choix entre des enregistrements avec ou sans alias.

Rubriques

- Type d'enregistrement
- Type d'enregistrement AAAA
- Type d'enregistrement CAA
- Type d'enregistrement CNAME
- Type d'enregistrement DS
- Type d'enregistrement HTTPS
- Type d'enregistrement MX
- Type d'enregistrement NAPTR
- Type d'enregistrement NS

- Type d'enregistrement PTR
- Type d'enregistrement SOA
- Type d'enregistrement SPF
- Type d'enregistrement SRV
- Type d'enregistrement SSHFP
- Type d'enregistrement SVCB
- Type d'enregistrement TLSA
- Type d'enregistrement TXT

Type d'enregistrement

Vous utilisez un enregistrement A pour acheminer le trafic vers une ressource, telle qu'un serveur Web, en utilisant une IPv4 adresse en notation décimale en pointillés.

Exemple pour la console Amazon Route 53

```
192.0.2.1
```

Exemple pour l'API Route 53

```
<Value>192.0.2.1</Value>
```

Type d'enregistrement AAAA

Vous utilisez un enregistrement AAAA pour acheminer le trafic vers une ressource, telle qu'un serveur Web, en utilisant une IPv6 adresse au format hexadécimal séparé par des deux-points.

Exemple pour la console Amazon Route 53

```
2001:0db8:85a3:0:0:8a2e:0370:7334
```

Exemple pour l'API Route 53

```
<Value>2001:0db8:85a3:0:0:8a2e:0370:7334</Value>
```

Type d'enregistrement CAA

Un enregistrement CAA indique quelles autorités de certification (CAs) sont autorisées à délivrer des certificats pour un domaine ou un sous-domaine. La création d'un enregistrement CAA permet d'éviter que des personnes mal CAs intentionnées ne délivrent des certificats pour vos domaines. Un enregistrement CAA ne se substitue pas exigences de sécurité formulées par votre autorité de certification, dont celle vous imposant de confirmer que vous êtes le propriétaire d'un domaine.

Vous pouvez utiliser des enregistrements CAA pour spécifier ce qui suit :

- Quelles autorités de certification (CAs) peuvent délivrer SSL/TLS des certificats, le cas échéant
- L'adresse e-mail ou l'URL à contacter quand une autorité de certification émet un certificat pour le domaine ou le sous-domaine

Lorsque vous ajoutez un enregistrement CAA à votre zone hébergée, vous devez spécifier trois paramètres séparés par des espaces :

```
flags tag "value"
```

Notez ce qui suit à propos du format des enregistrements CAA :

- La valeur de `tag` peut uniquement contenir les caractères A-Z, a-z et 0-9.
- Veillez à toujours placer `value` entre guillemets ("").
- Certains CAs autorisent ou exigent des valeurs supplémentaires pour`value`. Spécifiez les valeurs supplémentaires en tant que paires nom-valeur, en les séparant par des points-virgules (;), par exemple :

  ```
  0 issue "ca.example.net; account=123456"
  ```
- Si une autorité de certification reçoit une demande de certificat pour un sous-domaine (par exemple, www.example.com) et s'il n'existe aucun enregistrement CAA pour le sous-domaine, l'autorité de certification soumet une requête DNS portant sur un enregistrement CAA pour le domaine parent (comme example.com). S'il existe un enregistrement pour le domaine parent et si la demande de certificat est valide, l'autorité de certification émet le certificat pour le sous-domaine.
- Nous vous invitons à vous renseigner auprès de votre autorité de certification pour savoir quelles valeurs spécifier pour un enregistrement CAA.
- Vous ne pouvez pas créer un enregistrement CAA et un enregistrement CNAME ayant le même nom, car DNS ne permet pas d'utiliser le même nom pour un enregistrement CNAME et pour tout autre type d'enregistrement.

Rubriques

- Autoriser une autorité de certification à émettre un certificat pour un domaine ou un sous-domaine
- Autoriser une autorité de certification à émettre un certificat générique pour un domaine ou un sous-domaine
- Empêcher toute autorité de certification d'émettre un certificat pour un domaine ou sous-domaine
- Demander à n'importe quelle autorité de certification de vous contacter si elle reçoit une demande de certificat non valide
- Utiliser un autre paramètre pris en charge par l'autorité de certification
- Exemples

Autoriser une autorité de certification à émettre un certificat pour un domaine ou un sous-domaine

Pour autoriser une autorité de certification à émettre un certificat pour un domaine ou un sous-domaine, créez un enregistrement portant le même nom que le domaine ou sous-domaine, et spécifiez les paramètres suivants :

- flags (indicateurs) – `0`
- étiquette — `issue`
- value (valeur) – le code de l'autorité de certification que vous autorisez à émettre un certificat pour le domaine ou sous-domaine

Par exemple, supposons que vous voulez autoriser ca.example.net pour émettre un certificat pour exemple.com. Vous allez créer un enregistrement CAA pour exemple.com avec les paramètres suivants :

```
0 issue "ca.example.net"
```

Pour plus d'informations sur la façon AWS Certificate Manager d'autoriser l'émission d'un certificat, voir Configurer un enregistrement CAA dans le guide de AWS Certificate Manager l'utilisateur.

Autoriser une autorité de certification à émettre un certificat générique pour un domaine ou un sous-domaine

Pour autoriser une autorité de certification à émettre un certificat générique pour un domaine ou un sous-domaine, créez un enregistrement portant le même nom que le domaine ou sous-domaine, et

spécifiez les paramètres suivants. Un certificat générique s'applique au domaine ou sous-domaine et à tous ses sous-domaines.

- flags (indicateurs) – `0`
- étiquette — `issuewild`
- value (valeur) – le code de l'autorité de certification que vous autorisez à émettre un certificat pour le domaine ou le sous-domaine et ses sous-domaines

Par exemple, supposons que vous voulez autoriser ca.example.net à émettre un certificat générique pour example.com, qui s'applique à example.com et à l'ensemble de ses sous-domaines. Vous allez créer un enregistrement CAA pour exemple.com avec les paramètres suivants :

```
0 issuewild "ca.example.net"
```

Si vous souhaitez autoriser une autorité de certification à émettre un certificat générique pour un domaine ou un sous-domaine, créez un enregistrement portant le même nom que le domaine ou sous-domaine, et spécifiez les paramètres suivants. Un certificat générique s'applique au domaine ou sous-domaine et à tous ses sous-domaines.

Empêcher toute autorité de certification d'émettre un certificat pour un domaine ou sous-domaine

Pour empêcher une autorité de certification d'émettre un certificat générique pour un domaine ou un sous-domaine, créez un enregistrement portant le même nom que le domaine ou sous-domaine, et spécifiez les paramètres suivants :

- flags (indicateurs) – `0`
- étiquette — `issue`
- valeur – `";"`

Par exemple, supposons que vous ne voulez qu'aucune autorité de certification n'émette de certificat pour example.com. Vous allez créer un enregistrement CAA pour exemple.com avec les paramètres suivants :

`0 issue ";"`

Si vous ne voulez pas qu'une autorité de certification émette de certificat pour example.com ou ses sous-domaines, vous devez créer un enregistrement CAA pour example.com avec les paramètres suivants :

```
0 issuewild ";"
```

> **Note**
>
> Si vous créez un enregistrement CAA pour example.com et spécifiez les deux valeurs suivantes, une autorité de certification qui utilise la valeur ca.example.net peut émettre le certificat pour example.com :
>
> ```
> 0 issue ";"
> 0 issue "ca.example.net"
> ```

Demander à n'importe quelle autorité de certification de vous contacter si elle reçoit une demande de certificat non valide

Si vous souhaitez qu'une autorité de certification vous contacte si elle reçoit une demande de certificat non valide, spécifiez les paramètres suivants :

- flags (indicateurs) – `0`
- étiquette — `iodef`
- value (valeur) – l'URL ou l'adresse e-mail que vous souhaitez que l'autorité de certification contacte si elle reçoit une requête non valide demandant un certificat. Utilisez le format applicable :

  `"mailto:email-address"`

  `"http://URL"`

  `"https://URL"`

Par exemple, si vous voulez que toute autorité de certification qui reçoit une demande de certificat non valide envoie un e-mail à admin@example.com, vous devez créer un enregistrement CAA avec les paramètres suivants :

```
0 iodef "mailto:admin@example.com"
```

Utiliser un autre paramètre pris en charge par l'autorité de certification

Si votre autorité de certification prend en charge une fonctionnalité qui n'est pas définie dans la spécification RFC pour les enregistrements CAA, spécifiez les paramètres suivants :

- flags (indicateurs) – 128 (cette valeur empêche l'autorité de certification d'émettre un certificat si celle-ci ne prend pas en charge la fonction spécifiée.)
- tag (balise) – la balise que vous autorisez l'autorité de certification à utiliser
- value (valeur) – la valeur qui correspond à la valeur de tag

Par exemple, supposons que votre autorité de certification envoie un SMS si elle reçoit une demande de certificat non valide. (Nous n'en connaissons aucun CAs qui supporte cette option.) Les paramètres de l'enregistrement peuvent prendre la forme suivante :

```
128 exampletag "15555551212"
```

Exemples

Exemple pour la console Route 53

```
0 issue "ca.example.net"
0 iodef "mailto:admin@example.com"
```

Exemple pour l'API Route 53

```
<ResourceRecord>
   <Value>0 issue "ca.example.net"</Value>
   <Value>0 iodef "mailto:admin@example.com"</Value>
</ResourceRecord>
```

Type d'enregistrement CNAME

Un enregistrement CNAME mappe les requêtes DNS pour le nom de l'enregistrement actuel, comme acme.example.com, à un autre domaine (example.com ou example.net) ou sous-domaine (acme.example.com ou zenith.example.org).

> **Important**
>
> Le protocole DNS ne permet pas de créer un enregistrement CNAME pour le nœud supérieur d'un espace de nom DNS, également dénommé zone apex. Par exemple, si vous enregistrez le nom DNS example.com, la zone apex est example.com. Vous ne pouvez pas créer un enregistrement CNAME pour example.com, mais vous pouvez créer des enregistrements CNAME pour www.example.com, newproduct.example.com, etc.

En outre, si vous créez un enregistrement CNAME pour un sous-domaine, vous ne pouvez pas créer d'autres enregistrements pour ce sous-domaine. Par exemple, si vous créez un enregistrement CNAME pour www.example.com, vous ne pouvez pas créer d'autres enregistrements dont la valeur du champ Name (nom) est www.example.com.

Amazon Route 53 prend également en charge les enregistrements d'alias, qui vous permettent d'acheminer les requêtes vers AWS des ressources sélectionnées, telles que CloudFront les distributions et les compartiments Amazon S3. Les alias sont relativement similaires au type d'enregistrement CNAME. Cependant, vous pouvez créer un alias pour la zone apex. Pour de plus amples informations, veuillez consulter Choix entre des enregistrements avec ou sans alias.

Exemple pour la console Route 53

```
hostname.example.com
```

Exemple pour l'API Route 53

```
<Value>hostname.example.com</Value>
```

Type d'enregistrement DS

Un enregistrement de signataire de délégation (DS) fait référence à une clé de zone pour une zone de sous-domaine déléguée. Vous pouvez créer un enregistrement DS lorsque vous établissez une chaîne d'approbation lorsque vous configurez la signature DNSSEC. Pour plus d'informations sur la configuration DNSSEC dans Route 53, consultez Configuration de la signature DNSSEC dans Amazon Route 53.

Les trois premières valeurs sont des nombres décimaux représentant la balise clé, l'algorithme et le type de prétraitement. La quatrième valeur est le prétraitement de la clé de zone. Pour plus de détails sur le format d'enregistrement DS, consultez la spécification RFC 4034.

Exemple pour la console Route 53

```
123 4 5 1234567890abcdef1234567890absdef
```

Exemple pour l'API Route 53

```
<Value>123 4 5 1234567890abcdef1234567890absdef</Value>
```

Type d'enregistrement HTTPS

Un enregistrement de ressource HTTPS est une forme d'enregistrement DNS SVCB (Service Binding) qui fournit des informations de configuration étendues, permettant à un client de se connecter facilement et en toute sécurité à un service via un protocole HTTP. Les informations de configuration sont fournies dans des paramètres qui permettent la connexion en une seule requête DNS, plutôt que de nécessiter plusieurs requêtes DNS.

Le format d'un enregistrement de ressource HTTPS est le suivant :

```
SvcPriority TargetName SvcParams(optional)
```

Les paramètres suivants sont décrits dans la RFC 9460, section 9.1.

SvcPriority

Un entier qui représente la priorité. La priorité 0 signifie le mode alias et est généralement destiné à l'alias au sommet de la zone. Cette valeur est un entier compris entre 0 et 32767 pour Route 53, dont 1 à 32767 sont des enregistrements en mode service. Plus la priorité est faible, plus la préférence est élevée.

TargetName

Le nom de domaine de l'alias cible (pour le mode alias) ou du point de terminaison alternatif (pourServiceMode).

SvcParams (facultatif)

Une liste séparée par des espaces, chaque paramètre étant constitué d'une paire Key=Value ou d'une clé autonome. S'il existe plusieurs valeurs, elles sont présentées sous forme de liste séparée par des virgules. Les éléments suivants sont définis SvcParams :

- `1:alpn`— Protocole de négociation du protocole de couche application IDs. La valeur par défaut est HTTP/1.1, h2 HTTP/2 sur TLS et h3 HTTP/3 (protocole HTTP sur QUIC).
- `2:no-default-alpn`— La valeur par défaut n'est pas prise en charge et vous devez fournir un `alpn` paramètre.
- `3:port`— le point de terminaison alternatif ou le port où le service peut être atteint.
- `4:ipv4hint`— indications IPv4 d'adresse.
- `5:ech`— Client crypté Bonjour.
- `6:ipv6hint`— indications IPv6 d'adresse.
- `7:dohpath`— Modèle DNS sur HTTPS

- `8:ohttp`— Le service utilise une cible HTTP Oblivious

Exemple pour la console Amazon Route 53 en mode alias

```
0 example.com
```

Exemple pour la console Amazon Route 53 en mode service

```
16 example.com alpn="h2,h3" port=808
```

Exemple d'API Amazon Route 53 pour le mode alias

```
<Value>0 example.com</Value>
```

Exemple d'API Route 53 pour le mode service

```
<Value>16 example.com alpn="h2,h3" port=808</Value>
```

Pour plus d'informations, consultez la RFC 9460, Liaison de service et spécification des paramètres via le DNS (enregistrements de ressources SVCB et HTTPS).

> **Note**
>
> Route 53 ne prend pas en charge le format de présentation arbitraire à clé inconnue `keyNNNNN`

Type d'enregistrement MX

Un enregistrement MX spécifie les noms de vos serveurs de messagerie et, si vous disposez de plusieurs serveurs de messagerie, l'ordre de priorité. Chaque valeur d'un enregistrement MX contient deux valeurs, la priorité et le nom de domaine.

Priorité

Un nombre entier qui représente la priorité pour un serveur de messagerie. Si vous ne spécifiez qu'un seul serveur, la priorité peut être n'importe quel nombre entier compris entre 0 et 65 535. Si vous spécifiez plusieurs serveurs, la valeur que vous spécifiez pour la priorité indique vers quel serveur de messagerie vous voulez que les e-mails soient acheminés en premier, en deuxième,

et ainsi de suite. Le serveur avec la valeur de priorité la plus basse est prioritaire. Par exemple, si vous avez deux serveurs de messagerie et que vous spécifiez les valeurs de priorité 10 et 20, les e-mails vont toujours vers le serveur qui a la priorité 10, sauf s'il n'est pas disponible. Si vous spécifiez les valeurs 10 et 10, les e-mails sont acheminés vers les deux serveurs de façon relativement équitable.

Nom de domaine

Le nom de domaine du serveur de messagerie. Spécifiez le nom (par exemple mail.example.com) d'un enregistrement A ou AAAA. Dans RFC 2181, Clarifications to the DNS Specification, la section 10.3 interdit de spécifier le nom d'un enregistrement CNAME pour la valeur du nom de domaine. (Lorsque le RFC indique « alias », cela indique un enregistrement CNAME, et non un enregistrement d'alias Route 53.)

Exemple pour la console Amazon Route 53

```
10 mail.example.com
```

Exemple pour l'API Route 53

```
<Value>10 mail.example.com</Value>
```

Type d'enregistrement NAPTR

Un pointeur d'autorité de nom (NAPTR) est un type d'enregistrement qui est utilisé par les applications DDDS (Dynamic Delegation Discovery System) pour convertir une valeur en une autre ou remplacer une valeur par une autre. Par exemple, une utilisation courante consiste à convertir des numéros de téléphone en SIP URIs.

L'élément `Value` d'un enregistrement NAPTR se compose de six valeurs séparées par des espaces :

Ordre

Lorsque vous spécifiez plusieurs enregistrements, l'ordre dans lequel vous souhaitez que l'application DDDS évalue les enregistrements. Valeurs valides : 0 - 65535.

Préférence

Lorsque vous spécifiez deux ou plusieurs enregistrements ayant le même ordre, votre préférence pour l'ordre dans lequel ces enregistrements sont évalués. Par exemple, si deux enregistrements

ont un ordre de 1, l'application DDDS évalue d'abord l'enregistrement ayant la préférence la plus basse. Valeurs valides : 0 - 65535.

Indicateurs

Paramètre spécifique aux applications DDDS. Les valeurs actuellement définies dans RFC 3404 sont les lettres « A », « P », « S » et « U » en majuscules et minuscules et la chaîne vide, « ». Placez les indicateurs entre guillemets.

Service

Paramètre spécifique aux applications DDDS. Placez le service entre guillemets.

Pour plus d'informations, consultez le document applicable RFCs :

- Application DDDS URI — https://tools.ietf.org/html/rfc3404 #section -4.4
- Application DDDS S-NAPTR — /rfc3958 #section -6.5 https://tools.ietf.org/html
- Application DDDS U-NAPTR — /rfc4848 #section -4.5 https://tools.ietf.org/html

Regexp

Expression régulière que l'application DDDS utilise pour convertir une valeur d'entrée en une valeur de sortie. Par exemple, un système de téléphonie IP peut utiliser une expression régulière pour convertir un numéro de téléphone qui est entré par un utilisateur en une URI SIP. Placez Regexp entre guillemets. Spécifiez une valeur pour Regexp ou Remplacement, mais pas les deux.

L'expression régulière peut inclure les caractères ASCII imprimables suivants :

- a-z
- 0-9
- - (trait d'union)
- (espace)
- ! # $ % & ' ( ) * + , - / : ; < = > ? @ [ ] ^ _ ` { | } ~ .
- " (guillemet). Pour inclure un guillemet dans une chaîne, faites-le précéder par un caractère \ : \".
- \ (barre oblique inverse). Pour inclure une barre oblique inverse dans une chaîne, faites-la précéder par un caractère \ : \\.

Spécifiez toutes les autres valeurs, telles que les noms de domaine internationaux, au format octal.

Pour la syntaxe de Regexp, consultez la RFC 3402, section 3.2, Substitution Expression Syntax

Remplacement

Le nom de domaine complet (FQDN) du prochain nom de domaine pour lequel vous souhaitez que l'application DDDS soumettre une requête DNS. L'application DDDS remplace la valeur d'entrée par la valeur que vous spécifiez dans Remplacement, le cas échéant. Spécifiez une valeur pour Regexp ou Remplacement, mais pas les deux. Si vous indiquez une valeur pour Regexp, spécifiez un point (.) pour Remplacement.

Le nom de domaine peut inclure a-z, 0-9 et - (tiret).

Pour plus d'informations sur les applications DDDS et sur les enregistrements NAPTR, consultez les rubriques suivantes : RFCs

- RFC 3401
- RFC 3402
- RFC 3403
- RFC 3404

Exemple pour la console Amazon Route 53

```
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!" .
```

Exemple pour l'API Route 53

```
<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>
```

Type d'enregistrement NS

Un enregistrement NS identifie les serveurs de noms de la zone hébergée. Remarques :

- L'utilisation la plus courante d'un enregistrement NS consiste à contrôler le routage du trafic Internet pour un domaine. Pour utiliser les enregistrements d'une zone hébergée pour acheminer le trafic d'un domaine, vous mettez à jour les paramètres d'enregistrement de domaine pour utiliser les quatre serveurs de noms dans l'enregistrement NS par défaut. (Il s'agit de l'enregistrement NS portant le même nom que la zone hébergée.)
- Vous pouvez créer une zone hébergée distincte pour un sous-domaine (acme.example.com) et utiliser cette zone hébergée pour acheminer le trafic Internet pour le sous-domaine et ses sous-domaines (subdomain.acme.example.com). Vous définissez cette configuration, qualifiée de « délégation de la responsabilité d'un sous-domaine à une zone hébergée » en créant un autre enregistrement NS dans la zone hébergée pour le domaine racine (example.com). Pour de plus amples informations, veuillez consulter Acheminement du trafic pour les sous-domaines.
- Vous utilisez également des enregistrements NS pour configurer des serveurs de noms en marque blanche. Pour de plus amples informations, veuillez consulter Configuration de serveurs de noms en marque blanche.
- Un enregistrement NS peut également être utilisé pour les zones hébergées privées lorsque vous créez une règle de délégation pour déléguer l'autorité d'un sous-domaine à votre résolveur local. Vous devez créer cet enregistrement NS avant de créer une règle de délégation. Pour de plus amples informations, veuillez consulter Comment le point de terminaison Route 53 Resolver transfère les requêtes DNS de vous VPCs vers votre réseau.

Pour plus d'informations sur les enregistrements NS, consultez la section Registres NS et SOA créés par Amazon Route 53 pour une zone hébergée publique.

Exemple pour la console Amazon Route 53

```
ns-1.example.com
```

Exemple pour l'API Route 53

```
<Value>ns-1.example.com</Value>
```

Type d'enregistrement PTR

Un enregistrement PTR mappe une adresse IP au nom de domaine correspondant.

Exemple pour la console Amazon Route 53

```
hostname.example.com
```

Exemple pour l'API Route 53

```
<Value>hostname.example.com</Value>
```

Type d'enregistrement SOA

Un enregistrement de source de noms (SOA) fournit des informations concernant un domaine et la zone hébergée Amazon Route 53. Pour plus d'informations sur les champs d'un enregistrement SOA, consultez Registres NS et SOA créés par Amazon Route 53 pour une zone hébergée publique.

Exemple pour la console Route 53

```
ns-2048.awsdns-64.net hostmaster.awsdns.com 1 1 1 1 60
```

Exemple pour l'API Route 53

```
<Value>ns-2048.awsdns-64.net hostmaster.awsdns.com 1 1 1 1 60</Value>
```

Type d'enregistrement SPF

Auparavant, les enregistrements SPF étaient utilisés pour vérifier l'identité de l'expéditeur d'e-mails. Toutefois, nous vous recommandons de ne plus créer d'enregistrements pour lesquels le type d'enregistrement est SPF. La RFC 7208, Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, version 1, a été mise à jour pour indiquer : «... [L] 'existence et le mécanisme définis dans [RFC4408] ont entraîné certains problèmes d'interopérabilité. Accordingly, its use is no longer appropriate for SPF version 1; implementations are not to use it. » Dans la norme RFC 7208, consultez la section 14.1 The SPF DNS Record Type.

Plutôt que de créer un enregistrement SPF, nous vous recommandons de créer un enregistrement TXT contenant la valeur applicable. Pour plus d'informations sur les valeurs valides, consultez l'article Wikipédia Sender Policy Framework.

Exemple pour la console Amazon Route 53

```
"v=spf1 ip4:192.168.0.1/16 -all"
```

Exemple pour l'API Route 53

```
<Value>"v=spf1 ip4:192.168.0.1/16 -all"</Value>
```

Type d'enregistrement SRV

Un élément `Value` d'un enregistrement SRV se compose de quatre valeurs séparées par des espaces. Les trois premières valeurs sont des nombres décimaux représentant la priorité, la pondération et le port. La quatrième valeur est un nom de domaine. Les enregistrements SRV sont utilisés pour accéder à des services, tels qu'un service pour le courrier électronique ou les communications. Pour plus d'informations sur le format d'enregistrement SRV, consultez la documentation du service auquel vous souhaitez vous connecter.

Exemple pour la console Amazon Route 53

```
10 5 80 hostname.example.com
```

Exemple pour l'API Route 53

```
<Value>10 5 80 hostname.example.com</Value>
```

Type d'enregistrement SSHFP

Un enregistrement d'empreintes digitales Secure Shell (SSHFP) identifie les clés SSH associées au nom de domaine. Les enregistrements SSHFP doivent être sécurisés par le protocole DNSSEC pour qu'une chaîne de confiance soit établie. Pour plus d'informations sur le protocole DNSSEC, voir Configuration de la signature DNSSEC dans Amazon Route 53

Le format d'un enregistrement de ressource SSHFP est le suivant :

```
[Key Algorithm] [Hash Type] Fingerprint
```

Les paramètres suivants sont définis dans la RFC 4255.

Algorithme clé

Type d'algorithme :

- `0`— Réservé et non utilisé.
- `1: RSA`— L'algorithme Rivest-Shamir-Adleman est l'un des premiers systèmes cryptographiques à clé publique et est toujours utilisé pour la transmission sécurisée de données.

- `2: DSA`— L'algorithme de signature numérique est une norme fédérale de traitement de l'information pour les signatures numériques. Le DSA est basé sur l'exponentiation modulaire et les modèles mathématiques du logarithme discret.
- `3: ECDSA`— L'algorithme de signature numérique à courbe elliptique est une variante du DSA qui utilise la cryptographie à courbe elliptique.
- `4: Ed25519`— L'algorithme Ed25519 est le schéma de signature eDDSA qui utilise SHA-512 (SHA-2) et Curve25519.
- `6: Ed448`— Ed448 est le schéma de signature eDDSA qui utilise et Curve448. SHAKE256

Type de hachage

Algorithme utilisé pour créer le hachage de la clé publique :

- `0`—Réservé et non utilisé.
- `1: SHA-1`
- `2: SHA-256`

Empreinte digitale

Représentation hexadécimale du hachage.

Exemple pour la console Amazon Route 53

```
1 1 09F6A01D2175742B257C6B98B7C72C44C4040683
```

Exemple pour l'API Route 53

```
<Value>1 1 09F6A01D2175742B257C6B98B7C72C44C4040683</Value>
```

Pour plus d'informations, consultez la RFC 4255 : Utilisation du DNS pour publier en toute sécurité les empreintes clés du protocole Secure Shell (SSH).

Type d'enregistrement SVCB

Vous utilisez un enregistrement SVCB pour fournir des informations de configuration permettant d'accéder aux points de terminaison du service. Le SVCB est un enregistrement DNS générique qui peut être utilisé pour négocier les paramètres de divers protocoles d'application.

Le format d'un enregistrement de ressource SVCB est le suivant :

`SvcPriority TargetName SvcParams(optional)`

Les paramètres suivants sont décrits dans la RFC 9460, section 2.3.

SvcPriority

Un entier qui représente la priorité. La priorité 0 signifie le mode alias et est généralement destiné à l'alias au sommet de la zone. Plus la priorité est faible, plus la préférence est élevée.

TargetName

Le nom de domaine de l'alias cible (pour le mode alias) ou du point de terminaison alternatif (pourServiceMode).

SvcParams (facultatif)

Une liste séparée par des espaces, chaque paramètre étant constitué d'une paire Key=Value ou d'une clé autonome. S'il existe plusieurs valeurs, elles sont présentées sous forme de liste séparée par des virgules. Cette valeur est un entier compris entre 0 et 32767 pour Route 53, dont 1 à 32767 sont des enregistrements en mode service. Les éléments suivants sont définis SvcParams :

- `1:alpn`— Protocole de négociation du protocole de couche application IDs. La valeur par défaut est HTTP/1.1, h2 HTTP/2 sur TLS et h3 HTTP/3 (protocole HTTP sur QUIC).
- `2:no-default-alpn`— La valeur par défaut n'est pas prise en charge et vous devez fournir un `alpn` paramètre.
- `3:port`— le port de l'autre point de terminaison où le service peut être atteint.
- `4:ipv4hint`— indications IPv4 d'adresse.
- `5:ech`— Client crypté Bonjour.
- `6:ipv6hint`— indications IPv6 d'adresse.
- `7:dohpath`— Modèle DNS sur HTTPS
- `8:ohttp`— Le service utilise une cible HTTP Oblivious

Exemple pour la console Amazon Route 53 en mode alias

```
0 example.com
```

Exemple pour la console Amazon Route 53 en mode service

```
16 example.com alpn="h2,h3" port=808
```

Exemple d'API Amazon Route 53 pour le mode alias

```
<Value>0 example.com</Value>
```

Exemple d'API Route 53 pour le mode service

```
<Value>16 example.com alpn="h2,h3" port=808</Value>
```

Pour plus d'informations, consultez la RFC 9460, Liaison de service et spécification des paramètres via le DNS (enregistrements de ressources SVCB et HTTPS).

> **Note**
>
> Route 53 ne prend pas en charge le format de présentation arbitraire à clé inconnue `keyNNNNN`

Type d'enregistrement TLSA

Vous utilisez un enregistrement TLSA pour utiliser l'authentification des entités nommées (DANE) basée sur le DNS. Un enregistrement TLSA associe une certificate/public clé à un point de terminaison TLS (Transport Layer Security), et les clients peuvent valider la certificate/public clé à l'aide d'un enregistrement TLSA signé avec DNSSEC.

Les enregistrements TLSA ne sont fiables que si le protocole DNSSEC est activé sur votre domaine. Pour plus d'informations sur le protocole DNSSEC, voir Configuration de la signature DNSSEC dans Amazon Route 53

Le format d'un enregistrement de ressource TLSA est le suivant :

```
[Certificate usage] Selector [Matching type] [Certificate association data]
```

Les paramètres suivants sont spécifiés dans la RFC 6698, section 3.

Utilisation des certificats

Spécifie l'association fournie qui sera utilisée pour correspondre au certificat présenté dans le handshake TLS :

- 0 : contrainte CA — Le certificat ou la clé publique doit se trouver dans l'un des chemins de certification de l'infrastructure à clé publique (PKIX) pour le certificat d'entité finale fourni par le serveur dans TLS. Cette contrainte limite ce qui CAs peut être utilisé pour émettre des certificats pour un service spécifique.
- 1 : Contrainte de certificat de service — Spécifie un certificat d'entité finale (ou la clé publique) qui doit correspondre au certificat d'entité finale fourni par le serveur dans TLS. Cette certification limite le certificat d'entité finale qui peut être utilisé par un service spécifique sur un hôte.
- 2 : Une assertion d'ancrage de confiance — Spécifie un certificat (ou la clé publique) qui doit être utilisé comme « ancre de confiance » lors de la validation du certificat d'entité finale fourni par le serveur dans TLS. Permet à un administrateur de domaine de spécifier une ancre de confiance.
- 3 : Certification délivrée par le domaine — Spécifie un certificat (ou la clé publique) qui doit correspondre au certificat d'entité finale fourni par le serveur dans TLS. Cette certification permet à un administrateur de domaine d'émettre des certificats pour un domaine sans faire appel à une autorité de certification tierce. Ce certificat n'a pas besoin de passer la validation PKIX.

Selector

Spécifie la partie du certificat présentée par le serveur lors de la poignée de main qui correspond à la valeur de l'association :

- 0 : L'intégralité du certificat doit correspondre.
- 1 : La clé publique du sujet, ou la structure binaire codée DER, doit correspondre.

Type correspondant

Spécifie la présentation (telle que déterminée par le champ de sélection) du certificat correspondant :

- 0 : Correspondance exacte du contenu.
- 1 : hachage SHA-256.
- 2 : hachage SHA-512.

Données d'association de certificats

Les données à comparer en fonction des paramètres des autres champs.

Exemple pour la console Amazon Route 53

```
0 0 1 d2abde240d7cd3ee6b4b28c54df034b97983a1d16e8a410e4561cb106618e971
```

Exemple pour l'API Route 53

```
<Value>0 0 1 d2abde240d7cd3ee6b4b28c54df034b97983a1d16e8a410e4561cb106618e971</Value>
```

Pour plus d'informations, consultez la RFC 6698, Protocole de sécurité de la couche de transport (TLS) basé sur le DNS pour l'authentification des entités nommées (DANE) : TLSA.

Type d'enregistrement TXT

Un enregistrement TXT contient une ou plusieurs chaînes entre guillemets doubles ("). Lorsque vous utilisez la stratégie de routage simple, incluez toutes les valeurs d'un domaine (example.com) ou d'un sous-domaine (www.example.com) dans le même enregistrement TXT.

Rubriques

- Saisie des valeurs d'enregistrement TXT
- Caractères spéciaux dans une valeur d'enregistrement TXT
- Majuscules et minuscules dans une valeur d'enregistrement TXT
- Exemples

Saisie des valeurs d'enregistrement TXT

Une seule chaîne peut contenir jusqu'à 255 caractères des types suivants :

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

Si vous devez entrer une valeur supérieure à 255 caractères, divisez-la en chaînes de 255 caractères ou moins et placez chaque chaîne entre guillemets doubles ("). Dans la console, listez toutes les chaînes sur la même ligne :

```
"String 1" "String 2" "String 3"
```

Pour l'API, incluez toutes les chaînes dans le même élément `Value` :

```
<Value>"String 1" "String 2" "String 3"</Value>
```

La longueur maximale d'une valeur dans un enregistrement TXT est de 4 000 caractères.

Pour entrer plusieurs valeurs TXT, entrez une valeur par ligne.

Caractères spéciaux dans une valeur d'enregistrement TXT

Si votre enregistrement TXT contient l'un des caractères suivants, vous devez spécifier les caractères en utilisant des codes d'échappement au format `\` *`three-digit octal code`* :

- Caractères 000 à 040 octal (0 à 32 décimal, 0x00 à 0x20 hexadécimal)
- Caractères 177 à 377 octal (127 à 255 décimal, 0x7F à 0xFF hexadécimal)

Par exemple, si la valeur de votre enregistrement TXT est `"exämple.com"`, vous devez spécifier `"ex\344mple.com"`.

Pour établir un mappage entre les caractères ASCII et les codes octaux, effectuez une recherche sur Internet pour trouver des « codes octaux ASCII ». La référence ASCII Code - The extended ASCII table peut vous être utile.

Pour inclure un guillemet (`"`) dans une chaîne, placez une barre oblique inversée (`\`) avant le guillemet : `\"`.

Majuscules et minuscules dans une valeur d'enregistrement TXT

La casse étant conservée, `"Ab"` et `"aB"` sont des valeurs différentes.

Exemples

Exemple pour la console Amazon Route 53

Placez chaque valeur sur une ligne distincte :

```
"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"
```

Exemple pour l'API Route 53

Placez chaque valeur dans un élément `Value` distinct :

```
<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>
```

Création d'enregistrements à l'aide de la console Amazon Route 53

La procédure suivante explique comment créer des enregistrements à l'aide de la console Amazon Route 53. Pour plus d'informations sur la création d'enregistrements à l'aide de l'API Route 53, consultez ChangeResourceRecordSetsle manuel Amazon Route 53 API Reference.

> **Note**
>
> Pour créer des enregistrements pour des configurations de routage complexes, vous pouvez également utiliser l'éditeur visuel Traffic Flow et enregistrer la configuration en tant que politique de trafic. Vous pouvez ensuite associer la stratégie de trafic à un ou plusieurs noms de domaine (par exemple, example.com) ou noms de sous-domaine (par exemple, www.example.com), dans la même zone hébergée ou dans plusieurs zones hébergées. En outre, vous pouvez restaurer les mises à jour si la nouvelle configuration ne fonctionne pas comme vous l'aviez prévu. Pour de plus amples informations, veuillez consulter Utiliser Traffic Flow pour acheminer le trafic DNS.

Pour créer un enregistrement à l'aide de la console Route 53

1. Si vous ne créez pas d'enregistrement d'alias, passez à l'étape 2.

   Passez également à l'étape 2 si vous créez un enregistrement d'alias qui achemine le trafic DNS vers une AWS ressource autre qu'un équilibreur de charge Elastic Load Balancing ou un autre enregistrement Route 53.

   Si vous créez un enregistrement d'alias qui achemine le trafic vers un équilibreur de charge Elastic Load Balancing, et si vous avez créé votre zone hébergée et votre équilibreur de charge

à l'aide de différents comptes, exécutez la procédure Obtention du nom DNS d'un équilibreur de charge Elastic Load Balancing pour obtenir le nom DNS de l'équilibreur de charge.

2. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
3. Dans le panneau de navigation, choisissez Zones hébergées.
4. Si vous disposez déjà d'une zone hébergée pour votre domaine, passez à l'étape 5. Si ce n'est pas le cas, exécutez la procédure applicable pour créer une zone hébergée :
   - Pour acheminer le trafic Internet vers vos ressources, telles que les compartiments Amazon S3 ou les EC2 instances Amazon, consultezCréation d'une zone hébergée publique.
   - Pour acheminer le trafic dans votre VPC, consultez Création d'une zone hébergée privée.
5. Sur la page Hosted zones (Zones hébergées), choisissez le nom de la zone hébergée dans laquelle vous voulez créer des enregistrements.
6. Choisissez Créer un registre.
7. Choisissez et définissez la stratégie de routage et les valeurs applicables. Pour plus d'informations, consultez la rubrique pour le type d'enregistrement que vous souhaitez créer :
   - Valeurs communes à toutes les politiques de routage
   - Valeurs communes aux enregistrements d'alias pour toutes les politiques de routage
   - Valeurs spécifiques aux enregistrements simples
   - Valeurs spécifiques aux enregistrements d'alias simples
   - Valeurs spécifiques aux enregistrements de basculement
   - Valeurs spécifiques aux enregistrements d'alias de basculement
   - Valeurs spécifiques aux enregistrements de géolocalisation
   - Valeurs spécifiques aux enregistrements d'alias de géolocalisation
   - Valeurs spécifiques aux enregistrements de géoproximité
   - Valeurs spécifiques aux enregistrements d'alias de géoproximité
   - Valeurs spécifiques aux enregistrements de latence
   - Valeurs spécifiques aux enregistrements d'alias de latence
   - Valeurs spécifiques aux enregistrements basés sur IP
   - Valeurs spécifiques aux enregistrements d'alias basés sur IP
   - Valeurs spécifiques pour les enregistrements de réponses multivaleur
   - Valeurs spécifiques aux enregistrements pondérés

- Valeurs spécifiques aux enregistrements d'alias pondérés

8. Choisissez Créer des enregistrements.

> **Note**
>
> La propagation de vos nouveaux registres sur les serveurs DNS Route 53 prend un certain temps. À l'heure actuelle, le seul moyen de vérifier que les modifications se sont propagées consiste à utiliser l'action GetChangeAPI. Les changements se propagent généralement sur tous les serveurs de Route 53 en 60 secondes.

9. Si vous créez plusieurs enregistrements, répétez les étapes 7 à 8.

Obtention du nom DNS d'un équilibreur de charge Elastic Load Balancing

1. Connectez-vous à l' AWS Management Console aide du AWS compte qui a été utilisé pour créer le Classic, l'Application ou le Network Load Balancer pour lequel vous souhaitez créer un enregistrement d'alias.
2. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
3. Dans le volet de navigation, choisissez Load Balancers.
4. Dans la liste des équilibreurs de charge, sélectionnez celui pour lequel vous souhaitez créer un enregistrement d'alias.
5. Dans l'onglet Description, obtenez la valeur de DNS name.
6. Si vous souhaitez créer des enregistrements d'alias pour d'autres équilibreurs de charge Elastic Load Balancing, répétez les étapes 4 et 5.
7. Déconnectez-vous du AWS Management Console.
8. Connectez-vous à AWS Management Console nouveau à l'aide du AWS compte que vous avez utilisé pour créer la zone hébergée Route 53.
9. Revenez à l'étape 3 de la procédure Création d'enregistrements à l'aide de la console Amazon Route 53.

Autorisations relatives aux ensembles d'enregistrements

Les autorisations relatives aux ensembles d'enregistrements de ressources utilisent les conditions de politique de gestion des identités et des accès (IAM) pour vous permettre de définir des

autorisations granulaires pour les actions sur la console Route 53 ou pour l'utilisation de l'ChangeResourceRecordSetsAPI.

Un ensembles d'enregistrements de ressources est défini comme plusieurs enregistrements de ressources portant le même nom et le même type (et la même classe, mais dans la plupart des cas, la classe est toujours IN ou Internet), cependant ils contiennent des données différentes. Par exemple, si vous choisissez le routage de géolocalisation, vous pouvez avoir plusieurs enregistrements A ou AAAA pointant vers différents points de terminaison pour le même domaine. Tous ces enregistrements A ou AAAA se combinent pour former un ensemble d'enregistrements de ressources. Pour plus d'informations sur la terminologie DNS, consultez RFC 7719.

Avec les conditions de la politique IAM,, `route53:ChangeResourceRecordSetsNormalizedRecordNamesroute53:ChangeResourceRecor` `etroute53:ChangeResourceRecordSetsActions`, vous pouvez accorder des droits administratifs granulaires à d'autres AWS utilisateurs sur n'importe quel autre AWS compte. Cela vous permet d'accorder à quelqu'un les autorisations nécessaires pour :

- un ensemble d'enregistrements de ressource unique ;
- tous les ensembles d'enregistrements de ressources d'un type d'enregistrement DNS spécifique ;
- des ensembles d'enregistrements de ressources dont les noms contiennent une chaîne spécifique.
- Effectuez une ou toutes les `CREATE | UPSERT | DELETE` actions lorsque vous utilisez l'ChangeResourceRecordSetsAPI ou la console Route 53.

Vous pouvez également créer des autorisations d'accès qui combinent toutes les conditions de politique de Route 53. Par exemple, vous pouvez accorder à quelqu'un l'autorisation de modifier les données de l'enregistrement A pour marketing-example.com, mais ne pas autoriser cet utilisateur à supprimer des enregistrements.

Pour plus d'informations sur les autorisations relatives aux ensembles d'enregistrements de ressources et pour des exemples de leur utilisation, consultezUtilisation de conditions de politique IAM pour un contrôle d'accès précis.

Pour savoir comment authentifier AWS les utilisateurs, consultez Authentification par des identités et pour savoir comment contrôler l'accès aux ressources Route 53, voirContrôle d'accès.

Valeurs à spécifier lorsque vous créez ou modifiez des enregistrements Amazon Route 53

Lorsque vous créez des enregistrements à l'aide de la console Amazon Route 53, les valeurs que vous spécifiez dépendent de la politique de routage que vous souhaitez utiliser et du fait que vous créez ou non des enregistrements d'alias, qui acheminent le trafic vers les AWS ressources.

Enregistrements d'alias qui acheminent le trafic vers certaines AWS ressources pour lesquelles vous spécifiez la ressource cible (par exemple, Elastic Load Balancing, CloudFront distribution, compartiment Amazon S3). Vous pouvez également éventuellement associer des contrôles de santé et configurer une évaluation de l'état cible. Les rubriques suivantes fournissent des informations détaillées sur les valeurs requises pour chaque politique de routage et chaque type d'enregistrement, afin de vous aider à configurer efficacement vos enregistrements Route 53.

Rubriques

- Valeurs communes à toutes les politiques de routage
- Valeurs communes aux enregistrements d'alias pour toutes les politiques de routage
- Valeurs spécifiques aux enregistrements simples
- Valeurs spécifiques aux enregistrements d'alias simples
- Valeurs spécifiques aux enregistrements de basculement
- Valeurs spécifiques aux enregistrements d'alias de basculement
- Valeurs spécifiques aux enregistrements de géolocalisation
- Valeurs spécifiques aux enregistrements d'alias de géolocalisation
- Valeurs spécifiques aux enregistrements de géoproximité
- Valeurs spécifiques aux enregistrements d'alias de géoproximité
- Valeurs spécifiques aux enregistrements de latence
- Valeurs spécifiques aux enregistrements d'alias de latence
- Valeurs spécifiques aux enregistrements basés sur IP
- Valeurs spécifiques aux enregistrements d'alias basés sur IP
- Valeurs spécifiques pour les enregistrements de réponses multivaleur
- Valeurs spécifiques aux enregistrements pondérés
- Valeurs spécifiques aux enregistrements d'alias pondérés

Valeurs communes à toutes les politiques de routage

Ce sont les valeurs communes que vous pouvez spécifier lorsque vous créez ou modifiez des enregistrements Amazon Route 53. Ces valeurs sont utilisées par toutes les politiques de routage.

Rubriques

- Nom de l'enregistrement
- Valeur/acheminer le trafic vers
- TTL (secondes)

Nom de l'enregistrement

Saisissez le nom de domaine ou de sous-domaine vers lequel vous souhaitez acheminer le trafic. La valeur par défaut est le nom de la zone hébergée.

> **Note**
>
> Si vous créez un enregistrement qui porte le même nom que la zone hébergée, n'entrez aucune valeur (par exemple, un symbole @) dans le champ Name (Nom).

Enregistrements CNAME

Si vous créez un enregistrement dont la valeur est CNAME pour Record type (Type d'enregistrement), le nom de l'enregistrement ne peut être identique à celui de la zone hébergée.

Caractères spéciaux

Pour plus d'informations sur la spécification d'autres caractères que a-z, 0-9 et - (trait d'union), et de noms de domaine internationaux, consultez Format de nom de domaine DNS.

Caractères génériques

Vous pouvez utiliser un astérisque (*) dans le nom. DNS traite le caractère * comme un caractère générique ou comme le caractère * (ASCII 42), en fonction de son emplacement dans le nom. Pour de plus amples informations, veuillez consulter Utilisation d'un astérisque (*) dans les noms des zones hébergées et des enregistrements.

> **Important**
>
> Vous ne pouvez pas utiliser le caractère générique * pour les jeux d'enregistrements de ressources de type NS.

Valeur/acheminer le trafic vers

Choisissez IP address or another value depending on the record type (Adresse IP ou autre valeur selon le type d'enregistrement). Entrez une valeur appropriée pour la valeur Record type (Type d'enregistrement). Pour tous les types à l'exception de CNAME, vous pouvez entrer plusieurs valeurs. Entrez chaque valeur sur une ligne distincte.

A — IPv4 adresse

Adresse IP au IPv4 format 192.0.2.235, par exemple.

AAAA — adresse IPv6

Une adresse IP au IPv6 format, par exemple, 2001:0 db 8:85 a 3:0:0:8 a2e : 0370:7334.

CAA — Autorisation de l'autorité de certification

Trois valeurs séparées par un espace qui contrôlent les autorités de certification qui sont autorisées à émettre des certificats ou des certificats génériques pour le domaine ou le sous-domaine spécifié par Record name (Nom de l'enregistrement). Vous pouvez utiliser des enregistrements CAA pour spécifier ce qui suit :

- Quelles autorités de certification (CAs) peuvent délivrer des certificats SSL/TLS, le cas échéant
- L'adresse e-mail ou l'URL à contacter quand une autorité de certification émet un certificat pour le domaine ou le sous-domaine

CNAME — Nom canonique

Nom de domaine complet (par exemple, www.exemple.com) que Route 53 doit renvoyer en réponse à des requêtes DNS pour cet enregistrement. Un point final est facultatif. Route 53 part du principe que le nom de domaine est complet. Cela signifie que Route 53 traite www.example.com (sans point final) et www.example.com. (avec un point final) de la même façon.

MX — Échange de courrier

Priorité et nom de domaine spécifiant un serveur de messagerie, par exemple, 10 mailserver.example.com. Le point final est traité comme facultatif.

NAPTR — Pointeur d'autorité de nom

Six paramètres séparés par des espaces utilisés par les applications DDDS (Dynamic Delegation Discovery System) pour convertir une valeur en une autre valeur ou pour remplacer une valeur par une autre. Pour de plus amples informations, veuillez consulter Type d'enregistrement NAPTR.

PTR — Pointeur

Nom de domaine que vous voulez que Route 53 renvoie.

NS — Serveur de noms

Nom de domaine d'un serveur de noms, par exemple, ns1.example.com.

> **Note**
>
> Vous ne pouvez spécifier un enregistrement NS qu'avec une politique de routage simple.

SPF — Sender Policy Framework

Enregistrement SPF entre guillemets, par exemple, "v=spf1 ip4:192.168.0.1/16-all". Les enregistrements SPF ne sont pas recommandés. Pour de plus amples informations, veuillez consulter Types d'enregistrements DNS pris en charge.

SRV — Localisateur de service

Enregistrement SRV. Les enregistrements SRV sont utilisés pour accéder à des services, tels qu'un service pour le courrier électronique ou les communications. Pour plus d'informations sur le format d'enregistrement SRV, consultez la documentation du service auquel vous souhaitez vous connecter. Le point final est traité comme facultatif.

Le format d'un enregistrement SRV est :

[priorité] [poids] [port] [nom d'hôte serveur]

Par exemple :

1 10 5269 xmpp-server.example.com.

TXT — Texte

Enregistrement de type texte. Placez le texte entre guillemets, par exemple, "Exemple d'entrée de texte".

TTL (secondes)

Durée, en secondes, pendant laquelle vous voulez que les résolveurs DNS récursifs mettent en cache les informations relatives à cet enregistrement. Si vous spécifiez une valeur plus longue (par exemple, 172 800 secondes, soit deux jours), vous limitez le nombre d'appels que les résolveurs DNS récursifs doivent passer à Route 53 pour obtenir les dernières informations de cet enregistrement. Vous réduisez ainsi la latence et le montant de votre facture pour le service Route 53. Pour de plus amples informations, veuillez consulter Comment Amazon Route 53 achemine le trafic de votre domaine.

Cependant, si vous spécifiez une valeur de durée de vie plus longue, les modifications apportées à l'enregistrement (par exemple, une nouvelle adresse IP) mettent plus de temps à prendre effet, car les résolveurs récursifs utilisent les valeurs qui se trouvent dans leur cache pendant plus longtemps avant de demander les informations les plus récentes à Route 53. Si vous modifiez les paramètres d'un domaine ou d'un sous-domaine déjà utilisé, nous vous conseillons de spécifier initialement une valeur plus courte, par exemple 300 secondes, et d'augmenter la valeur une fois que vous avez vérifié que les nouveaux paramètres sont corrects.

Si vous associez cet enregistrement à une vérification de l'état, nous vous recommandons de spécifier une durée de vie de 60 secondes au maximum afin que les clients répondent rapidement aux modifications de l'état de santé.

Valeurs communes aux enregistrements d'alias pour toutes les politiques de routage

Ce sont les valeurs d'alias communes que vous pouvez spécifier lorsque vous créez ou modifiez des enregistrements Amazon Route 53. Ces valeurs sont utilisées par toutes les politiques de routage.

Rubriques

- Nom de l'enregistrement
- Valeur/acheminer le trafic vers

Nom de l'enregistrement

Saisissez le nom de domaine ou de sous-domaine vers lequel vous souhaitez acheminer le trafic. La valeur par défaut est le nom de la zone hébergée.

> **Note**
>
> Si vous créez un enregistrement qui porte le même nom que la zone hébergée, n'entrez aucune valeur (par exemple, un symbole @) dans le champ Name (Nom).

Enregistrements CNAME

Si vous créez un enregistrement dont la valeur est CNAME pour Type, le nom de l'enregistrement ne peut être identique à celui de la zone hébergée.

Alias des CloudFront distributions et des compartiments Amazon S3

La valeur que vous spécifiez dépend en partie de la AWS ressource vers laquelle vous acheminez le trafic :

- CloudFront distribution — Votre distribution doit inclure un autre nom de domaine correspondant au nom de l'enregistrement. Par exemple, si le nom de l'enregistrement est acme.example.com, votre distribution CloudFront doit inclure acme.example.com parmi les autres noms de domaine. Pour plus d'informations, consultez la section Utilisation de noms de domaine alternatifs (CNAMEs) dans le manuel Amazon CloudFront Developer Guide.
- Compartiment Amazon S3 : le nom de l'enregistrement doit correspondre au nom de votre compartiment Amazon S3. Par exemple, si le nom de votre compartiment est acme.example.com, le nom de cet enregistrement doit également être acme.example.com.

En outre, vous devez configurer le compartiment pour l'hébergement de site web. Pour de plus amples informations, veuillez consulter la section Configurer un compartiment pour l'hébergement de sites Web dans le Guide de l'utilisateur Amazon Simple Storage Service.

Caractères spéciaux

Pour plus d'informations sur la spécification d'autres caractères que a-z, 0-9 et - (trait d'union), et de noms de domaine internationaux, consultez Format de nom de domaine DNS.

Caractères génériques

Vous pouvez utiliser un astérisque (*) dans le nom. DNS traite le caractère * comme un caractère générique ou comme le caractère * (ASCII 42), en fonction de son emplacement dans le nom. Pour de plus amples informations, veuillez consulter Utilisation d'un astérisque (*) dans les noms des zones hébergées et des enregistrements.

Valeur/acheminer le trafic vers

La valeur que vous choisissez dans la liste ou que vous saisissez dans le champ dépend de la AWS ressource vers laquelle vous acheminez le trafic.

Pour plus d'informations sur la configuration de Route 53 pour acheminer le trafic vers des AWS ressources spécifiques, consultezAcheminement du trafic Internet vers vos AWS ressources.

> **Important**
>
> Si vous avez utilisé le même AWS compte pour créer votre zone hébergée et la ressource vers laquelle vous acheminez le trafic, et si votre ressource n'apparaît pas dans la liste des points de terminaison, vérifiez les points suivants :
>
> - Vérifiez que la valeur choisie pour Record type (Type d'enregistrement) est prise en charge. Les valeurs prise en charge dépendent de la ressource vers laquelle vous acheminez du trafic. Par exemple, pour acheminer le trafic vers un compartiment S3, vous devez choisir A — IPv4 address pour le type d'enregistrement.
> - Vérifiez que le compte dispose des autorisations IAM nécessaires pour répertorier les ressources applicables. Par exemple, pour que les distributions CloudFront fassent partie de la liste Endpoint (Point de terminaison), le compte doit être autorisé à effectuer l'action suivante : `cloudfront:ListDistributions`.

Pour obtenir un exemple de politique IAM, consultez Autorisations requises pour utiliser la console Amazon Route 53.

Si vous avez utilisé différents AWS comptes pour créer la zone hébergée et la ressource, la liste des points de terminaison n'affiche pas votre ressource. Consultez la documentation suivante correspondant à votre type de ressource afin de déterminer la valeur à saisir dans Endpoint (Point de terminaison).

API Gateway personnalisé, régional APIs et optimisé pour les périphériques APIs

Pour une API Gateway personnalisée régionale APIs et optimisée pour les périphériques APIs, effectuez l'une des opérations suivantes :

- Si vous avez utilisé le même compte pour créer votre zone hébergée Route 53 et votre API : sélectionnez Endpoint (Point de terminaison) et choisissez une API dans la liste. Si vous en avez beaucoup APIs, vous pouvez saisir les premiers caractères du point de terminaison de l'API pour filtrer la liste.

  > **Note**
  >
  > Le nom de l'enregistrement doit correspondre à un nom de domaine personnalisé pour votre API, tel que api.example.com.

- Si vous avez utilisé des comptes différents pour créer votre zone hébergée Route 53 et votre API : entrez le point de terminaison d'API pour l'API, par exemple api.example.com.

  Si vous avez utilisé un AWS compte pour créer la zone hébergée actuelle et un autre compte pour créer une API, l'API n'apparaîtra pas dans la liste des points de terminaison sous API Gateway APIs.

  Si vous avez utilisé un compte pour créer la zone hébergée actuelle et un ou plusieurs comptes différents pour créer toutes les vôtres APIs, la liste des points de terminaison indique qu'aucune cible n'est disponible sous API Gateway APIs. Pour de plus amples informations, veuillez consulter Acheminer le trafic vers une API Amazon API Gateway à l'aide de votre nom de domaine.

CloudFront distributions

Pour les CloudFront distributions, effectuez l'une des opérations suivantes :

- Si vous avez utilisé le même compte pour créer votre zone hébergée Route 53 et votre CloudFront distribution, choisissez Endpoint et choisissez une distribution dans la liste. Si vous disposez de beaucoup de distributions, vous pouvez entrer les premiers caractères du nom de domaine de votre distribution afin de filtrer la liste.

  Si votre distribution n'apparaît pas dans la liste, notez les points suivants :

  - Le nom de l'enregistrement doit correspondre à un autre nom de domaine dans votre distribution.
  - Si vous venez d'ajouter un autre nom de domaine à votre distribution, la propagation de vos modifications à tous les emplacements CloudFront périphériques peut prendre 15 minutes. Tant que les modifications ne sont pas propagées, Route 53 ne peut pas connaître le nouveau nom de domaine.
- Si vous avez utilisé différents comptes pour créer votre zone hébergée Route 53 et votre distribution, entrez le nom de CloudFront domaine de la distribution, par exemple d111111abcdef8.cloudfront.net.

  Si vous avez utilisé un AWS compte pour créer la zone hébergée actuelle et un autre compte pour créer une distribution, la distribution n'apparaîtra pas dans la liste des points de terminaison.

  Si vous avez utilisé un compte pour créer la zone hébergée actuelle et un ou plusieurs comptes différents pour créer toutes vos distributions, la liste Endpoints indique qu'aucune cible n'est disponible dans le cadre des CloudFront distributions.

> **Important**
>
> N'acheminez pas les requêtes vers une CloudFront distribution qui ne s'est pas propagée à tous les emplacements périphériques, sinon vos utilisateurs ne pourront pas accéder au contenu applicable.

Votre CloudFront distribution doit inclure un autre nom de domaine correspondant au nom de l'enregistrement. Par exemple, si le nom de l'enregistrement est acme.exemple.com, votre CloudFront distribution doit inclure acme.example.com comme l'un des noms de domaine

alternatifs. Pour plus d'informations, consultez la section Utilisation de noms de domaine alternatifs (CNAMEs) dans le manuel Amazon CloudFront Developer Guide.

Si la distribution IPv6 est activée, créez deux enregistrements, l'un avec la valeur A — IPv4 adresse pour le type d'enregistrement, et l'autre avec la valeur AAAA — IPv6 adresse. Pour de plus amples informations, veuillez consulter Acheminement du trafic vers une CloudFront distribution Amazon à l'aide de votre nom de domaine.

Service App Runner

Pour le service App Runner, effectuez l'une des opérations suivantes :

- Si vous avez utilisé le même compte pour créer votre zone hébergée Route 53 et votre service App Runner, choisissez le Région AWS, puis le nom de domaine de l'environnement vers lequel vous souhaitez acheminer le trafic dans la liste.
- Si vous avez utilisé différents comptes pour créer votre zone hébergée Route 53 et votre App Runner, entrez le nom de domaine personnalisé. Pour plus d'informations, consultez Gestion des noms de domaine personnalisés pour App Runner.

  Si vous avez utilisé un AWS compte pour créer la zone hébergée actuelle et un autre compte pour créer un App Runner, l'App Runner n'apparaîtra pas dans la liste des points de terminaison.

Pour de plus amples informations, veuillez consulter Configuration d'Amazon Route 53 pour acheminer le trafic vers un service App Runner.

Environnements Elastic Beanstalk comportant des sous-domaines régionalisés

Si le nom de domaine de votre environnement Elastic Beanstalk inclut la région dans laquelle vous avez déployé l'environnement, vous pouvez créer un enregistrement d'alias qui achemine le trafic vers l'environnement. Par exemple, le nom de domaine `my-environment.us-west-2.elasticbeanstalk.com` est un nom de domaine régionalisé.

> **Important**
>
> Concernant les environnements qui ont été créés avant début 2016, le nom de domaine n'inclut pas la région. Pour acheminer le trafic vers ces environnements, vous devez créer un enregistrement CNAME au lieu d'un enregistrement d'alias. Notez que vous ne pouvez pas créer un enregistrement CNAME pour le nom de domaine racine. Par exemple, si votre nom de domaine est example.com, vous pouvez créer un enregistrement qui achemine le trafic pour acme.example.com vers votre environnement Elastic Beanstalk,

mais vous ne pouvez pas créer d'enregistrement qui achemine le trafic pour example.com vers votre environnement Elastic Beanstalk.

Pour les environnements Elastic Beanstalk comportant des sous-domaines régionalisés, effectuez l'une des actions suivantes :

- Si vous avez utilisé le même compte pour créer votre zone hébergée Route 53 et votre environnement Elastic Beanstalk : sélectionnez Endpoint (Point de terminaison) et choisissez un environnement dans la liste. Si vous disposez de beaucoup d'environnements, vous pouvez entrer les premiers caractères de l'attribut CNAME de l'environnement afin de filtrer la liste.
- Si vous avez utilisé différents comptes pour créer votre zone hébergée Route 53 et votre environnement Elastic Beanstalk : entrez l'attribut CNAME de l'environnement Elastic Beanstalk.

Pour de plus amples informations, veuillez consulter Acheminement du trafic vers un AWS Elastic Beanstalk environnement.

Équilibreurs de charge ELB

Pour les équilibreurs de charge ELB, effectuez l'une des actions suivantes :

- Si vous avez utilisé le même compte pour créer votre zone hébergée Route 53 et votre équilibreur de charge : sélectionnez Endpoint (Point de terminaison) et choisissez un équilibreur de charge dans la liste. Si vous disposez de beaucoup d'équilibreurs de charge, vous pouvez entrer les premiers caractères du nom DNS afin de filtrer la liste.
- Si vous avez utilisé différents comptes pour créer votre zone hébergée Route 53 et votre équilibreur de charge : entrez la valeur que vous avez obtenue au cours de la procédure Obtention du nom DNS d'un équilibreur de charge Elastic Load Balancing.

  Si vous avez utilisé un AWS compte pour créer la zone hébergée actuelle et un autre compte pour créer un équilibreur de charge, l'équilibreur de charge n'apparaîtra pas dans la liste des points de terminaison.

  Si vous avez utilisé un compte pour créer la zone hébergée actuelle et un ou plusieurs autres comptes pour créer tous vos équilibreurs de charge, la liste Endpoints (Points de terminaison) affiche No targets available (Aucune cible disponible) sous Elastic Load Balancers.

La console ajoute le préfixe dualstack. pour l'Application et le Classic Load Balancer à partir d'un compte différent. Lorsqu'un client, tel qu'un navigateur Web, demande l'adresse IP de votre nom

de domaine (exemple.com) ou de votre nom de sous-domaine (www.exemple.com), le client peut demander une IPv4 adresse (enregistrement A), une IPv6 adresse (enregistrement AAAA), ou les deux IPv4 et des IPv6 adresses (dans des demandes distinctes). La désignation dualstack. permet à Route 53 de répondre avec l'adresse IP appropriée pour votre équilibreur de charge en fonction du format d'adresse IP que le client a demandé.

Pour de plus amples informations, veuillez consulter Routage du trafic vers un équilibreur de charge ELB.

AWS Accélérateurs Global Accelerator

Pour les accélérateurs AWS Global Accelerator, entrez le nom DNS de l'accélérateur. Vous pouvez saisir le nom DNS d'un accélérateur que vous avez créé à l'aide du AWS compte actuel ou d'un autre AWS compte.

Compartiments Amazon S3

Pour les compartiments Amazon S3 qui sont configurés en tant que points de terminaison de site Web, effectuez l'une des actions suivantes :

- Si vous avez utilisé le même compte pour créer votre zone hébergée Route 53 et votre compartiment Amazon S3 : sélectionnez Endpoint (Point de terminaison) et choisissez un compartiment dans la liste. Si vous disposez de beaucoup de compartiments, vous pouvez entrer les premiers caractères du nom DNS afin de filtrer la liste.

  La valeur Endpoint (Point de terminaison) change pour le point de terminaison du site web Amazon S3 de votre compartiment.

- Si vous avez utilisé différents comptes pour créer votre zone hébergée Route 53 et votre compartiment Amazon S3 : saisissez le nom de la région dans laquelle vous avez créé votre compartiment S3. Utilisez la valeur applicable de la colonne Point de terminaison des sites Web dans le tableau Points de terminaison des sites Web Amazon S3 dans le Référence générale d'Amazon Web Services.

  Si vous avez utilisé AWS des comptes autres que le compte actuel pour créer vos compartiments Amazon S3, le compartiment n'apparaîtra pas dans la liste des points de terminaison.

Vous devez configurer le compartiment pour l'hébergement de site web. Pour de plus amples informations, veuillez consulter la section Configurer un compartiment pour l'hébergement de sites Web dans le Guide de l'utilisateur Amazon Simple Storage Service.

Le nom de l'enregistrement doit correspondre au nom de votre compartiment Amazon S3. Par exemple, si le nom de votre compartiment Amazon S3 est acme.example.com, le nom de cet enregistrement doit également être acme.example.com.

Dans un groupe d'enregistrements d'alias pondérés, d'alias de latence, d'alias de basculement ou d'alias de géolocalisation, vous ne pouvez créer qu'un seul enregistrement qui achemine les requêtes vers un compartiment Amazon S3, car le nom de l'enregistrement doit correspondre au nom du compartiment et les noms de compartiment doivent être globalement uniques.

Amazon OpenSearch Service

Pour le OpenSearch service, effectuez l'une des opérations suivantes :

- OpenSearch Domaine personnalisé du service : le nom de l'enregistrement doit correspondre au domaine personnalisé. Par exemple, si le nom de votre domaine personnalisé est test.example.com, le nom de cet enregistrement doit également être test.example.com.
- Si vous avez utilisé le même compte pour créer votre zone hébergée Route 53 et votre domaine de OpenSearch service, choisissez le Région AWS, puis le nom de domaine.
- Si vous avez utilisé différents comptes pour créer votre zone hébergée Route 53 et votre domaine de OpenSearch service, entrez le nom de domaine personnalisé. Pour plus d'informations, voir Création d'un point de terminaison personnalisé.

  Si vous avez utilisé un AWS compte pour créer la zone hébergée actuelle et un autre compte pour créer un domaine de OpenSearch service, le domaine n'apparaîtra pas dans la liste des points de terminaison.

  Si vous avez utilisé un compte pour créer la zone hébergée actuelle et un ou plusieurs comptes différents pour créer tous vos domaines de OpenSearch service, la liste des points de terminaison indique qu'aucune cible n'est disponible sous OpenSearch Service.

Pour de plus amples informations, veuillez consulter Configuration d'Amazon Route 53 pour acheminer le trafic vers un point de terminaison OpenSearch de domaine Amazon Service.

Points de terminaison de l'interface d'un VPC Amazon

Pour les points de terminaison d'interface d'un VPC Amazon, effectuez l'une des actions suivantes :

- Si vous avez utilisé le même compte pour créer votre zone hébergée Route 53 et votre point de terminaison d'interface : sélectionnez Endpoint (Point de terminaison), puis choisissez un point de terminaison d'interface dans la liste. Si vous disposez de beaucoup de points de terminaison d'interface, vous pouvez entrer les premiers caractères du nom DNS afin de filtrer la liste.

- Si vous avez utilisé différents comptes pour créer votre zone hébergée Route 53 et votre point de terminaison d'interface, entrez le nom d'hôte DNS du point de terminaison d'interface, par exemple vpce-123456789abcdef01- -1a.elasticloadbalancing.us-east-1.vpce.amazonaws.com. example-us-east

  Si vous avez utilisé un AWS compte pour créer la zone hébergée actuelle et un autre compte pour créer un point de terminaison d'interface, le point de terminaison d'interface n'apparaîtra pas dans la liste des points de terminaison sous points de terminaison VPC.

  Si vous avez utilisé un compte pour créer la zone hébergée actuelle et un ou plusieurs autres comptes pour créer tous vos points de terminaison d'interface, la liste Endpoint (Point de terminaison) affiche No targets available (Aucune cible disponible) sous VPC endpoints (Points de terminaison d'un VPC).

  Pour de plus amples informations, veuillez consulter Acheminer le trafic vers un point de terminaison d'interface Amazon Virtual Private Cloud à l'aide de votre nom de domaine.

Enregistrements dans cette zone hébergée

Pour les enregistrements dans cette zone hébergée, sélectionnez Endpoint (Point de terminaison) et choisissez l'enregistrement applicable. Si vous disposez de beaucoup d'enregistrements, vous pouvez entrer les premiers caractères du nom afin de filtrer la liste.

Si la zone hébergée contient uniquement les enregistrements NS et SOA par défaut, la liste Endpoints (Points de terminaison) affiche No targets available (Aucune cible disponible).

> **Note**
>
> Si vous créez un enregistrement d'alias qui a le même nom que la zone hébergée (appelée aussi zone apex), vous ne pouvez pas choisir un enregistrement dont la valeur Record type (Type d'enregistrement) est CNAME. Cela est dû au fait que l'enregistrement d'alias doit être du même type que l'enregistrement vers lequel vous acheminez le trafic et que la création d'un enregistrement CNAME pour la zone apex n'est pas prise en charge, même pour un enregistrement d'alias.

Valeurs spécifiques aux enregistrements simples

Lorsque vous créez des enregistrements simples, vous spécifiez les valeurs suivantes.

Rubriques

- Stratégie de routage
- Nom de l'enregistrement
- Valeur/acheminer le trafic vers
- Type de registre
- TTL (secondes)

Stratégie de routage

Choisissez Simple routing (Routage simple).

Nom de l'enregistrement

Saisissez le nom de domaine ou de sous-domaine vers lequel vous souhaitez acheminer le trafic. La valeur par défaut est le nom de la zone hébergée.

> **Note**
>
> Si vous créez un enregistrement qui porte le même nom que la zone hébergée, n'entrez aucune valeur (par exemple, un symbole @) dans le champ Name (Nom).

Pour plus d'informations sur les noms d'enregistrements, veuillez consulter Nom de l'enregistrement.

Valeur/acheminer le trafic vers

Choisissez IP address or another value depending on the record type (Adresse IP ou autre valeur selon le type d'enregistrement). Entrez une valeur appropriée pour la valeur Record type (Type d'enregistrement). Pour tous les types à l'exception de CNAME, vous pouvez entrer plusieurs valeurs. Entrez chaque valeur sur une ligne distincte.

Vous pouvez acheminer le trafic vers, ou spécifier les valeurs suivantes :

- A — IPv4 adresse
- AAAA — adresse IPv6

- CAA : autorisation de l'autorité de certification
- CNAME : nom canonique
- MX : échange de courrier
- NAPTR : nom d'indicateur d'autorité
- NS — Serveur de noms

  Nom de domaine d'un serveur de noms, par exemple, ns1.example.com.

  > **Note**
  >
  > Vous ne pouvez spécifier un enregistrement NS qu'avec une politique de routage simple.

- PTR : indicateur
- SPF : cadre de la politique de l'envoyeur
- SRV : localisateur de service
- TXT : texte

Pour plus d'informations sur les valeurs ci-dessus, consultez valeurs communes pour Valeur/Acheminement du trafic vers.

Type de registre

Type d'enregistrement DNS. Pour de plus amples informations, veuillez consulter Types d'enregistrements DNS pris en charge.

Sélectionnez la valeur pour le champ Record type (Type d'enregistrement) en fonction de la façon dont vous voulez que Route 53 réponde aux requêtes DNS.

TTL (secondes)

Durée, en secondes, pendant laquelle vous voulez que les résolveurs DNS récursifs mettent en cache les informations relatives à cet enregistrement. Si vous spécifiez une valeur plus longue (par exemple, 172 800 secondes, soit deux jours), vous limitez le nombre d'appels que les résolveurs DNS récursifs doivent passer à Route 53 pour obtenir les dernières informations de cet enregistrement. Vous réduisez ainsi la latence et le montant de votre facture pour le service Route 53. Pour de plus amples informations, veuillez consulter Comment Amazon Route 53 achemine le trafic de votre domaine.

Cependant, si vous spécifiez une valeur de durée de vie plus longue, les modifications apportées à l'enregistrement (par exemple, une nouvelle adresse IP) mettent plus de temps à prendre effet, car les résolveurs récursifs utilisent les valeurs qui se trouvent dans leur cache pendant plus longtemps avant de demander les informations les plus récentes à Route 53. Si vous modifiez les paramètres d'un domaine ou d'un sous-domaine déjà utilisé, nous vous conseillons de spécifier initialement une valeur plus courte, par exemple 300 secondes, et d'augmenter la valeur une fois que vous avez vérifié que les nouveaux paramètres sont corrects.

Valeurs spécifiques aux enregistrements d'alias simples

Lorsque vous créez des enregistrements d'alias, vous spécifiez les valeurs suivantes. Pour de plus amples informations, veuillez consulter Choix entre des enregistrements avec ou sans alias.

> **Note**
>
> Si vous utilisez Route 53 dans le AWS GovCloud (US) Region, cette fonctionnalité comporte certaines restrictions. Pour plus d'informations, consultez la page Amazon Route 53 dans le Guide de l'utilisateur AWS GovCloud (US) .

Rubriques

- Stratégie de routage
- Nom de l'enregistrement
- Valeur/acheminer le trafic vers
- Type de registre
- Évaluer l'état de la cible

Stratégie de routage

Choisissez Simple routing (Routage simple).

Nom de l'enregistrement

Saisissez le nom de domaine ou de sous-domaine vers lequel vous souhaitez acheminer le trafic. La valeur par défaut est le nom de la zone hébergée.

> **Note**
>
> Si vous créez un enregistrement qui porte le même nom que la zone hébergée, n'entrez aucune valeur (par exemple, un symbole @) dans le champ Name (Nom).

Pour plus d'informations sur les noms d'enregistrements, veuillez consulter Nom de l'enregistrement.

Valeur/acheminer le trafic vers

La valeur que vous choisissez dans la liste ou que vous saisissez dans le champ dépend de la AWS ressource vers laquelle vous acheminez le trafic.

Pour plus d'informations sur les AWS ressources que vous pouvez cibler, consultez les valeurs communes des enregistrements d'alias destinés au trafic de valeurs/d'itinéraires.

Pour plus d'informations sur la configuration de Route 53 pour acheminer le trafic vers des AWS ressources spécifiques, consultezAcheminement du trafic Internet vers vos AWS ressources.

Type de registre

Type d'enregistrement DNS. Pour de plus amples informations, veuillez consulter Types d'enregistrements DNS pris en charge.

Sélectionnez la valeur applicable en fonction de la AWS ressource vers laquelle vous acheminez le trafic :

API régionale personnalisée API Gateway et API optimisée pour la périphérie

Sélectionnez A — IPv4 adresse.

Points de terminaison de l'interface d'un VPC Amazon

Sélectionnez A — IPv4 adresse.

CloudFront distribution

Sélectionnez A — IPv4 adresse.

Si cette option IPv6 est activée pour la distribution, créez deux enregistrements, l'un avec la valeur A — IPv4 adresse pour Type, et l'autre avec la valeur AAAA — IPv6 adresse.

Service App Runner

Sélectionnez A — IPv4 adresse

Environnement Elastic Beanstalk comportant des sous-domaines régionalisés

Sélectionnez A — IPv4 adresse

ELB load balancer

Sélectionnez A — IPv4 adresse ou AAAA — IPv6 adresse

Compartiment Amazon S3

Sélectionnez A — IPv4 adresse

OpenSearch Service

Sélectionnez A — IPv4 adresse ou AAAA — IPv6 adresse

Autre enregistrement de cette zone hébergée

Sélectionnez le type d'enregistrement pour lequel vous créez l'alias. Tous les types sont pris en charge, sauf NS et SOA.

> **Note**
>
> Si vous créez un enregistrement d'alias qui a le même nom que la zone hébergée (appelée aussi zone apex), vous ne pouvez pas acheminer le trafic vers un enregistrement dont la valeur pour Type (Type) est CNAME. Cela est dû au fait que l'enregistrement d'alias doit être du même type que l'enregistrement vers lequel vous acheminez le trafic et que la création d'un enregistrement CNAME pour la zone apex n'est pas prise en charge, même pour un enregistrement d'alias.

Évaluer l'état de la cible

Lorsque la valeur de Routing policy (Politique de routage) est Simple (Simple), vous pouvez choisir No (Non) ou la valeur par défaut Yes (Oui), car Evaluate target health (Évaluer l'état de la cible) n'a aucun effet pour le routage Simple (Simple). Si vous avez un seul enregistrement avec un nom et un type donnés, Route 53 répond aux requêtes DNS à l'aide des valeurs de cet enregistrement que la ressource soit saine ou non.

Valeurs spécifiques aux enregistrements de basculement

Lorsque vous créez des enregistrements de basculement, vous spécifiez les valeurs suivantes.

> **Note**
>
> Pour plus d'informations sur la création d'enregistrements de basculement dans une zone hébergée privée, consultez Configuration du basculement dans une zone hébergée privée.

Rubriques

- Stratégie de routage
- Nom de l'enregistrement
- Type de registre
- TTL (secondes)
- Valeur/acheminer le trafic vers
- Type d'enregistrement de basculement
- Surveillance de l'état
- ID d'enregistrement

Stratégie de routage

Choisissez Basculement.

Nom de l'enregistrement

Saisissez le nom de domaine ou de sous-domaine vers lequel vous souhaitez acheminer le trafic. La valeur par défaut est le nom de la zone hébergée.

> **Note**
>
> Si vous créez un enregistrement qui porte le même nom que la zone hébergée, n'entrez aucune valeur (par exemple, un symbole @) dans le champ Record name (Nom de l'enregistrement).

Entrez le même nom pour les deux enregistrements du groupe d'enregistrements de basculement.

Pour plus d'informations sur les noms d'enregistrements, veuillez consulter Nom de l'enregistrement.

Type de registre

Type d'enregistrement DNS. Pour de plus amples informations, veuillez consulter Types d'enregistrements DNS pris en charge.

Sélectionnez la même valeur pour les enregistrements de basculement principaux et secondaires.

TTL (secondes)

Durée, en secondes, pendant laquelle vous voulez que les résolveurs DNS récursifs mettent en cache les informations relatives à cet enregistrement. Si vous spécifiez une valeur plus longue (par exemple, 172 800 secondes, soit deux jours), vous limitez le nombre d'appels que les résolveurs DNS récursifs doivent passer à Route 53 pour obtenir les dernières informations de cet enregistrement. Vous réduisez ainsi la latence et le montant de votre facture pour le service Route 53. Pour de plus amples informations, veuillez consulter Comment Amazon Route 53 achemine le trafic de votre domaine.

Cependant, si vous spécifiez une valeur de durée de vie plus longue, les modifications apportées à l'enregistrement (par exemple, une nouvelle adresse IP) mettent plus de temps à prendre effet, car les résolveurs récursifs utilisent les valeurs qui se trouvent dans leur cache pendant plus longtemps avant de demander les informations les plus récentes à Route 53. Si vous modifiez les paramètres d'un domaine ou d'un sous-domaine déjà utilisé, nous vous conseillons de spécifier initialement une valeur plus courte, par exemple 300 secondes, et d'augmenter la valeur une fois que vous avez vérifié que les nouveaux paramètres sont corrects.

Si vous associez cet enregistrement à une vérification de l'état, nous vous recommandons de spécifier une durée de vie de 60 secondes au maximum afin que les clients répondent rapidement aux modifications de l'état de santé.

Valeur/acheminer le trafic vers

Choisissez IP address or another value depending on the record type (Adresse IP ou autre valeur selon le type d'enregistrement). Entrez une valeur appropriée pour la valeur Record type (Type d'enregistrement). Pour tous les types à l'exception de CNAME, vous pouvez entrer plusieurs valeurs. Entrez chaque valeur sur une ligne distincte.

Vous pouvez acheminer le trafic vers, ou spécifier les valeurs suivantes :

- A — IPv4 adresse

- AAAA — adresse IPv6
- CAA : autorisation de l'autorité de certification
- CNAME : nom canonique
- MX : échange de courrier
- NAPTR : nom d'indicateur d'autorité
- PTR : indicateur
- SPF : cadre de la politique de l'envoyeur
- SRV : localisateur de service
- TXT : texte

Pour plus d'informations sur les valeurs ci-dessus, consultez valeurs communes pour Valeur/Acheminement du trafic vers.

Type d'enregistrement de basculement

Sélectionnez la valeur applicable pour cet enregistrement. Pour que le basculement fonctionne correctement, vous devez créer un enregistrement de basculement principal et un secondaire.

Vous ne pouvez pas créer d'enregistrements qui ne sont pas de type basculement en utilisant les mêmes valeurs pour les champs Record name (Nom de l'enregistrement) et Record type (Type d'enregistrement) que celles des enregistrements de basculement.

Surveillance de l'état

Sélectionnez une surveillance de l'état si vous voulez que Route 53 vérifie l'état d'un point de terminaison spécifique et réponde aux requêtes DNS à l'aide de cet enregistrement uniquement lorsque le point de terminaison est sain.

Route 53 ne vérifie pas l'état du point de terminaison spécifié dans l'enregistrement, par exemple, le point de terminaison indiqué par l'adresse IP dans le champ Value (Valeur). Lorsque vous sélectionnez une surveillance de l'état pour un enregistrement, Route 53 vérifie l'état du point de terminaison que vous avez spécifié dans la surveillance de l'état. Pour plus d'informations sur la façon dont Route 53 détermine si un point de terminaison est sain, consultez Comment Amazon Route 53 détermine si une surveillance de l'état est saine.

L'association d'une surveillance de l'état à un enregistrement est utile uniquement lorsque Route 53 doit choisir entre plusieurs enregistrements pour répondre à une requête DNS et que vous souhaitez

que Route 53 base en partie son choix sur le statut d'une surveillance de l'état. Utilisez des surveillances de l'état uniquement dans les configurations suivantes :

- Vous vérifiez l'état de santé de tous les enregistrements d'un groupe d'enregistrements portant le même nom, le même type et la même politique de routage (tels que le basculement ou les enregistrements pondérés), et vous spécifiez un contrôle de santé IDs pour tous les enregistrements. Si la surveillance de l'état d'un enregistrement spécifie un point de terminaison qui n'est pas sain, Route 53 cesse de répondre aux requêtes utilisant la valeur indiquée pour cet enregistrement.
- Vous sélectionnez Yes (Oui) pour Evaluate target health (Évaluer l'état de la cible) pour un enregistrement d'alias ou les enregistrements dans un groupe d'enregistrements d'alias de basculement, d'alias de géolocalisation, d'alias de latence, d'alias basés sur IP ou d'alias pondérés. Si les enregistrements d'alias font référence à des enregistrements sans alias dans une même zone hébergée, vous devez spécifier les surveillances d'état pour les enregistrements référencés. Si vous associez une surveillance de l'état à un enregistrement d'alias et que vous sélectionnez également Yes (Oui) pour Evaluate Target Health (Évaluer l'état de la cible), les deux doivent être évalués à vrai. Pour de plus amples informations, veuillez consulter Que se passe-t-il lorsque vous associez une surveillance de l'état à un enregistrement d'alias ?.

Si vos surveillances de l'état spécifient le point de terminaison uniquement par nom de domaine, nous vous recommandons de créer une surveillance de l'état distincte pour chaque point de terminaison. Par exemple, créez une surveillance de l'état pour chaque serveur HTTP qui diffuse du contenu pour www.example.com. Pour la valeur du champ Nom de domaine, indiquez le nom de domaine du serveur (par exemple, us-east-2-www.example.com), et non pas le nom des enregistrements (example.com).

> **Important**
>
> Dans cette configuration, si vous créez une surveillance de l'état pour laquelle la valeur du champ Nom de domaine correspond au nom des enregistrements et si vous associez ensuite la surveillance de l'état à ces enregistrements, les résultats de la surveillance de l'état seront imprévisibles.

ID d'enregistrement

Entrez une valeur qui identifie de façon unique les enregistrements principaux et secondaires.

Valeurs spécifiques aux enregistrements d'alias de basculement

Lorsque vous créez des enregistrements d'alias de basculement, vous spécifiez les valeurs suivantes.

Pour plus d'informations, consultez les rubriques suivantes :

- Pour plus d'informations sur la création d'enregistrements de basculement dans une zone hébergée privée, consultez Configuration du basculement dans une zone hébergée privée.
- Pour plus d'informations sur les enregistrements d'alias, consultez Choix entre des enregistrements avec ou sans alias.

Rubriques

- Stratégie de routage
- Nom de l'enregistrement
- Type de registre
- Valeur/acheminer le trafic vers
- Type d'enregistrement de basculement
- Surveillance de l'état
- Évaluer l'état de la cible
- ID d'enregistrement

Stratégie de routage

Choisissez Basculement.

Nom de l'enregistrement

Saisissez le nom de domaine ou de sous-domaine vers lequel vous souhaitez acheminer le trafic. La valeur par défaut est le nom de la zone hébergée.

> **Note**
>
> Si vous créez un enregistrement qui porte le même nom que la zone hébergée, n'entrez aucune valeur (par exemple, un symbole @) dans le champ Record name (Nom de l'enregistrement).

Entrez le même nom pour les deux enregistrements du groupe d'enregistrements de basculement.

Pour plus d'informations sur les noms d'enregistrements, veuillez consulter Nom de l'enregistrement.

Type de registre

Type d'enregistrement DNS. Pour de plus amples informations, veuillez consulter Types d'enregistrements DNS pris en charge.

Sélectionnez la valeur applicable en fonction de la AWS ressource vers laquelle vous acheminez le trafic. Sélectionnez la même valeur pour les enregistrements de basculement principaux et secondaires :

API régionale personnalisée API Gateway et API optimisée pour la périphérie

Sélectionnez A — IPv4 adresse.

Points de terminaison de l'interface d'un VPC Amazon

Sélectionnez A — IPv4 adresse.

CloudFront distribution

Sélectionnez A — IPv4 adresse.

Si cette option IPv6 est activée pour la distribution, créez deux enregistrements, l'un avec la valeur A — IPv4 adresse pour Type, et l'autre avec la valeur AAAA — IPv6 adresse.

Service App Runner

Sélectionnez A — IPv4 adresse

Environnement Elastic Beanstalk comportant des sous-domaines régionalisés

Sélectionnez A — IPv4 adresse

ELB load balancer

Sélectionnez A — IPv4 adresse ou AAAA — IPv6 adresse

Compartiment Amazon S3

Sélectionnez A — IPv4 adresse

OpenSearch Service

Sélectionnez A — IPv4 adresse ou AAAA — IPv6 adresse

Autre enregistrement de cette zone hébergée

Sélectionnez le type d'enregistrement pour lequel vous créez l'alias. Tous les types sont pris en charge, sauf NS et SOA.

> **Note**
>
> Si vous créez un enregistrement d'alias qui a le même nom que la zone hébergée (appelée aussi zone apex), vous ne pouvez pas acheminer le trafic vers un enregistrement dont la valeur pour Type (Type) est CNAME. Cela est dû au fait que l'enregistrement d'alias doit être du même type que l'enregistrement vers lequel vous acheminez le trafic et que la création d'un enregistrement CNAME pour la zone apex n'est pas prise en charge, même pour un enregistrement d'alias.

Valeur/acheminer le trafic vers

La valeur que vous choisissez dans la liste ou que vous saisissez dans le champ dépend de la AWS ressource vers laquelle vous acheminez le trafic.

Pour plus d'informations sur les AWS ressources que vous pouvez cibler, consultez les valeurs communes des enregistrements d'alias vers lesquels le trafic de valeurs/d'itinéraires est destiné.

Pour plus d'informations sur la configuration de Route 53 pour acheminer le trafic vers des AWS ressources spécifiques, consultezAcheminement du trafic Internet vers vos AWS ressources.

> **Note**
>
> Lorsque vous créez des enregistrements de basculement principaux et secondaires, vous pouvez éventuellement créer un enregistrement de basculement et un enregistrement d'alias de basculement ayant les mêmes valeurs pour les champs Name (Nom) et Record type (Type d'enregistrement). Si vous mélangez des enregistrements de basculement et d'alias de basculement, n'importe lequel d'entre eux peut être l'enregistrement principal.

Type d'enregistrement de basculement

Sélectionnez la valeur applicable pour cet enregistrement. Pour que le basculement fonctionne correctement, vous devez créer un enregistrement de basculement principal et un secondaire.

Vous ne pouvez pas créer d'enregistrements qui ne sont pas de type basculement en utilisant les mêmes valeurs pour les champs Record name (Nom de l'enregistrement) et Record type (Type d'enregistrement) que celles des enregistrements de basculement.

Surveillance de l'état

Sélectionnez une surveillance de l'état si vous voulez que Route 53 vérifie l'état d'un point de terminaison spécifique et réponde aux requêtes DNS à l'aide de cet enregistrement uniquement lorsque le point de terminaison est sain.

Route 53 ne vérifie pas l'état du point de terminaison spécifié dans l'enregistrement, par exemple, le point de terminaison indiqué par l'adresse IP dans le champ Value (Valeur). Lorsque vous sélectionnez une surveillance de l'état pour un enregistrement, Route 53 vérifie l'état du point de terminaison que vous avez spécifié dans la surveillance de l'état. Pour plus d'informations sur la façon dont Route 53 détermine si un point de terminaison est sain, consultez Comment Amazon Route 53 détermine si une surveillance de l'état est saine.

L'association d'une surveillance de l'état à un enregistrement est utile uniquement lorsque Route 53 doit choisir entre plusieurs enregistrements pour répondre à une requête DNS et que vous souhaitez que Route 53 base en partie son choix sur le statut d'une surveillance de l'état. Utilisez des surveillances de l'état uniquement dans les configurations suivantes :

- Vous vérifiez l'état de santé de tous les enregistrements d'un groupe d'enregistrements portant le même nom, le même type et la même politique de routage (tels que le basculement ou les enregistrements pondérés), et vous spécifiez un contrôle de santé IDs pour tous les enregistrements. Si la surveillance de l'état d'un enregistrement spécifie un point de terminaison qui n'est pas sain, Route 53 cesse de répondre aux requêtes utilisant la valeur indiquée pour cet enregistrement.
- Vous sélectionnez Yes (Oui) pour Evaluate target health (Évaluer l'état de la cible) pour un enregistrement d'alias ou les enregistrements dans un groupe d'enregistrements d'alias de basculement, d'alias de géolocalisation, d'alias de latence, d'alias basés sur IP ou d'alias pondérés. Si les enregistrements d'alias font référence à des enregistrements sans alias dans une même zone hébergée, vous devez spécifier les surveillances d'état pour les enregistrements référencés. Si vous associez une surveillance de l'état à un enregistrement d'alias et que vous sélectionnez également Yes (Oui) pour Evaluate Target Health (Évaluer l'état de la cible), les deux doivent être évalués à vrai. Pour de plus amples informations, veuillez consulter Que se passe-t-il lorsque vous associez une surveillance de l'état à un enregistrement d'alias ?.

Si vos surveillances de l'état spécifient le point de terminaison uniquement par nom de domaine, nous vous recommandons de créer une surveillance de l'état distincte pour chaque point de terminaison. Par exemple, créez une surveillance de l'état pour chaque serveur HTTP qui diffuse du contenu pour www.example.com. Pour la valeur du champ Nom de domaine, indiquez le nom de domaine du serveur (par exemple, us-east-2-www.example.com), et non pas le nom des enregistrements (example.com).

> **Important**
>
> Dans cette configuration, si vous créez une surveillance de l'état pour laquelle la valeur du champ Nom de domaine correspond au nom des enregistrements et si vous associez ensuite la surveillance de l'état à ces enregistrements, les résultats de la surveillance de l'état seront imprévisibles.

Évaluer l'état de la cible

Sélectionnez Yes (Oui) si vous voulez que Route 53 détermine s'il doit répondre aux requêtes DNS à l'aide de cet enregistrement en vérifiant l'état de la ressource spécifiée dans le champ Endpoint (Point de terminaison).

Remarques :

API Gateway personnalisé, régional APIs et optimisé pour les périphériques APIs

Il n'y a aucune exigence spécifique pour la définition du champ Evaluate target health (Évaluer l'état de la cible) sur Yes (Oui) lorsque le point de terminaison est une API régionale personnalisée API Gateway ou une API optimisée pour la périphérie.

CloudFront distributions

Vous ne pouvez pas définir Evaluate target health sur Oui lorsque le point de terminaison est une CloudFront distribution.

Environnements Elastic Beanstalk comportant des sous-domaines régionalisés

Si vous spécifiez un environnement Elastic Beanstalk dans Endpoint et que celui-ci contient un équilibreur de charge ELB, Elastic Load Balancing achemine les requêtes uniquement vers les instances Amazon EC2 saines enregistrées auprès de l'équilibreur de charge. (Un environnement contient automatiquement un équilibreur de charge ELB s'il inclut plusieurs EC2 instances

Amazon.) Si vous définissez Evaluate target health sur Oui et que les EC2 instances Amazon ne sont pas saines ou que l'équilibreur de charge lui-même ne fonctionne pas correctement, Route 53 achemine les requêtes vers d'autres ressources disponibles qui sont saines, le cas échéant.

Si l'environnement contient une seule EC2 instance Amazon, il n'y a aucune exigence particulière.

Equilibreurs de charge ELB

Le comportement de la surveillance de l'état dépend du type de l'équilibreur de charge :

- Équilibreurs de charge classiques : si vous spécifiez un ELB Classic Load Balancer dans Endpoint, Elastic Load Balancing achemine les requêtes uniquement vers les instances EC2 Amazon saines enregistrées auprès de l'équilibreur de charge. Si vous définissez Evaluate target health sur Oui et qu'aucune EC2 instance n'est saine ou que l'équilibreur de charge lui-même est défaillant, Route 53 achemine les requêtes vers d'autres ressources.
- Équilibreurs de charge d'application et Network Load Balancer : si vous spécifiez un équilibreur de charge ELB d'application ou Network Load Balancer et que vous définissez Evaluate Target health (Évaluer l'état de la cible) sur Yes (Oui), Route 53 achemine les requêtes vers l'équilibreur de charge en fonction de l'état des groupes cible associés à l'équilibreur de charge :
  - Pour qu'un équilibreur d'application ou un équilibreur Network Load Balancer soit considéré comme sain, un groupe cible contenant des cibles doit en contenir au moins une saine. Si un groupe cible contient uniquement des cibles qui ne sont pas saines, l'équilibreur de charge est considéré comme étant lui-même défectueux et Route 53 achemine les requêtes vers d'autres ressources.
  - Un groupe cible qui n'a pas de cibles enregistrées est considéré comme non sain.

> **Note**
>
> Lorsque vous créez un équilibreur de charge, vous configurez les paramètres des surveillances de l'état Elastic Load Balancing ; il ne s'agit pas de surveillances de l'état Route 53, mais elles jouent le même rôle. Ne créez pas de bilans de santé Route 53 pour les EC2 instances que vous enregistrez auprès d'un équilibreur de charge ELB.

Compartiments S3

Il n'y a aucune exigence spécifique pour la définition du champ Evaluate target health (Évaluer l'état de la cible) sur Yes (Oui) lorsque le point de terminaison est un compartiment S3.

Points de terminaison de l'interface d'un VPC Amazon

Il n'y a aucune exigence spécifique pour la définition du champ Evaluate target health (Évaluer l'état de la cible) sur Yes (Oui) lorsque le point de terminaison est un point de terminaison d'interface d'un VPC Amazon.

Autres enregistrements dans la même zone hébergée

Si la AWS ressource que vous spécifiez dans Endpoint est un enregistrement ou un groupe d'enregistrements (par exemple, un groupe d'enregistrements pondérés) mais qu'il ne s'agit pas d'un autre enregistrement alias, nous vous recommandons d'associer un bilan de santé à tous les enregistrements du point de terminaison. Pour de plus amples informations, veuillez consulter Que se passe-t-il lorsque vous omettez des surveillances de l'état ?.

ID d'enregistrement

Entrez une valeur qui identifie de façon unique les enregistrements principaux et secondaires.

Valeurs spécifiques aux enregistrements de géolocalisation

Lorsque vous créez des enregistrements de géolocalisation, vous spécifiez les valeurs suivantes.

Rubriques

- Stratégie de routage
- Nom de l'enregistrement
- Type de registre
- TTL (secondes)
- Valeur/acheminer le trafic vers
- Emplacement
- États des États-Unis
- Surveillance de l'état
- ID d'enregistrement

Stratégie de routage

Sélectionnez Geolocation (Géolocalisation).

Nom de l'enregistrement

Saisissez le nom de domaine ou de sous-domaine vers lequel vous souhaitez acheminer le trafic. La valeur par défaut est le nom de la zone hébergée.

> **Note**
>
> Si vous créez un enregistrement qui porte le même nom que la zone hébergée, n'entrez aucune valeur (par exemple, un symbole @) dans le champ Name (Nom).

Entrez le même nom pour tous les enregistrements du groupe d'enregistrements de géolocalisation.

Pour plus d'informations sur les noms d'enregistrements, veuillez consulter Nom de l'enregistrement.

Type de registre

Type d'enregistrement DNS. Pour de plus amples informations, veuillez consulter Types d'enregistrements DNS pris en charge.

Sélectionnez la même valeur pour tous les enregistrements du groupe d'enregistrements de géolocalisation :

TTL (secondes)

Durée, en secondes, pendant laquelle vous voulez que les résolveurs DNS récursifs mettent en cache les informations relatives à cet enregistrement. Si vous spécifiez une valeur plus longue (par exemple, 172 800 secondes, soit deux jours), vous limitez le nombre d'appels que les résolveurs DNS récursifs doivent passer à Route 53 pour obtenir les dernières informations de cet enregistrement. Vous réduisez ainsi la latence et le montant de votre facture pour le service Route 53. Pour de plus amples informations, veuillez consulter Comment Amazon Route 53 achemine le trafic de votre domaine.

Cependant, si vous spécifiez une valeur de durée de vie plus longue, les modifications apportées à l'enregistrement (par exemple, une nouvelle adresse IP) mettent plus de temps à prendre effet, car les résolveurs récursifs utilisent les valeurs qui se trouvent dans leur cache pendant plus longtemps avant de demander les informations les plus récentes à Route 53. Si vous modifiez les paramètres d'un domaine ou d'un sous-domaine déjà utilisé, nous vous conseillons de spécifier initialement une valeur plus courte, par exemple 300 secondes, et d'augmenter la valeur une fois que vous avez vérifié que les nouveaux paramètres sont corrects.

Si vous associez cet enregistrement à une vérification de l'état, nous vous recommandons de spécifier une durée de vie de 60 secondes au maximum afin que les clients répondent rapidement aux modifications de l'état de santé.

Valeur/acheminer le trafic vers

Choisissez IP address or another value depending on the record type (Adresse IP ou autre valeur selon le type d'enregistrement). Entrez une valeur appropriée pour la valeur Record type (Type d'enregistrement). Pour tous les types à l'exception de CNAME, vous pouvez entrer plusieurs valeurs. Entrez chaque valeur sur une ligne distincte.

Vous pouvez acheminer le trafic vers, ou spécifier les valeurs suivantes :

- A — IPv4 adresse
- AAAA — adresse IPv6
- CAA : autorisation de l'autorité de certification
- CNAME : nom canonique
- MX : échange de courrier

- NAPTR : nom d'indicateur d'autorité
- PTR : indicateur
- SPF : cadre de la politique de l'envoyeur
- SRV : localisateur de service
- TXT : texte

Pour plus d'informations sur les valeurs ci-dessus, consultez valeurs communes pour Valeur/Acheminement du trafic vers.

Emplacement

Lorsque vous configurez Route 53 pour qu'il réponde aux requêtes DNS en fonction de leur emplacement d'origine, sélectionnez le continent ou le pays pour lequel vous voulez que Route 53 réponde avec les paramètres figurant dans cet enregistrement. Si vous voulez que Route 53 réponde aux requêtes DNS pour certains États des États-Unis, sélectionnez United States (États-Unis) dans la liste Location (Localisation), puis choisissez l'État sous le groupe Sublocation (Sous-localisation).

Pour une zone hébergée privée, sélectionnez le continent, le pays ou la subdivision le plus proche de Région AWS celui dans lequel se trouve votre ressource. Par exemple, si votre ressource se trouve dans us-east-1, vous pouvez spécifier Amérique du Nord, États-Unis ou Virginie.

> **Important**
>
> Nous vous conseillons de créer un enregistrement de géolocalisation ayant la valeur Default (Par défaut) pour Location (Localisation). Ainsi, les emplacements géographiques pour lesquels vous n'avez pas créé d'enregistrements et les adresses IP dont Route 53 ne peut identifier l'emplacement sont couverts.

Vous ne pouvez pas créer d'enregistrements qui ne sont pas de type géolocalisation en utilisant les mêmes valeurs pour les champs Record name (Nom de l'enregistrement) et Record type (Type d'enregistrement) que celles des enregistrements de géolocalisation.

Pour de plus amples informations, veuillez consulter Routage de géolocalisation.

Voici les pays qu'Amazon Route 53 associe à chaque continent. Les codes des pays suivent la norme ISO 3166. Pour plus d'informations, consultez l'article Wikipédia ISO 3166-1 alpha-2 :

Afrique (AF)

AO, BF, BI, BJ, BW, CD, CF, CG, CI, CM, CV, DJ, DZ, EG, ER, ET, GA, GH, GM, GN, GQ, GW, KE, KM, LR, LS, LY, MA, MG, ML, MR, MU, MW, MZ, NA, NE, NG, RE, RW, SC, SD, SH, SL, SN, SO, SS, ST, SZ, TD, TG, TN, TZ, UG, YT, ZA, ZM, ZW

Antarctique (AN)

AQ, GS, TF

Asie (AS)

AE, AF, AM, AZ, BD, BH, BN, BT, CC, CN, GE, HK, ID, IL, IN, IO, IQ, IR, JO, JP, KG, KH, KP, KR, KW, KZ, LA, LB, LK, MM, MN, MO, MV, MY, NP, OM, PH, PK, PS, QA, SA, SG, SY, TH, TJ, TM, TW, UZ, VN, YE

Europe (EU)

AD, AL, AT, AX, BA, BE, BG, BY, CH, CY, CZ, DE, DK, EE, ES, FI, FO, FR, GB, GG, GI, GR, HR, HU, IE, IM, IS, IT, JE, LI, LT, LU, LV, MC, MD, ME, MK, MT, NL, NO, PL, PT, RO, RS, RU, SE, SI, SJ, SK, SM, TR, UA, VA, XK

> **Note**
>
> Certains fournisseurs considèrent que TR se trouve en Asie et les adresses IP refléteront cela.

Amérique du Nord (NA)

AG, AI, AW, BB, BL, BM, BQ, BS, BZ, CA, CR, CU, CW, DM, DO, GD, GL, GP, GT, HN, HT, JM, KN, KY, LC, MF, MQ, MS, MX, NI, PA, PM, PR, SV, SX, TC, TT, US, VC, VG, VI

Océanie (OC)

AS, AU, CK, FJ, FM, GU, KI, MH, MP, NC, NF, NR, NU, NZ, PF, PG, PN, PW, SB, TK, TL, TO, TV, UM, VU, WF, WS

Amérique du Sud (SA)

AR, BO, BR, CL, CO, EC, FK, GF, GY, PE, PY, SR, UY, VE

> **Note**
>
> Route 53 ne prend pas en charge la création d'enregistrements de géolocalisation pour les pays suivants : Île Bouvet (BV), Île Christmas (CX), Sahara Occidental (EH) et Île et McDonald îles Heard (HM). Aucune donnée n'est disponible sur les adresses IP pour ces pays.

États des États-Unis

Lorsque vous configurez Route 53 pour qu'il réponde aux requêtes DNS en fonction de l'État des États-Unis dont elles proviennent, sélectionnez l'État dans la liste U.S. states (États des États-Unis). Les territoires des Etats-Unis (par exemple, Porto Rico) sont répertoriés en tant que pays dans la liste Localisation.

> **Important**
>
> Certaines adresses IP sont associées aux États-Unis, mais pas à un état individuel. Si vous créez des enregistrements pour tous les États des États-Unis, nous vous recommandons de créer également un enregistrement pour les États-Unis pour acheminer les requêtes pour ces adresses IP non associées. Si vous ne créez pas d'enregistrement pour les États-Unis, Route 53 répond aux requêtes DNS provenant des adresses IP non associées des États-Unis avec les paramètres de l'enregistrement de géolocalisation par défaut (si vous en avez créé un) ou avec un message « aucune réponse ».

Surveillance de l'état

Sélectionnez une surveillance de l'état si vous voulez que Route 53 vérifie l'état d'un point de terminaison spécifique et réponde aux requêtes DNS à l'aide de cet enregistrement uniquement lorsque le point de terminaison est sain.

Route 53 ne vérifie pas l'état du point de terminaison spécifié dans l'enregistrement, par exemple, le point de terminaison indiqué par l'adresse IP dans le champ Value (Valeur). Lorsque vous sélectionnez une surveillance de l'état pour un enregistrement, Route 53 vérifie l'état du point de terminaison que vous avez spécifié dans la surveillance de l'état. Pour plus d'informations sur la façon dont Route 53 détermine si un point de terminaison est sain, consultez Comment Amazon Route 53 détermine si une surveillance de l'état est saine.

L'association d'une surveillance de l'état à un enregistrement est utile uniquement lorsque Route 53 doit choisir entre plusieurs enregistrements pour répondre à une requête DNS et que vous souhaitez que Route 53 base en partie son choix sur le statut d'une surveillance de l'état. Utilisez des surveillances de l'état uniquement dans les configurations suivantes :

- Vous vérifiez l'état de santé de tous les enregistrements d'un groupe d'enregistrements portant le même nom, le même type et la même politique de routage (tels que le basculement ou les enregistrements pondérés), et vous spécifiez un contrôle de santé IDs pour tous les enregistrements. Si la surveillance de l'état d'un enregistrement spécifie un point de terminaison qui n'est pas sain, Route 53 cesse de répondre aux requêtes utilisant la valeur indiquée pour cet enregistrement.
- Vous sélectionnez Yes (Oui) pour Evaluate target health (Évaluer l'état de la cible) pour un enregistrement d'alias ou les enregistrements dans un groupe d'enregistrements d'alias de basculement, d'alias de géolocalisation, d'alias de latence, d'alias basés sur IP ou d'alias pondérés. Si les enregistrements d'alias font référence à des enregistrements sans alias dans une même zone hébergée, vous devez spécifier les surveillances d'état pour les enregistrements référencés. Si vous associez une surveillance de l'état à un enregistrement d'alias et que vous sélectionnez également Yes (Oui) pour Evaluate Target Health (Évaluer l'état de la cible), les deux doivent être évalués à vrai. Pour de plus amples informations, veuillez consulter Que se passe-t-il lorsque vous associez une surveillance de l'état à un enregistrement d'alias ?.

Si vos surveillances de l'état spécifient le point de terminaison uniquement par nom de domaine, nous vous recommandons de créer une surveillance de l'état distincte pour chaque point de terminaison. Par exemple, créez une surveillance de l'état pour chaque serveur HTTP qui diffuse du contenu pour www.example.com. Pour la valeur du champ Nom de domaine, indiquez le nom de domaine du serveur (par exemple, us-east-2-www.example.com), et non pas le nom des enregistrements (example.com).

> **Important**
>
> Dans cette configuration, si vous créez une surveillance de l'état pour laquelle la valeur du champ Nom de domaine correspond au nom des enregistrements et si vous associez ensuite la surveillance de l'état à ces enregistrements, les résultats de la surveillance de l'état seront imprévisibles.

Pour les enregistrements de géolocalisation, si un point de terminaison n'est pas sain, Route 53 recherche un enregistrement pour la région géographique associée de taille supérieure. Par exemple, supposons que vous disposez d'enregistrements pour un État des États-Unis, pour les États-Unis, pour l'Amérique du Nord et pour tous les emplacements (la valeur du champ Location [Emplacement] est Default [Par défaut]). Si le point de terminaison de l'enregistrement de l'État n'est pas sain, Route 53 vérifie les enregistrements pour les États-Unis, pour l'Amérique du Nord, ainsi que pour tous les emplacements, dans cet ordre, jusqu'à ce qu'il trouve un enregistrement comportant un point de terminaison sain. Si tous les enregistrements applicables sont défaillants, y compris l'enregistrement pour tous les emplacements, Route 53 répond à la requête DNS à l'aide de la valeur pour l'enregistrement de la région géographique la plus petite.

ID d'enregistrement

Entrez une valeur qui identifie de manière unique cet enregistrement dans le groupe d'enregistrements de géolocalisation.

Valeurs spécifiques aux enregistrements d'alias de géolocalisation

Lorsque vous créez des enregistrements d'alias de géolocalisation, vous spécifiez les valeurs suivantes.

Pour de plus amples informations, veuillez consulter Choix entre des enregistrements avec ou sans alias.

Rubriques

- Stratégie de routage
- Nom de l'enregistrement
- Type de registre
- Valeur/acheminer le trafic vers
- Emplacement
- États des États-Unis
- Surveillance de l'état
- Évaluer l'état de la cible
- ID d'enregistrement

Stratégie de routage

Sélectionnez Geolocation (Géolocalisation).

Nom de l'enregistrement

Saisissez le nom de domaine ou de sous-domaine vers lequel vous souhaitez acheminer le trafic. La valeur par défaut est le nom de la zone hébergée.

> **Note**
>
> Si vous créez un enregistrement qui porte le même nom que la zone hébergée, n'entrez aucune valeur (par exemple, un symbole @) dans le champ Record name (Nom de l'enregistrement).

Entrez le même nom pour tous les enregistrements du groupe d'enregistrements de géolocalisation.

Pour plus d'informations sur les noms d'enregistrements, veuillez consulter Nom de l'enregistrement.

Type de registre

Type d'enregistrement DNS. Pour de plus amples informations, veuillez consulter Types d'enregistrements DNS pris en charge.

Sélectionnez la valeur applicable en fonction de la AWS ressource vers laquelle vous acheminez le trafic. Sélectionnez la même valeur pour tous les enregistrements du groupe d'enregistrements de géolocalisation :

API régionale personnalisée API Gateway et API optimisée pour la périphérie

Sélectionnez A — IPv4 adresse.

Points de terminaison de l'interface d'un VPC Amazon

Sélectionnez A — IPv4 adresse.

CloudFront distribution

Sélectionnez A — IPv4 adresse.

Si cette option IPv6 est activée pour la distribution, créez deux enregistrements, l'un avec la valeur A — IPv4 adresse pour Type, et l'autre avec la valeur AAAA — IPv6 adresse.

Service App Runner

Sélectionnez A — IPv4 adresse

Environnement Elastic Beanstalk comportant des sous-domaines régionalisés

Sélectionnez A — IPv4 adresse

Équilibreur de charge ELB

Sélectionnez A — IPv4 adresse ou AAAA — IPv6 adresse

Compartiment Amazon S3

Sélectionnez A — IPv4 adresse

OpenSearch Service

Sélectionnez A — IPv4 adresse ou AAAA — IPv6 adresse

Autre enregistrement de cette zone hébergée

Sélectionnez le type d'enregistrement pour lequel vous créez l'alias. Tous les types sont pris en charge, sauf NS et SOA.

> **Note**
>
> Si vous créez un enregistrement d'alias qui a le même nom que la zone hébergée (appelée aussi zone apex), vous ne pouvez pas acheminer le trafic vers un enregistrement dont la valeur pour Type (Type) est CNAME. Cela est dû au fait que l'enregistrement d'alias doit être du même type que l'enregistrement vers lequel vous acheminez le trafic et que la création d'un enregistrement CNAME pour la zone apex n'est pas prise en charge, même pour un enregistrement d'alias.

Valeur/acheminer le trafic vers

La valeur que vous choisissez dans la liste ou que vous saisissez dans le champ dépend de la AWS ressource vers laquelle vous acheminez le trafic.

Pour plus d'informations sur AWS les ressources que vous pouvez cibler, consultezValeur/acheminer le trafic vers.

Pour plus d'informations sur la configuration de Route 53 pour acheminer le trafic vers des AWS ressources spécifiques, consultezAcheminement du trafic Internet vers vos AWS ressources.

Emplacement

Lorsque vous configurez Route 53 pour qu'il réponde aux requêtes DNS en fonction de leur emplacement d'origine, sélectionnez le continent ou le pays pour lequel vous voulez que Route 53 réponde avec les paramètres figurant dans cet enregistrement. Si vous voulez que Route 53 réponde aux requêtes DNS pour certains États des États-Unis, sélectionnez United States (ÉEtats-Unis) dans la liste Location (Localisation), puis choisissez l'État dans la liste U.S. states (États des États-Unis).

Pour une zone hébergée privée, sélectionnez le continent, le pays ou la subdivision le plus proche de Région AWS celui dans lequel se trouve votre ressource. Par exemple, si votre ressource se trouve dans us-east-1, vous pouvez spécifier Amérique du Nord, États-Unis ou Virginie.

> **Important**
>
> Nous vous conseillons de créer un enregistrement de géolocalisation ayant la valeur Default (Par défaut) pour Location (Localisation). Ainsi, les emplacements géographiques pour lesquels vous n'avez pas créé d'enregistrements et les adresses IP dont Route 53 ne peut identifier l'emplacement sont couverts.

Vous ne pouvez pas créer d'enregistrements qui ne sont pas de type géolocalisation en utilisant les mêmes valeurs pour les champs Record name (Nom de l'enregistrement) et Record type (Type d'enregistrement) que celles des enregistrements de géolocalisation.

Pour de plus amples informations, veuillez consulter Routage de géolocalisation.

Voici les pays qu'Amazon Route 53 associe à chaque continent. Les codes des pays suivent la norme ISO 3166. Pour plus d'informations, consultez l'article Wikipédia ISO 3166-1 alpha-2 :

Afrique (AF)

AO, BF, BI, BJ, BW, CD, CF, CG, CI, CM, CV, DJ, DZ, EG, ER, ET, GA, GH, GM, GN, GQ, GW, KE, KM, LR, LS, LY, MA, MG, ML, MR, MU, MW, MZ, NA, NE, NG, RE, RW, SC, SD, SH, SL, SN, SO, SS, ST, SZ, TD, TG, TN, TZ, UG, YT, ZA, ZM, ZW

Antarctique (AN)

AQ, GS, TF

Asie (AS)

AE, AF, AM, AZ, BD, BH, BN, BT, CC, CN, GE, HK, ID, IL, IN, IO, IQ, IR, JO, JP, KG, KH, KP, KR, KW, KZ, LA, LB, LK, MM, MN, MO, MV, MY, NP, OM, PH, PK, PS, QA, SA, SG, SY, TH, TJ, TM, TW, UZ, VN, YE

Europe (EU)

AD, AL, AT, AX, BA, BE, BG, BY, CH, CY, CZ, DE, DK, EE, ES, FI, FO, FR, GB, GG, GI, GR, HR, HU, IE, IM, IS, IT, JE, LI, LT, LU, LV, MC, MD, ME, MK, MT, NL, NO, PL, PT, RO, RS, RU, SE, SI, SJ, SK, SM, TR, UA, VA, XK

> **Note**
>
> Certains fournisseurs considèrent que TR se trouve en Asie et les adresses IP refléteront cela.

Amérique du Nord (NA)

AG, AI, AW, BB, BL, BM, BQ, BS, BZ, CA, CR, CU, CW, DM, DO, GD, GL, GP, GT, HN, HT, JM, KN, KY, LC, MF, MQ, MS, MX, NI, PA, PM, PR, SV, SX, TC, TT, US, VC, VG, VI

Océanie (OC)

AS, AU, CK, FJ, FM, GU, KI, MH, MP, NC, NF, NR, NU, NZ, PF, PG, PN, PW, SB, TK, TL, TO, TV, UM, VU, WF, WS

Amérique du Sud (SA)

AR, BO, BR, CL, CO, EC, FK, GF, GY, PE, PY, SR, UY, VE

> **Note**
>
> Route 53 ne prend pas en charge la création d'enregistrements de géolocalisation pour les pays suivants : Île Bouvet (BV), Île Christmas (CX), Sahara Occidental (EH) et Île et McDonald îles Heard (HM). Aucune donnée n'est disponible sur les adresses IP pour ces pays.

États des États-Unis

Lorsque vous configurez Route 53 pour qu'il réponde aux requêtes DNS en fonction de l'État des États-Unis dont elles proviennent, sélectionnez l'État dans la liste U.S. states (États des États-Unis). Les territoires des Etats-Unis (par exemple, Porto Rico) sont répertoriés en tant que pays dans la liste Localisation.

> **Important**
>
> Certaines adresses IP sont associées aux États-Unis, mais pas à un état individuel. Si vous créez des enregistrements pour tous les États des États-Unis, nous vous recommandons de créer également un enregistrement pour les États-Unis pour acheminer les requêtes pour ces adresses IP non associées. Si vous ne créez pas d'enregistrement pour les États-Unis, Route 53 répond aux requêtes DNS provenant des adresses IP non associées des États-Unis avec les paramètres de l'enregistrement de géolocalisation par défaut (si vous en avez créé un) ou avec un message « aucune réponse ».

Surveillance de l'état

Sélectionnez une surveillance de l'état si vous voulez que Route 53 vérifie l'état d'un point de terminaison spécifique et réponde aux requêtes DNS à l'aide de cet enregistrement uniquement lorsque le point de terminaison est sain.

Route 53 ne vérifie pas l'état du point de terminaison spécifié dans l'enregistrement, par exemple, le point de terminaison indiqué par l'adresse IP dans le champ Value (Valeur). Lorsque vous sélectionnez une surveillance de l'état pour un enregistrement, Route 53 vérifie l'état du point de terminaison que vous avez spécifié dans la surveillance de l'état. Pour plus d'informations sur la façon dont Route 53 détermine si un point de terminaison est sain, consultez Comment Amazon Route 53 détermine si une surveillance de l'état est saine.

L'association d'une surveillance de l'état à un enregistrement est utile uniquement lorsque Route 53 doit choisir entre plusieurs enregistrements pour répondre à une requête DNS et que vous souhaitez que Route 53 base en partie son choix sur le statut d'une surveillance de l'état. Utilisez des surveillances de l'état uniquement dans les configurations suivantes :

- Vous vérifiez l'état de santé de tous les enregistrements d'un groupe d'enregistrements portant le même nom, le même type et la même politique de routage (tels que le basculement ou les enregistrements pondérés), et vous spécifiez un contrôle de santé IDs pour tous les enregistrements. Si la surveillance de l'état d'un enregistrement spécifie un point de terminaison qui n'est pas sain, Route 53 cesse de répondre aux requêtes utilisant la valeur indiquée pour cet enregistrement.
- Vous sélectionnez Yes (Oui) pour Evaluate target health (Évaluer l'état de la cible) pour un enregistrement d'alias ou les enregistrements dans un groupe d'enregistrements d'alias de basculement, d'alias de géolocalisation, d'alias de latence, d'alias basés sur IP, ou d'alias pondérés. Si les enregistrements d'alias font référence à des enregistrements sans alias dans une même zone hébergée, vous devez spécifier les surveillances d'état pour les enregistrements référencés. Si vous associez une surveillance de l'état à un enregistrement d'alias et que vous sélectionnez également Yes (Oui) pour Evaluate Target Health (Évaluer l'état de la cible), les deux doivent être évalués à vrai. Pour de plus amples informations, veuillez consulter Que se passe-t-il lorsque vous associez une surveillance de l'état à un enregistrement d'alias ?.

Si vos surveillances de l'état spécifient le point de terminaison uniquement par nom de domaine, nous vous recommandons de créer une surveillance de l'état distincte pour chaque point de terminaison. Par exemple, créez une surveillance de l'état pour chaque serveur HTTP qui diffuse du contenu pour www.example.com. Pour la valeur du champ Domain name (Nom de domaine), indiquez le nom de domaine du serveur (par exemple, us-east-2-www.example.com), et non pas le nom des enregistrements (example.com).

> **Important**
>
> Dans cette configuration, si vous créez une vérification de l'état pour laquelle la valeur du champ Domain name (Nom de domaine) correspond au nom des enregistrements et si vous associez ensuite la vérification de l'état à ces enregistrements, les résultats de la vérification de l'état seront imprévisibles.

Pour les enregistrements de géolocalisation, si un point de terminaison n'est pas sain, Route 53 recherche un enregistrement pour la région géographique associée de taille supérieure. Par exemple, supposons que vous disposez d'enregistrements pour un État des États-Unis, pour les États-Unis, pour l'Amérique du Nord et pour tous les emplacements (la valeur du champ Location [Emplacement] est Default [Par défaut]). Si le point de terminaison de l'enregistrement de l'État n'est pas sain, Route 53 vérifie les enregistrements pour les États-Unis, pour l'Amérique du Nord, ainsi que pour tous les emplacements, dans cet ordre, jusqu'à ce qu'il trouve un enregistrement comportant un point de terminaison sain. Si tous les enregistrements applicables sont défaillants, y compris l'enregistrement pour tous les emplacements, Route 53 répond à la requête DNS à l'aide de la valeur pour l'enregistrement de la région géographique la plus petite.

Évaluer l'état de la cible

Sélectionnez Yes (Oui) si vous voulez que Route 53 détermine s'il doit répondre aux requêtes DNS à l'aide de cet enregistrement en vérifiant l'état de la ressource spécifiée dans le champ Endpoint (Point de terminaison).

Remarques :

API Gateway personnalisé, régional APIs et optimisé pour les périphériques APIs

Il n'y a aucune exigence spécifique pour la définition du champ Evaluate target health (Évaluer l'état de la cible) sur Yes (Oui) lorsque le point de terminaison est une API régionale personnalisée API Gateway ou une API optimisée pour la périphérie.

CloudFront distributions

Vous ne pouvez pas définir Evaluate target health sur Oui lorsque le point de terminaison est une CloudFront distribution.

Environnements Elastic Beanstalk comportant des sous-domaines régionalisés

Si vous spécifiez un environnement Elastic Beanstalk dans Endpoint et que celui-ci contient un équilibreur de charge ELB, Elastic Load Balancing achemine les requêtes uniquement vers les instances Amazon EC2 saines enregistrées auprès de l'équilibreur de charge. (Un environnement contient automatiquement un équilibreur de charge ELB s'il inclut plusieurs EC2 instances Amazon.) Si vous définissez Evaluate target health sur Oui et que les EC2 instances Amazon ne sont pas saines ou que l'équilibreur de charge lui-même ne fonctionne pas correctement, Route 53 achemine les requêtes vers d'autres ressources disponibles qui sont saines, le cas échéant.

Si l'environnement contient une seule EC2 instance Amazon, il n'y a aucune exigence particulière.

Equilibreurs de charge ELB

Le comportement de la surveillance de l'état dépend du type de l'équilibreur de charge :

- Classic Load Balancers : si vous spécifiez un ELB Classic Load Balancer dans Endpoint, Elastic Load Balancing achemine les requêtes uniquement vers les instances EC2 Amazon saines enregistrées auprès de l'équilibreur de charge. Si vous définissez Evaluate target health sur Oui et qu'aucune EC2 instance n'est saine ou que l'équilibreur de charge lui-même est défaillant, Route 53 achemine les requêtes vers d'autres ressources.
- Équilibreurs de charge d'application et Network Load Balancer : si vous spécifiez un équilibreur de charge ELB d'application ou Network Load Balancer et que vous définissez Evaluate target health (Évaluer l'état de la cible) sur Yes (Oui), Route 53 achemine les requêtes vers l'équilibreur de charge en fonction de l'état des groupes cible associés à l'équilibreur de charge :
  - Pour qu'un équilibreur d'application ou un équilibreur Network Load Balancer soit considéré comme sain, chaque groupe cible contenant des cibles doit en contenir au moins une saine. Si un groupe cible contient uniquement des cibles qui ne sont pas saines, l'équilibreur de charge est considéré comme étant lui-même défectueux et Route 53 achemine les requêtes vers d'autres ressources.
  - Un groupe cible qui n'a pas de cibles enregistrées est considéré comme non sain.

> **Note**
>
> Lorsque vous créez un équilibreur de charge, vous configurez les paramètres des surveillances de l'état Elastic Load Balancing ; il ne s'agit pas de surveillances de l'état Route 53, mais elles jouent le même rôle. Ne créez pas de bilans de santé Route 53 pour les EC2 instances que vous enregistrez auprès d'un équilibreur de charge ELB.

Compartiments S3

Il n'y a aucune exigence spécifique pour la définition du champ Evaluate target health (Évaluer l'état de la cible) sur Yes (Oui) lorsque le point de terminaison est un compartiment S3.

Points de terminaison de l'interface d'un VPC Amazon

Il n'y a aucune exigence spécifique pour la définition du champ Evaluate target health (Évaluer l'état de la cible) sur Yes (Oui) lorsque le point de terminaison est un point de terminaison d'interface d'un VPC Amazon.

Autres enregistrements dans la même zone hébergée

Si la AWS ressource que vous spécifiez dans Endpoint est un enregistrement ou un groupe d'enregistrements (par exemple, un groupe d'enregistrements pondérés) mais qu'il ne s'agit pas d'un autre enregistrement alias, nous vous recommandons d'associer un bilan de santé à tous les enregistrements du point de terminaison. Pour de plus amples informations, veuillez consulter Que se passe-t-il lorsque vous omettez des surveillances de l'état ?.

ID d'enregistrement

Entrez une valeur qui identifie de manière unique cet enregistrement dans le groupe d'enregistrements de géolocalisation.

Valeurs spécifiques aux enregistrements de géoproximité

Lorsque vous créez des enregistrements de géoproximité, vous spécifiez les valeurs suivantes.

Rubriques

- Stratégie de routage
- Nom de l'enregistrement
- Type de registre
- TTL (secondes)
- Valeur/acheminer le trafic vers
- Emplacement du point de terminaison
- Écart
- Surveillance de l'état
- ID d'enregistrement

Stratégie de routage

Choisissez Geoproximity.

Nom de l'enregistrement

Saisissez le nom de domaine ou de sous-domaine vers lequel vous souhaitez acheminer le trafic. La valeur par défaut est le nom de la zone hébergée.

> **Note**
>
> Si vous créez un enregistrement qui porte le même nom que la zone hébergée, n'entrez aucune valeur (par exemple, un symbole @) dans le champ Name (Nom).

Entrez le même nom pour tous les enregistrements du groupe d'enregistrements de géoproximité.

Pour plus d'informations sur les noms d'enregistrements, veuillez consulter Nom de l'enregistrement.

Type de registre

Type d'enregistrement DNS. Pour de plus amples informations, veuillez consulter Types d'enregistrements DNS pris en charge.

Sélectionnez la même valeur pour tous les enregistrements du groupe d'enregistrements de géoproximité.

TTL (secondes)

Durée, en secondes, pendant laquelle vous voulez que les résolveurs DNS récursifs mettent en cache les informations relatives à cet enregistrement. Si vous spécifiez une valeur plus longue (par exemple, 172 800 secondes, soit deux jours), vous limitez le nombre d'appels que les résolveurs DNS récursifs doivent passer à Route 53 pour obtenir les dernières informations de cet enregistrement. Vous réduisez ainsi la latence et le montant de votre facture pour le service Route 53. Pour de plus amples informations, veuillez consulter Comment Amazon Route 53 achemine le trafic de votre domaine.

Cependant, si vous spécifiez une valeur de durée de vie plus longue, les modifications apportées à l'enregistrement (par exemple, une nouvelle adresse IP) mettent plus de temps à prendre effet, car les résolveurs récursifs utilisent les valeurs qui se trouvent dans leur cache pendant plus longtemps avant de demander les informations les plus récentes à Route 53. Si vous modifiez les paramètres d'un domaine ou d'un sous-domaine déjà utilisé, nous vous conseillons de spécifier initialement une valeur plus courte, par exemple 300 secondes, et d'augmenter la valeur une fois que vous avez vérifié que les nouveaux paramètres sont corrects.

Si vous associez cet enregistrement à une vérification de l'état, nous vous recommandons de spécifier une durée de vie de 60 secondes au maximum afin que les clients répondent rapidement aux modifications de l'état de santé.

Valeur/acheminer le trafic vers

Choisissez IP address or another value depending on the record type (Adresse IP ou autre valeur selon le type d'enregistrement). Entrez une valeur appropriée pour la valeur Record type (Type d'enregistrement). Pour tous les types à l'exception de CNAME, vous pouvez entrer plusieurs valeurs. Entrez chaque valeur sur une ligne distincte.

Vous pouvez acheminer le trafic vers, ou spécifier les valeurs suivantes :

- A — IPv4 adresse
- AAAA — adresse IPv6
- CAA : autorisation de l'autorité de certification
- CNAME : nom canonique

- MX : échange de courrier
- NAPTR : nom d'indicateur d'autorité
- PTR : indicateur
- SPF : cadre de la politique de l'envoyeur
- SRV : localisateur de service
- TXT : texte

Pour plus d'informations sur les valeurs ci-dessus, consultez valeurs communes pour Valeur/Acheminement du trafic vers.

Emplacement du point de terminaison

Vous pouvez spécifier l'emplacement du point de terminaison de la ressource en utilisant l'une des méthodes suivantes :

Coordonnées personnalisées

Spécifiez la longitude et la latitude d'une zone géographique.

Région AWS

Choisissez une région disponible dans la liste des emplacements.

Pour plus d'informations sur les régions, consultez la section Infrastructure AWS mondiale.

AWS Groupe de zones local

Choisissez un groupe de zones local disponible dans la liste des emplacements.

Pour plus d'informations sur les zones locales, consultez la section Zones locales disponibles dans le guide de l'utilisateur des zones AWS locales. Un groupe de zones local est généralement la zone locale sans le caractère final. Par exemple, si la zone locale est `us-east-1-bue-1a` le groupe de zones local l'est`us-east-1-bue-1`.

Vous pouvez également identifier le groupe de zones locales pour une zone locale spécifique à l'aide de la commande describe-availability-zonesCLI :

```
aws ec2 describe-availability-zones --region us-west-2 --all-availability-zones --query
 "AvailabilityZones[?ZoneName=='us-west-2-den-1a']" | grep "GroupName"
```

Cette commande renvoie :`"GroupName": "us-west-2-den-1"`, en spécifiant que la zone locale `us-west-2-den-1a` appartient au groupe de zones localesus-west-2-den-1.

Vous ne pouvez pas créer d'enregistrements non liés à la géoproximité ayant les mêmes valeurs pour le nom et le type d'enregistrement que pour les enregistrements de géoproximité.

Vous ne pouvez pas non plus créer deux jeux d'enregistrements de ressources de géoproximité qui spécifient le même emplacement pour le même nom et le même type d'enregistrement.

Écart

Un biais étend ou réduit une zone géographique à partir de laquelle la Route 53 achemine le trafic vers une ressource. Un biais positif élargit la zone et un biais négatif la réduit. Pour de plus amples informations, veuillez consulter Comment Amazon Route 53 utilise une valeur d'écart pour acheminer le trafic.

Surveillance de l'état

Sélectionnez une surveillance de l'état si vous voulez que Route 53 vérifie l'état d'un point de terminaison spécifique et réponde aux requêtes DNS à l'aide de cet enregistrement uniquement lorsque le point de terminaison est sain.

Route 53 ne vérifie pas l'état du point de terminaison spécifié dans l'enregistrement, par exemple, le point de terminaison indiqué par l'adresse IP dans le champ Value (Valeur). Lorsque vous sélectionnez une surveillance de l'état pour un enregistrement, Route 53 vérifie l'état du point de terminaison que vous avez spécifié dans la surveillance de l'état. Pour plus d'informations sur la façon dont Route 53 détermine si un point de terminaison est sain, consultez Comment Amazon Route 53 détermine si une surveillance de l'état est saine.

L'association d'une surveillance de l'état à un enregistrement est utile uniquement lorsque Route 53 doit choisir entre plusieurs enregistrements pour répondre à une requête DNS et que vous souhaitez que Route 53 base en partie son choix sur le statut d'une surveillance de l'état. Utilisez des surveillances de l'état uniquement dans les configurations suivantes :

- Vous vérifiez l'état de santé de tous les enregistrements d'un groupe d'enregistrements portant le même nom, le même type et la même politique de routage (tels que le basculement ou les enregistrements pondérés), et vous spécifiez un contrôle de santé IDs pour tous les enregistrements. Si la surveillance de l'état d'un enregistrement spécifie un point de terminaison qui n'est pas sain, Route 53 cesse de répondre aux requêtes utilisant la valeur indiquée pour cet enregistrement.

- Vous sélectionnez Oui pour Evaluate Target Health pour un enregistrement d'alias ou pour les enregistrements d'un groupe composé d'alias de basculement, d'alias de géolocalisation, d'alias de géoproximité, d'alias de latence, d'alias basé sur IP ou d'enregistrement d'alias pondéré. Si les enregistrements d'alias font référence à des enregistrements sans alias dans une même zone hébergée, vous devez spécifier les surveillances d'état pour les enregistrements référencés. Si vous associez une surveillance de l'état à un enregistrement d'alias et que vous sélectionnez également Yes (Oui) pour Evaluate Target Health (Évaluer l'état de la cible), les deux doivent être évalués à vrai. Pour de plus amples informations, veuillez consulter Que se passe-t-il lorsque vous associez une surveillance de l'état à un enregistrement d'alias ?.

Si vos surveillances de l'état spécifient le point de terminaison uniquement par nom de domaine, nous vous recommandons de créer une surveillance de l'état distincte pour chaque point de terminaison. Par exemple, créez une surveillance de l'état pour chaque serveur HTTP qui diffuse du contenu pour www.example.com. Pour la valeur du champ Nom de domaine, indiquez le nom de domaine du serveur (par exemple, us-east-2-www.example.com), et non pas le nom des enregistrements (example.com).

> **Important**
>
> Dans cette configuration, si vous créez une surveillance de l'état pour laquelle la valeur du champ Nom de domaine correspond au nom des enregistrements et si vous associez ensuite la surveillance de l'état à ces enregistrements, les résultats de la surveillance de l'état seront imprévisibles.

Pour les enregistrements de géoproximité, si un point de terminaison est défectueux, Route 53 recherche le point de terminaison le plus proche qui est toujours sain.

ID d'enregistrement

Entrez une valeur identifiant de manière unique cet enregistrement dans le groupe d'enregistrements de géoproximité.

Valeurs spécifiques aux enregistrements d'alias de géoproximité

Lorsque vous créez des enregistrements d'alias de géoproximité, vous spécifiez les valeurs suivantes.

Pour de plus amples informations, veuillez consulter Choix entre des enregistrements avec ou sans alias.

Rubriques

- Stratégie de routage
- Nom de l'enregistrement
- Type de registre
- Valeur/acheminer le trafic vers
- Emplacement du point de terminaison
- Écart
- Surveillance de l'état
- Évaluer l'état de la cible
- ID d'enregistrement

Stratégie de routage

Choisissez Geoproximity.

Nom de l'enregistrement

Saisissez le nom de domaine ou de sous-domaine vers lequel vous souhaitez acheminer le trafic. La valeur par défaut est le nom de la zone hébergée.

> **Note**
>
> Si vous créez un enregistrement qui porte le même nom que la zone hébergée, n'entrez aucune valeur (par exemple, un symbole @) dans le champ Record name (Nom de l'enregistrement).

Entrez le même nom pour tous les enregistrements du groupe d'enregistrements de géoproximité.

Pour plus d'informations sur les noms d'enregistrements, veuillez consulter Nom de l'enregistrement.

Type de registre

Type d'enregistrement DNS. Pour de plus amples informations, veuillez consulter Types d'enregistrements DNS pris en charge.

Sélectionnez la valeur applicable en fonction de la AWS ressource vers laquelle vous acheminez le trafic. Sélectionnez la même valeur pour tous les enregistrements du groupe d'enregistrements de géoproximité :

API régionale personnalisée API Gateway et API optimisée pour la périphérie

Sélectionnez A — IPv4 adresse.

Points de terminaison de l'interface d'un VPC Amazon

Sélectionnez A — IPv4 adresse.

CloudFront distribution

Sélectionnez A — IPv4 adresse.

Si cette option IPv6 est activée pour la distribution, créez deux enregistrements, l'un avec la valeur A — IPv4 adresse pour Type, et l'autre avec la valeur AAAA — IPv6 adresse.

Service App Runner

Sélectionnez A — IPv4 adresse

Environnement Elastic Beanstalk comportant des sous-domaines régionalisés

Sélectionnez A — IPv4 adresse

ELB load balancer

Sélectionnez A — IPv4 adresse ou AAAA — IPv6 adresse

Compartiment Amazon S3

Sélectionnez A — IPv4 adresse

OpenSearch Service

Sélectionnez A — IPv4 adresse ou AAAA — IPv6 adresse

Autre enregistrement de cette zone hébergée

Sélectionnez le type d'enregistrement pour lequel vous créez l'alias. Tous les types sont pris en charge, sauf NS et SOA.

> **Note**
>
> Si vous créez un enregistrement d'alias qui a le même nom que la zone hébergée (appelée aussi zone apex), vous ne pouvez pas acheminer le trafic vers un enregistrement dont la valeur pour Type (Type) est CNAME. Cela est dû au fait que l'enregistrement d'alias doit être du même type que l'enregistrement vers lequel vous acheminez le trafic et que la création d'un enregistrement CNAME pour la zone apex n'est pas prise en charge, même pour un enregistrement d'alias.

Valeur/acheminer le trafic vers

La valeur que vous choisissez dans la liste ou que vous saisissez dans le champ dépend de la AWS ressource vers laquelle vous acheminez le trafic.

Pour plus d'informations sur AWS les ressources que vous pouvez cibler, consultezValeur/acheminer le trafic vers.

Pour plus d'informations sur la façon de configurer Route 53 pour acheminer le trafic vers des AWS ressources spécifiques, consultezAcheminement du trafic Internet vers vos AWS ressources.

Emplacement du point de terminaison

Vous pouvez spécifier l'emplacement du point de terminaison de la ressource en utilisant l'une des méthodes suivantes :

Coordonnées personnalisées

Spécifiez la longitude et la latitude d'une zone géographique.

Région AWS

Choisissez une région disponible dans la liste des emplacements.

Pour plus d'informations sur les régions, consultez la section Infrastructure AWS mondiale.

AWS Groupe de zones local

Choisissez une région de zone locale disponible dans la liste des emplacements.

Pour plus d'informations sur les zones locales, consultez la section Zones locales disponibles dans le guide de l'utilisateur des zones AWS locales. Un groupe de zones local est généralement la zone locale sans le caractère final. Par exemple, si la zone locale est `us-east-1-bue-1a` le groupe de zones local l'est`us-east-1-bue-1`.

Vous pouvez également identifier le groupe de zones locales pour une zone locale spécifique à l'aide de la commande describe-availability-zonesCLI :

```
aws ec2 describe-availability-zones --region us-west-2 --all-availability-zones --query
 "AvailabilityZones[?ZoneName=='us-west-2-den-1a']" | grep "GroupName"
```

Cette commande renvoie :`"GroupName": "us-west-2-den-1"`, en spécifiant que la zone locale `us-west-2-den-1a` appartient au groupe de zones localesus-west-2-den-1.

Vous ne pouvez pas créer d'enregistrements non liés à la géoproximité ayant les mêmes valeurs pour le nom et le type d'enregistrement que pour les enregistrements de géoproximité.

Vous ne pouvez pas non plus créer deux jeux d'enregistrements de ressources de géoproximité qui spécifient le même emplacement pour le même nom et le même type d'enregistrement.

Pour plus d'informations, voir available-local-zones .html

Écart

Un biais étend ou réduit une zone géographique à partir de laquelle la Route 53 achemine le trafic vers une ressource. Un biais positif élargit la zone et un biais négatif la réduit. Pour de plus amples informations, veuillez consulter Comment Amazon Route 53 utilise une valeur d'écart pour acheminer le trafic.

Surveillance de l'état

Sélectionnez une surveillance de l'état si vous voulez que Route 53 vérifie l'état d'un point de terminaison spécifique et réponde aux requêtes DNS à l'aide de cet enregistrement uniquement lorsque le point de terminaison est sain.

Route 53 ne vérifie pas l'état du point de terminaison spécifié dans l'enregistrement, par exemple, le point de terminaison indiqué par l'adresse IP dans le champ Value (Valeur). Lorsque vous sélectionnez une surveillance de l'état pour un enregistrement, Route 53 vérifie l'état du point de terminaison que vous avez spécifié dans la surveillance de l'état. Pour plus d'informations sur la

façon dont Route 53 détermine si un point de terminaison est sain, consultez Comment Amazon Route 53 détermine si une surveillance de l'état est saine.

L'association d'une surveillance de l'état à un enregistrement est utile uniquement lorsque Route 53 doit choisir entre plusieurs enregistrements pour répondre à une requête DNS et que vous souhaitez que Route 53 base en partie son choix sur le statut d'une surveillance de l'état. Utilisez des surveillances de l'état uniquement dans les configurations suivantes :

- Vous vérifiez l'état de santé de tous les enregistrements d'un groupe d'enregistrements portant le même nom, le même type et la même politique de routage (tels que le basculement ou les enregistrements pondérés), et vous spécifiez un contrôle de santé IDs pour tous les enregistrements. Si la surveillance de l'état d'un enregistrement spécifie un point de terminaison qui n'est pas sain, Route 53 cesse de répondre aux requêtes utilisant la valeur indiquée pour cet enregistrement.
- Vous sélectionnez Oui pour évaluer l'état de santé de la cible pour un enregistrement d'alias ou les enregistrements d'un groupe d'alias de basculement, d'alias de géolocalisation, d'alias de géoproximité, d'alias de latence, d'alias basé sur l'IP ou d'enregistrement d'alias pondéré. Si les enregistrements d'alias font référence à des enregistrements sans alias dans une même zone hébergée, vous devez spécifier les surveillances d'état pour les enregistrements référencés. Si vous associez une surveillance de l'état à un enregistrement d'alias et que vous sélectionnez également Yes (Oui) pour Evaluate Target Health (Évaluer l'état de la cible), les deux doivent être évalués à vrai. Pour de plus amples informations, veuillez consulter Que se passe-t-il lorsque vous associez une surveillance de l'état à un enregistrement d'alias ?.

Si vos surveillances de l'état spécifient le point de terminaison uniquement par nom de domaine, nous vous recommandons de créer une surveillance de l'état distincte pour chaque point de terminaison. Par exemple, créez une surveillance de l'état pour chaque serveur HTTP qui diffuse du contenu pour www.example.com. Pour la valeur du champ Domain name (Nom de domaine), indiquez le nom de domaine du serveur (par exemple, us-east-2-www.example.com), et non pas le nom des enregistrements (example.com).

> **Important**
>
> Dans cette configuration, si vous créez une vérification de l'état pour laquelle la valeur du champ Domain name (Nom de domaine) correspond au nom des enregistrements et si vous associez ensuite la vérification de l'état à ces enregistrements, les résultats de la vérification de l'état seront imprévisibles.

Pour les enregistrements de géoproximité, si un point de terminaison est défectueux, Route 53 recherche le point de terminaison le plus proche qui est toujours sain.

Évaluer l'état de la cible

Sélectionnez Yes (Oui) si vous voulez que Route 53 détermine s'il doit répondre aux requêtes DNS à l'aide de cet enregistrement en vérifiant l'état de la ressource spécifiée dans le champ Endpoint (Point de terminaison).

Remarques :

API Gateway personnalisé, régional APIs et optimisé pour les périphériques APIs

Il n'y a aucune exigence spécifique pour la définition du champ Evaluate target health (Évaluer l'état de la cible) sur Yes (Oui) lorsque le point de terminaison est une API régionale personnalisée API Gateway ou une API optimisée pour la périphérie.

CloudFront distributions

Vous ne pouvez pas définir Evaluate target health sur Oui lorsque le point de terminaison est une CloudFront distribution.

Environnements Elastic Beanstalk comportant des sous-domaines régionalisés

Si vous spécifiez un environnement Elastic Beanstalk dans Endpoint et que celui-ci contient un équilibreur de charge ELB, Elastic Load Balancing achemine les requêtes uniquement vers les instances Amazon EC2 saines enregistrées auprès de l'équilibreur de charge. (Un environnement contient automatiquement un équilibreur de charge ELB s'il inclut plusieurs EC2 instances Amazon.) Si vous définissez Evaluate target health sur Oui et que les EC2 instances Amazon ne sont pas saines ou que l'équilibreur de charge lui-même ne fonctionne pas correctement, Route 53 achemine les requêtes vers d'autres ressources disponibles qui sont saines, le cas échéant.

Si l'environnement contient une seule EC2 instance Amazon, il n'y a aucune exigence particulière.

Equilibreurs de charge ELB

Le comportement de la surveillance de l'état dépend du type de l'équilibreur de charge :

- Classic Load Balancers : si vous spécifiez un ELB Classic Load Balancer dans Endpoint, Elastic Load Balancing achemine les requêtes uniquement vers les instances EC2 Amazon saines enregistrées auprès de l'équilibreur de charge. Si vous définissez Evaluate target health sur Oui et qu'aucune EC2 instance n'est saine ou que l'équilibreur de charge lui-même est défaillant, Route 53 achemine les requêtes vers d'autres ressources.

- Équilibreurs de charge d'application et Network Load Balancer : si vous spécifiez un équilibreur de charge ELB d'application ou Network Load Balancer et que vous définissez Evaluate target health (Évaluer l'état de la cible) sur Yes (Oui), Route 53 achemine les requêtes vers l'équilibreur de charge en fonction de l'état des groupes cible associés à l'équilibreur de charge :
  - Pour qu'un équilibreur d'application ou un équilibreur Network Load Balancer soit considéré comme sain, chaque groupe cible contenant des cibles doit en contenir au moins une saine. Si un groupe cible contient uniquement des cibles qui ne sont pas saines, l'équilibreur de charge est considéré comme étant lui-même défectueux et Route 53 achemine les requêtes vers d'autres ressources.
  - Un groupe cible qui n'a pas de cibles enregistrées est considéré comme non sain.

> **Note**
>
> Lorsque vous créez un équilibreur de charge, vous configurez les paramètres des surveillances de l'état Elastic Load Balancing ; il ne s'agit pas de surveillances de l'état Route 53, mais elles jouent le même rôle. Ne créez pas de bilans de santé Route 53 pour les EC2 instances que vous enregistrez auprès d'un équilibreur de charge ELB.

Compartiments S3

Il n'y a aucune exigence spécifique pour la définition du champ Evaluate target health (Évaluer l'état de la cible) sur Yes (Oui) lorsque le point de terminaison est un compartiment S3.

Points de terminaison de l'interface d'un VPC Amazon

Il n'y a aucune exigence spécifique pour la définition du champ Evaluate target health (Évaluer l'état de la cible) sur Yes (Oui) lorsque le point de terminaison est un point de terminaison d'interface d'un VPC Amazon.

Autres enregistrements dans la même zone hébergée

Si la AWS ressource que vous spécifiez dans Endpoint est un enregistrement ou un groupe d'enregistrements (par exemple, un groupe d'enregistrements pondérés) mais qu'il ne s'agit pas d'un autre enregistrement alias, nous vous recommandons d'associer un bilan de santé à tous les enregistrements du point de terminaison. Pour de plus amples informations, veuillez consulter Que se passe-t-il lorsque vous omettez des surveillances de l'état ?.

ID d'enregistrement

Entrez une valeur identifiant de manière unique cet enregistrement dans le groupe d'enregistrements de géoproximité.

Valeurs spécifiques aux enregistrements de latence

Lorsque vous créez des enregistrements de latence, vous spécifiez les valeurs suivantes.

Rubriques

- Stratégie de routage
- Nom de l'enregistrement
- Type de registre
- TTL (secondes)
- Valeur/acheminer le trafic vers
- Région
- Surveillance de l'état
- ID d'enregistrement

Stratégie de routage

Choisissez Latency (Latence).

Nom de l'enregistrement

Saisissez le nom de domaine ou de sous-domaine vers lequel vous souhaitez acheminer le trafic. La valeur par défaut est le nom de la zone hébergée.

> **Note**
>
> Si vous créez un enregistrement qui porte le même nom que la zone hébergée, n'entrez aucune valeur (par exemple, un symbole @) dans le champ Record name (Nom de l'enregistrement).

Entrez le même nom pour tous les enregistrements du groupe d'enregistrements de latence.

Pour plus d'informations sur les noms d'enregistrements, veuillez consulter Nom de l'enregistrement.

Type de registre

Type d'enregistrement DNS. Pour de plus amples informations, veuillez consulter Types d'enregistrements DNS pris en charge.

Sélectionnez la valeur pour le champ Type en fonction de la façon dont vous voulez que Route 53 réponde aux requêtes DNS.

Sélectionnez la même valeur pour tous les enregistrements du groupe d'enregistrements de latence.

TTL (secondes)

Durée, en secondes, pendant laquelle vous voulez que les résolveurs DNS récursifs mettent en cache les informations relatives à cet enregistrement. Si vous spécifiez une valeur plus longue (par exemple, 172 800 secondes, soit deux jours), vous limitez le nombre d'appels que les résolveurs DNS récursifs doivent passer à Route 53 pour obtenir les dernières informations de cet enregistrement. Vous réduisez ainsi la latence et le montant de votre facture pour le service Route 53. Pour de plus amples informations, veuillez consulter Comment Amazon Route 53 achemine le trafic de votre domaine.

Cependant, si vous spécifiez une valeur de durée de vie plus longue, les modifications apportées à l'enregistrement (par exemple, une nouvelle adresse IP) mettent plus de temps à prendre effet, car les résolveurs récursifs utilisent les valeurs qui se trouvent dans leur cache pendant plus longtemps avant de demander les informations les plus récentes à Route 53. Si vous modifiez les paramètres d'un domaine ou d'un sous-domaine déjà utilisé, nous vous conseillons de spécifier initialement une valeur plus courte, par exemple 300 secondes, et d'augmenter la valeur une fois que vous avez vérifié que les nouveaux paramètres sont corrects.

Si vous associez cet enregistrement à une vérification de l'état, nous vous recommandons de spécifier une durée de vie de 60 secondes au maximum afin que les clients répondent rapidement aux modifications de l'état de santé.

Valeur/acheminer le trafic vers

Choisissez IP address or another value depending on the record type (Adresse IP ou autre valeur selon le type d'enregistrement). Entrez une valeur appropriée pour la valeur Record type (Type d'enregistrement). Pour tous les types à l'exception de CNAME, vous pouvez entrer plusieurs valeurs. Entrez chaque valeur sur une ligne distincte.

Vous pouvez acheminer le trafic vers, ou spécifier les valeurs suivantes :

- A — IPv4 adresse
- AAAA — adresse IPv6
- CAA : autorisation de l'autorité de certification
- CNAME : nom canonique

- MX : échange de courrier
- NAPTR : nom d'indicateur d'autorité
- PTR : indicateur
- SPF : cadre de la politique de l'envoyeur
- SRV : localisateur de service
- TXT : texte

Pour plus d'informations sur les valeurs ci-dessus, consultez valeurs communes pour Valeur/Acheminement du trafic vers.

Région

La EC2 région Amazon dans laquelle réside la ressource que vous avez spécifiée dans cet enregistrement. Route 53 recommande une EC2 région Amazon en fonction des autres valeurs que vous avez spécifiées. Cela s'applique également aux zones hébergées privées. Nous vous conseillons de pas modifier cette valeur.

Remarques :

- Vous ne pouvez créer qu'un seul enregistrement de latence pour chaque EC2 région Amazon.
- Vous n'êtes pas obligé de créer des enregistrements de latence pour toutes les EC2 régions Amazon. Route 53 choisit la région dotée de la meilleure latence parmi les régions pour lesquelles vous créez des enregistrements de latence.
- Vous ne pouvez pas créer des enregistrements qui ne sont pas de type latence en utilisant les mêmes valeurs pour les champs Record name (Nom de l'enregistrement) et Record type (Type d'enregistrement) que celles des enregistrements de latence.
- Si vous créez un enregistrement balisé avec la région cn-north-1, Route 53 répond toujours aux requêtes en provenance de Chine en utilisant cet enregistrement, quelle que soit la latence.

Pour plus d'informations sur l'utilisation des enregistrements de latence, consultez Routage basé sur la latence.

Surveillance de l'état

Sélectionnez une surveillance de l'état si vous voulez que Route 53 vérifie l'état d'un point de terminaison spécifique et réponde aux requêtes DNS à l'aide de cet enregistrement uniquement lorsque le point de terminaison est sain.

Route 53 ne vérifie pas l'état du point de terminaison spécifié dans l'enregistrement, par exemple, le point de terminaison indiqué par l'adresse IP dans le champ Value (Valeur). Lorsque vous sélectionnez une surveillance de l'état pour un enregistrement, Route 53 vérifie l'état du point de terminaison que vous avez spécifié dans la surveillance de l'état. Pour plus d'informations sur la façon dont Route 53 détermine si un point de terminaison est sain, consultez Comment Amazon Route 53 détermine si une surveillance de l'état est saine.

L'association d'une surveillance de l'état à un enregistrement est utile uniquement lorsque Route 53 doit choisir entre plusieurs enregistrements pour répondre à une requête DNS et que vous souhaitez que Route 53 base en partie son choix sur le statut d'une surveillance de l'état. Utilisez des surveillances de l'état uniquement dans les configurations suivantes :

- Vous vérifiez l'état de santé de tous les enregistrements d'un groupe d'enregistrements portant le même nom, le même type et la même politique de routage (tels que le basculement ou les enregistrements pondérés), et vous spécifiez un contrôle de santé IDs pour tous les enregistrements. Si la surveillance de l'état d'un enregistrement spécifie un point de terminaison qui n'est pas sain, Route 53 cesse de répondre aux requêtes utilisant la valeur indiquée pour cet enregistrement.
- Vous sélectionnez Yes (Oui) pour Evaluate target health (Évaluer l'état de la cible) pour un enregistrement d'alias ou les enregistrements dans un groupe d'enregistrements d'alias de basculement, d'alias de géolocalisation, d'alias de latence, d'alias basés sur IP, ou d'alias pondérés. Si les enregistrements d'alias font référence à des enregistrements sans alias dans une même zone hébergée, vous devez spécifier les surveillances d'état pour les enregistrements référencés. Si vous associez une surveillance de l'état à un enregistrement d'alias et que vous sélectionnez également Yes (Oui) pour Evaluate Target Health (Évaluer l'état de la cible), les deux doivent être évalués à vrai. Pour de plus amples informations, veuillez consulter Que se passe-t-il lorsque vous associez une surveillance de l'état à un enregistrement d'alias ?.

Si vos surveillances de l'état spécifient le point de terminaison uniquement par nom de domaine, nous vous recommandons de créer une surveillance de l'état distincte pour chaque point de terminaison. Par exemple, créez une surveillance de l'état pour chaque serveur HTTP qui diffuse du contenu pour www.example.com. Pour la valeur du champ Domain name (Nom de domaine), indiquez le nom de domaine du serveur (par exemple, us-east-2-www.example.com), et non pas le nom des enregistrements (example.com).

> **Important**
>
> Dans cette configuration, si vous créez une vérification de l'état pour laquelle la valeur du champ Domain name (Nom de domaine) correspond au nom des enregistrements et si vous associez ensuite la vérification de l'état à ces enregistrements, les résultats de la vérification de l'état seront imprévisibles.

ID d'enregistrement

Entrez une valeur qui identifie de manière unique cet enregistrement dans le groupe d'enregistrements de latence.

Valeurs spécifiques aux enregistrements d'alias de latence

Lorsque vous créez des enregistrements d'alias de latence, vous spécifiez les valeurs suivantes.

Pour de plus amples informations, veuillez consulter Choix entre des enregistrements avec ou sans alias.

Rubriques

- Stratégie de routage
- Nom de l'enregistrement
- Type de registre
- Valeur/acheminer le trafic vers
- Région
- Surveillance de l'état
- Évaluer l'état de la cible
- ID d'enregistrement

Stratégie de routage

Choisissez Latency (Latence).

Nom de l'enregistrement

Saisissez le nom de domaine ou de sous-domaine vers lequel vous souhaitez acheminer le trafic. La valeur par défaut est le nom de la zone hébergée.

> **Note**
>
> Si vous créez un enregistrement qui porte le même nom que la zone hébergée, n'entrez aucune valeur (par exemple, un symbole @) dans le champ Record name (Nom de l'enregistrement).

Entrez le même nom pour tous les enregistrements du groupe d'enregistrements de latence.

Pour plus d'informations sur les noms d'enregistrements, veuillez consulter Nom de l'enregistrement

Type de registre

Type d'enregistrement DNS. Pour de plus amples informations, veuillez consulter Types d'enregistrements DNS pris en charge.

Sélectionnez la valeur applicable en fonction de la AWS ressource vers laquelle vous acheminez le trafic :

API régionale personnalisée API Gateway et API optimisée pour la périphérie

Sélectionnez A — IPv4 adresse.

Points de terminaison de l'interface d'un VPC Amazon

Sélectionnez A — IPv4 adresse.

CloudFront distribution

Sélectionnez A — IPv4 adresse.

Si cette option IPv6 est activée pour la distribution, créez deux enregistrements, l'un avec la valeur A — IPv4 adresse pour Type, et l'autre avec la valeur AAAA — IPv6 adresse.

Service App Runner

Sélectionnez A — IPv4 adresse

Environnement Elastic Beanstalk comportant des sous-domaines régionalisés

Sélectionnez A — IPv4 adresse

ELB load balancer

Sélectionnez A — IPv4 adresse ou AAAA — IPv6 adresse

Compartiment Amazon S3

Sélectionnez A — IPv4 adresse

OpenSearch Service

Sélectionnez A — IPv4 adresse ou AAAA — IPv6 adresse

Autre enregistrement de cette zone hébergée

Sélectionnez le type d'enregistrement pour lequel vous créez l'alias. Tous les types sont pris en charge, sauf NS et SOA.

> **Note**
>
> Si vous créez un enregistrement d'alias qui a le même nom que la zone hébergée (appelée aussi zone apex), vous ne pouvez pas acheminer le trafic vers un enregistrement dont la valeur pour Type (Type) est CNAME. Cela est dû au fait que l'enregistrement d'alias doit être du même type que l'enregistrement vers lequel vous acheminez le trafic et que la création d'un enregistrement CNAME pour la zone apex n'est pas prise en charge, même pour un enregistrement d'alias.

Sélectionnez la même valeur pour tous les enregistrements du groupe d'enregistrements de latence.

Valeur/acheminer le trafic vers

La valeur que vous choisissez dans la liste ou que vous saisissez dans le champ dépend de la AWS ressource vers laquelle vous acheminez le trafic.

Pour plus d'informations sur les AWS ressources que vous pouvez cibler, consultez les valeurs communes des enregistrements d'alias destinés au trafic de valeurs/d'itinéraires.

Pour plus d'informations sur la configuration de Route 53 pour acheminer le trafic vers des AWS ressources spécifiques, consultezAcheminement du trafic Internet vers vos AWS ressources.

Région

La EC2 région Amazon dans laquelle réside la ressource que vous avez spécifiée dans cet enregistrement. Route 53 recommande une EC2 région Amazon en fonction des autres valeurs que vous avez spécifiées. Cela s'applique également aux zones hébergées privées. Nous vous conseillons de pas modifier cette valeur.

Remarques :

- Vous ne pouvez créer qu'un seul enregistrement de latence pour chaque EC2 région Amazon.
- Vous n'êtes pas obligé de créer des enregistrements de latence pour toutes les EC2 régions Amazon. Route 53 choisit la région dotée de la meilleure latence parmi les régions pour lesquelles vous créez des enregistrements de latence.
- Vous ne pouvez pas créer des enregistrements qui ne sont pas de type latence en utilisant les mêmes valeurs pour les champs Record name (Nom de l'enregistrement) et Record type (Type d'enregistrement) que celles des enregistrements de latence.

- Si vous créez un enregistrement balisé avec la région cn-north-1, Route 53 répond toujours aux requêtes en provenance de Chine en utilisant cet enregistrement, quelle que soit la latence.

Pour plus d'informations sur l'utilisation des enregistrements de latence, consultez Routage basé sur la latence.

Surveillance de l'état

Sélectionnez une surveillance de l'état si vous voulez que Route 53 vérifie l'état d'un point de terminaison spécifique et réponde aux requêtes DNS à l'aide de cet enregistrement uniquement lorsque le point de terminaison est sain.

Route 53 ne vérifie pas l'état du point de terminaison spécifié dans l'enregistrement, par exemple, le point de terminaison indiqué par l'adresse IP dans le champ Value (Valeur). Lorsque vous sélectionnez une surveillance de l'état pour un enregistrement, Route 53 vérifie l'état du point de terminaison que vous avez spécifié dans la surveillance de l'état. Pour plus d'informations sur la façon dont Route 53 détermine si un point de terminaison est sain, consultez Comment Amazon Route 53 détermine si une surveillance de l'état est saine.

L'association d'une surveillance de l'état à un enregistrement est utile uniquement lorsque Route 53 doit choisir entre plusieurs enregistrements pour répondre à une requête DNS et que vous souhaitez que Route 53 base en partie son choix sur le statut d'une surveillance de l'état. Utilisez des surveillances de l'état uniquement dans les configurations suivantes :

- Vous vérifiez l'état de santé de tous les enregistrements d'un groupe d'enregistrements portant le même nom, le même type et la même politique de routage (tels que le basculement ou les enregistrements pondérés), et vous spécifiez un contrôle de santé IDs pour tous les enregistrements. Si la surveillance de l'état d'un enregistrement spécifie un point de terminaison qui n'est pas sain, Route 53 cesse de répondre aux requêtes utilisant la valeur indiquée pour cet enregistrement.
- Vous sélectionnez Yes (Oui) pour Evaluate target health (Évaluer l'état de la cible) pour un enregistrement d'alias ou les enregistrements dans un groupe d'enregistrements d'alias de basculement, d'alias de géolocalisation, d'alias de latence, d'alias basés sur IP, ou d'alias pondérés. Si les enregistrements d'alias font référence à des enregistrements sans alias dans une même zone hébergée, vous devez spécifier les surveillances d'état pour les enregistrements référencés. Si vous associez une surveillance de l'état à un enregistrement d'alias et que vous sélectionnez également Yes (Oui) pour Evaluate Target Health (Évaluer l'état de la cible), les deux

doivent être évalués à vrai. Pour de plus amples informations, veuillez consulter Que se passe-t-il lorsque vous associez une surveillance de l'état à un enregistrement d'alias ?.

Si vos surveillances de l'état spécifient le point de terminaison uniquement par nom de domaine, nous vous recommandons de créer une surveillance de l'état distincte pour chaque point de terminaison. Par exemple, créez une surveillance de l'état pour chaque serveur HTTP qui diffuse du contenu pour www.example.com. Pour la valeur du champ Domain name (Nom de domaine), indiquez le nom de domaine du serveur (par exemple, us-east-2-www.example.com), et non pas le nom des enregistrements (example.com).

> **Important**
>
> Dans cette configuration, si vous créez une surveillance de l'état pour laquelle la valeur du champ Nom de domaine correspond au nom des enregistrements et si vous associez ensuite la surveillance de l'état à ces enregistrements, les résultats de la surveillance de l'état seront imprévisibles.

Évaluer l'état de la cible

Sélectionnez Yes (Oui) si vous voulez que Route 53 détermine s'il doit répondre aux requêtes DNS à l'aide de cet enregistrement en vérifiant l'état de la ressource spécifiée dans le champ Endpoint (Point de terminaison).

Remarques :

API Gateway personnalisé, régional APIs et optimisé pour les périphériques APIs

Il n'y a aucune exigence spécifique pour la définition du champ Evaluate target health (Évaluer l'état de la cible) sur Yes (Oui) lorsque le point de terminaison est une API régionale personnalisée API Gateway ou une API optimisée pour la périphérie.

CloudFront distributions

Vous ne pouvez pas définir Evaluate Target Health sur Oui lorsque le point de terminaison est une CloudFront distribution.

Environnements Elastic Beanstalk comportant des sous-domaines régionalisés

Si vous spécifiez un environnement Elastic Beanstalk dans Endpoint et que celui-ci contient un équilibreur de charge ELB, Elastic Load Balancing achemine les requêtes uniquement vers les

instances Amazon EC2 saines enregistrées auprès de l'équilibreur de charge. (Un environnement contient automatiquement un équilibreur de charge ELB s'il inclut plusieurs EC2 instances Amazon.) Si vous définissez Evaluate target health sur Oui et que les EC2 instances Amazon ne sont pas saines ou que l'équilibreur de charge lui-même est défaillant, Route 53 achemine les requêtes vers d'autres ressources disponibles qui sont saines, le cas échéant.

Si l'environnement contient une seule EC2 instance Amazon, il n'y a aucune exigence particulière.

Equilibreurs de charge ELB

Le comportement de la surveillance de l'état dépend du type de l'équilibreur de charge :

- Classic Load Balancers : si vous spécifiez un ELB Classic Load Balancer dans Endpoint, Elastic Load Balancing achemine les requêtes uniquement vers les instances EC2 Amazon saines enregistrées auprès de l'équilibreur de charge. Si vous définissez Evaluate target health sur Oui et qu'aucune EC2 instance n'est saine ou que l'équilibreur de charge lui-même est défaillant, Route 53 achemine les requêtes vers d'autres ressources.
- Équilibreurs de charge d'application et Network Load Balancer : si vous spécifiez un équilibreur de charge ELB d'application ou Network Load Balancer et que vous définissez Evaluate target health (Évaluer l'état de la cible) sur Yes (Oui), Route 53 achemine les requêtes vers l'équilibreur de charge en fonction de l'état des groupes cible associés à l'équilibreur de charge :
  - Pour qu'un équilibreur d'application ou un équilibreur Network Load Balancer soit considéré comme sain, chaque groupe cible contenant des cibles doit en contenir au moins une saine. Si un groupe cible contient uniquement des cibles qui ne sont pas saines, l'équilibreur de charge est considéré comme étant lui-même défectueux et Route 53 achemine les requêtes vers d'autres ressources.
  - Un groupe cible qui n'a pas de cibles enregistrées est considéré comme non sain.

> **Note**
>
> Lorsque vous créez un équilibreur de charge, vous configurez les paramètres des surveillances de l'état Elastic Load Balancing ; il ne s'agit pas de surveillances de l'état Route 53, mais elles jouent le même rôle. Ne créez pas de bilans de santé Route 53 pour les EC2 instances que vous enregistrez auprès d'un équilibreur de charge ELB.

Compartiments S3

Il n'y a aucune exigence spécifique pour la définition du champ Evaluate target health (Évaluer l'état de la cible) sur Yes (Oui) lorsque le point de terminaison est un compartiment S3.

Points de terminaison de l'interface d'un VPC Amazon

Il n'y a aucune exigence spécifique pour la définition du champ Evaluate target health (Évaluer l'état de la cible) sur Yes (Oui) lorsque le point de terminaison est un point de terminaison d'interface d'un VPC Amazon.

Autres enregistrements dans la même zone hébergée

Si la AWS ressource que vous spécifiez dans Endpoint est un enregistrement ou un groupe d'enregistrements (par exemple, un groupe d'enregistrements pondérés) mais qu'il ne s'agit pas d'un autre enregistrement alias, nous vous recommandons d'associer un bilan de santé à tous les enregistrements du point de terminaison. Pour de plus amples informations, veuillez consulter Que se passe-t-il lorsque vous omettez des surveillances de l'état ?.

ID d'enregistrement

Entrez une valeur qui identifie de manière unique cet enregistrement dans le groupe d'enregistrements de latence.

Valeurs spécifiques aux enregistrements basés sur IP

Lorsque vous créez des enregistrements basés sur IP, vous spécifiez les valeurs suivantes.

> **Note**
>
> Bien que la création d'enregistrements basés sur IP dans une zone hébergée privée soit autorisée, elle n'est pas prise en charge.

Rubriques

- Stratégie de routage
- Nom de l'enregistrement
- Type de registre
- TTL (secondes)
- Valeur/acheminer le trafic vers
- Emplacement
- Surveillance de l'état
- ID d'enregistrement

Stratégie de routage

Choisissez IP-based (basé sur IP).

Nom de l'enregistrement

Saisissez le nom de domaine ou de sous-domaine vers lequel vous souhaitez acheminer le trafic. La valeur par défaut est le nom de la zone hébergée.

> **Note**
>
> Si vous créez un enregistrement qui porte le même nom que la zone hébergée, n'entrez aucune valeur (par exemple, un symbole @) dans le champ Record name (Nom de l'enregistrement).

Saisissez le même nom pour tous les enregistrements du groupe d'enregistrements basés sur IP.

Enregistrements CNAME

Si vous créez un enregistrement dont la valeur est CNAME pour Record type (Type d'enregistrement), le nom de l'enregistrement ne peut être identique à celui de la zone hébergée.

Caractères spéciaux

Pour plus d'informations sur la spécification d'autres caractères que a-z, 0-9 et - (trait d'union), et de noms de domaine internationaux, consultez Format de nom de domaine DNS.

Caractères génériques

Vous pouvez utiliser un astérisque (*) dans le nom. DNS traite le caractère * comme un caractère générique ou comme le caractère * (ASCII 42), en fonction de son emplacement dans le nom. Pour de plus amples informations, veuillez consulter Utilisation d'un astérisque (*) dans les noms des zones hébergées et des enregistrements.

Type de registre

Type d'enregistrement DNS. Pour de plus amples informations, veuillez consulter Types d'enregistrements DNS pris en charge.

Sélectionnez la valeur pour le champ Type en fonction de la façon dont vous voulez que Route 53 réponde aux requêtes DNS.

Sélectionnez la même valeur pour tous les enregistrements du groupe d'enregistrements basés sur IP.

TTL (secondes)

Durée, en secondes, pendant laquelle vous voulez que les résolveurs DNS récursifs mettent en cache les informations relatives à cet enregistrement. Si vous spécifiez une valeur plus longue (par exemple, 172 800 secondes, soit deux jours), vous limitez le nombre d'appels que les résolveurs DNS récursifs doivent passer à Route 53 pour obtenir les dernières informations de cet enregistrement. Vous réduisez ainsi la latence et le montant de votre facture pour le service Route 53. Pour de plus amples informations, veuillez consulter Comment Amazon Route 53 achemine le trafic de votre domaine.

Cependant, si vous spécifiez une valeur de durée de vie plus longue, les modifications apportées à l'enregistrement (par exemple, une nouvelle adresse IP) mettent plus de temps à prendre effet, car les résolveurs récursifs utilisent les valeurs qui se trouvent dans leur cache pendant plus longtemps avant de demander les informations les plus récentes à Route 53. Si vous modifiez les paramètres

d'un domaine ou d'un sous-domaine déjà utilisé, nous vous conseillons de spécifier initialement une valeur plus courte, par exemple 300 secondes, et d'augmenter la valeur une fois que vous avez vérifié que les nouveaux paramètres sont corrects.

Si vous associez cet enregistrement à une vérification de l'état, nous vous recommandons de spécifier une durée de vie de 60 secondes au maximum afin que les clients répondent rapidement aux modifications de l'état de santé.

Valeur/acheminer le trafic vers

Choisissez IP address or another value depending on the record type (Adresse IP ou autre valeur selon le type d'enregistrement). Entrez une valeur appropriée pour la valeur Record type (Type d'enregistrement). Pour tous les types à l'exception de CNAME, vous pouvez entrer plusieurs valeurs. Entrez chaque valeur sur une ligne distincte.

Vous pouvez acheminer le trafic vers, ou spécifier les valeurs suivantes :

- A — IPv4 adresse
- AAAA — adresse IPv6
- CAA : autorisation de l'autorité de certification
- CNAME : nom canonique
- MX : échange de courrier
- NAPTR : nom d'indicateur d'autorité
- PTR : indicateur
- SPF : cadre de la politique de l'envoyeur
- SRV : localisateur de service
- TXT : texte

Pour plus d'informations sur les valeurs ci-dessus, consultez Valeur/acheminer le trafic vers valeurs communes pour Valeur/Acheminement du trafic vers.

Emplacement

Le nom de l'emplacement CIDR où la ressource que vous avez spécifiée dans cet enregistrement est spécifiée par les valeurs de bloc d'adresse CIDR dans l'emplacement CIDR.

Pour plus d'informations sur l'utilisation des enregistrements basés sur IP, consultez Routage basé sur IP.

Surveillance de l'état

Sélectionnez une surveillance de l'état si vous voulez que Route 53 vérifie l'état d'un point de terminaison spécifique et réponde aux requêtes DNS à l'aide de cet enregistrement uniquement lorsque le point de terminaison est sain.

Route 53 ne vérifie pas l'état du point de terminaison spécifié dans l'enregistrement, par exemple, le point de terminaison indiqué par l'adresse IP dans le champ Value (Valeur). Lorsque vous sélectionnez une surveillance de l'état pour un enregistrement, Route 53 vérifie l'état du point de terminaison que vous avez spécifié dans la surveillance de l'état. Pour plus d'informations sur la façon dont Route 53 détermine si un point de terminaison est sain, consultez Comment Amazon Route 53 détermine si une surveillance de l'état est saine.

L'association d'une surveillance de l'état à un enregistrement est utile uniquement lorsque Route 53 doit choisir entre plusieurs enregistrements pour répondre à une requête DNS et que vous souhaitez que Route 53 base en partie son choix sur le statut d'une surveillance de l'état. Utilisez des surveillances de l'état uniquement dans les configurations suivantes :

- Vous vérifiez l'état de santé de tous les enregistrements d'un groupe d'enregistrements portant le même nom, le même type et la même politique de routage (tels que le basculement ou les enregistrements pondérés), et vous spécifiez un contrôle de santé IDs pour tous les enregistrements. Si la surveillance de l'état d'un enregistrement spécifie un point de terminaison qui n'est pas sain, Route 53 cesse de répondre aux requêtes utilisant la valeur indiquée pour cet enregistrement.
- Vous sélectionnez Yes (Oui) pour Evaluate target health (Évaluer l'état de la cible) pour un enregistrement d'alias ou les enregistrements dans un groupe d'enregistrements d'alias de basculement, d'alias de géolocalisation, d'alias basés sur IP, d'alias de latence ou d'alias pondérés. Si les enregistrements d'alias font référence à des enregistrements sans alias dans une même zone hébergée, vous devez spécifier les surveillances d'état pour les enregistrements référencés. Si vous associez une surveillance de l'état à un enregistrement d'alias et que vous sélectionnez également Yes (Oui) pour Evaluate Target Health (Évaluer l'état de la cible), les deux doivent être évalués à vrai. Pour de plus amples informations, veuillez consulter Que se passe-t-il lorsque vous associez une surveillance de l'état à un enregistrement d'alias ?.

Si vos surveillances de l'état spécifient le point de terminaison uniquement par nom de domaine, nous vous recommandons de créer une surveillance de l'état distincte pour chaque point de terminaison. Par exemple, créez une surveillance de l'état pour chaque serveur HTTP qui diffuse du contenu pour www.example.com. Pour la valeur du champ Domain name (Nom de domaine),

indiquez le nom de domaine du serveur (par exemple, us-east-2-www.example.com), et non pas le nom des enregistrements (example.com).

> **Important**
>
> Dans cette configuration, si vous créez une vérification de l'état pour laquelle la valeur du champ Domain name (Nom de domaine) correspond au nom des enregistrements et si vous associez ensuite la vérification de l'état à ces enregistrements, les résultats de la vérification de l'état seront imprévisibles.

ID d'enregistrement

Saisissez une valeur qui identifie de manière unique cet enregistrement dans le groupe d'enregistrements basés sur l'IP.

Valeurs spécifiques aux enregistrements d'alias basés sur IP

Lorsque vous créez des enregistrements d'alias basés sur l'IP, vous spécifiez les valeurs suivantes.

> **Note**
>
> Bien que la création d'enregistrements d'alias basés sur IP dans une zone hébergée privée soit autorisée, elle n'est pas prise en charge.

Pour de plus amples informations, veuillez consulter Choix entre des enregistrements avec ou sans alias.

Rubriques

- Stratégie de routage
- Nom de l'enregistrement
- Type de registre
- Valeur/acheminer le trafic vers
- Emplacement
- Surveillance de l'état
- Évaluer l'état de la cible
- ID d'enregistrement

Stratégie de routage

Choisissez IP-based (basé sur IP).

> **Note**
>
> Bien que la création d'enregistrements d'alias basés sur IP dans une zone hébergée privée soit autorisée, elle n'est pas prise en charge.

Nom de l'enregistrement

Saisissez le nom de domaine ou de sous-domaine vers lequel vous souhaitez acheminer le trafic. La valeur par défaut est le nom de la zone hébergée.

> **Note**
>
> Si vous créez un enregistrement qui porte le même nom que la zone hébergée, n'entrez aucune valeur (par exemple, un symbole @) dans le champ Record name (Nom de l'enregistrement).

Saisissez le même nom pour tous les enregistrements du groupe d'enregistrements basés sur IP.

Enregistrements CNAME

Si vous créez un enregistrement dont la valeur est CNAME pour Record type (Type d'enregistrement), le nom de l'enregistrement ne peut être identique à celui de la zone hébergée.

Alias des CloudFront distributions et des compartiments Amazon S3

La valeur que vous spécifiez dépend en partie de la AWS ressource vers laquelle vous acheminez le trafic :

- CloudFront distribution — Votre distribution doit inclure un autre nom de domaine correspondant au nom de l'enregistrement. Par exemple, si le nom de l'enregistrement est acme.example.com, votre distribution CloudFront doit inclure acme.example.com parmi les autres noms de domaine. Pour plus d'informations, consultez la section Utilisation de noms de domaine alternatifs (CNAMEs) dans le manuel Amazon CloudFront Developer Guide.
- Compartiment Amazon S3 : le nom de l'enregistrement doit correspondre au nom de votre compartiment Amazon S3. Par exemple, si le nom de votre compartiment est acme.example.com, le nom de cet enregistrement doit également être acme.example.com.

  En outre, vous devez configurer le compartiment pour l'hébergement de site web. Pour de plus amples informations, veuillez consulter la section Configurer un compartiment pour l'hébergement de sites Web dans le Guide de l'utilisateur Amazon Simple Storage Service.

Caractères spéciaux

Pour plus d'informations sur la spécification d'autres caractères que a-z, 0-9 et - (trait d'union), et de noms de domaine internationaux, consultez Format de nom de domaine DNS.

Caractères génériques

Vous pouvez utiliser un astérisque (*) dans le nom. DNS traite le caractère * comme un caractère générique ou comme le caractère * (ASCII 42), en fonction de son emplacement dans le nom.

Pour de plus amples informations, veuillez consulter Utilisation d'un astérisque (*) dans les noms des zones hébergées et des enregistrements.

Type de registre

Type d'enregistrement DNS. Pour de plus amples informations, veuillez consulter Types d'enregistrements DNS pris en charge.

Sélectionnez la valeur applicable en fonction de la AWS ressource vers laquelle vous acheminez le trafic. Sélectionnez la même valeur pour tous les enregistrements du groupe d'enregistrements basés sur IP :

API régionale personnalisée API Gateway et API optimisée pour la périphérie

Sélectionnez A — IPv4 adresse.

Points de terminaison de l'interface d'un VPC Amazon

Sélectionnez A — IPv4 adresse.

CloudFront distribution

Sélectionnez A — IPv4 adresse.

Si cette option IPv6 est activée pour la distribution, créez deux enregistrements, l'un avec la valeur A — IPv4 adresse pour Type, et l'autre avec la valeur AAAA — IPv6 adresse.

Service App Runner

Sélectionnez A — IPv4 adresse

Environnement Elastic Beanstalk comportant des sous-domaines régionalisés

Sélectionnez A — IPv4 adresse

Équilibreur de charge ELB

Sélectionnez A — IPv4 adresse ou AAAA — IPv6 adresse

Compartiment Amazon S3

Sélectionnez A — IPv4 adresse

OpenSearch Service

Sélectionnez A — IPv4 adresse ou AAAA — IPv6 adresse

Autre enregistrement de cette zone hébergée

Sélectionnez le type d'enregistrement pour lequel vous créez l'alias. Tous les types sont pris en charge, sauf NS et SOA.

> **Note**
>
> Si vous créez un enregistrement d'alias qui a le même nom que la zone hébergée (appelée aussi zone apex), vous ne pouvez pas acheminer le trafic vers un enregistrement dont la valeur pour Type (Type) est CNAME. Cela est dû au fait que l'enregistrement d'alias doit être du même type que l'enregistrement vers lequel vous acheminez le trafic et que la création d'un enregistrement CNAME pour la zone apex n'est pas prise en charge, même pour un enregistrement d'alias.

Valeur/acheminer le trafic vers

La valeur que vous choisissez dans la liste ou que vous saisissez dans le champ dépend de la AWS ressource vers laquelle vous acheminez le trafic.

Pour plus d'informations sur les AWS ressources que vous pouvez cibler, consultez les valeurs communes des enregistrements d'alias destinés au trafic de valeurs/d'itinéraires.

Pour plus d'informations sur la configuration de Route 53 pour acheminer le trafic vers des AWS ressources spécifiques, consultezAcheminement du trafic Internet vers vos AWS ressources.

Emplacement

Lorsque vous configurez Route 53 pour qu'il réponde aux requêtes DNS en fonction de leur emplacement d'origine, sélectionnez l'emplacement CIDR pour lequel vous voulez que Route 53 réponde avec les paramètres figurant dans cet enregistrement.

> **Important**
>
> Nous vous conseillons de créer un enregistrement basé sur IP ayant la valeur Default (Par défaut) pour Location (Emplacement). Ainsi, les emplacements pour lesquels vous n'avez pas créé d'enregistrements et les adresses IP dont Route 53 ne peut identifier l'emplacement sont couverts.

Vous ne pouvez pas créer d' non-IP-basedenregistrements dont les valeurs de nom et de type d'enregistrement sont les mêmes que celles des enregistrements basés sur l'adresse IP.

Pour de plus amples informations, veuillez consulter Routage basé sur IP.

Surveillance de l'état

Sélectionnez une surveillance de l'état si vous voulez que Route 53 vérifie l'état d'un point de terminaison spécifique et réponde aux requêtes DNS à l'aide de cet enregistrement uniquement lorsque le point de terminaison est sain.

Route 53 ne vérifie pas l'état du point de terminaison spécifié dans l'enregistrement, par exemple, le point de terminaison indiqué par l'adresse IP dans le champ Value (Valeur). Lorsque vous sélectionnez une surveillance de l'état pour un enregistrement, Route 53 vérifie l'état du point de terminaison que vous avez spécifié dans la surveillance de l'état. Pour plus d'informations sur la façon dont Route 53 détermine si un point de terminaison est sain, consultez Comment Amazon Route 53 détermine si une surveillance de l'état est saine.

L'association d'une surveillance de l'état à un enregistrement est utile uniquement lorsque Route 53 doit choisir entre plusieurs enregistrements pour répondre à une requête DNS et que vous souhaitez que Route 53 base en partie son choix sur le statut d'une surveillance de l'état. Utilisez des surveillances de l'état uniquement dans les configurations suivantes :

- Vous vérifiez l'état de santé de tous les enregistrements d'un groupe d'enregistrements portant le même nom, le même type et la même politique de routage (tels que le basculement ou les enregistrements pondérés), et vous spécifiez un contrôle de santé IDs pour tous les enregistrements. Si la surveillance de l'état d'un enregistrement spécifie un point de terminaison qui n'est pas sain, Route 53 cesse de répondre aux requêtes utilisant la valeur indiquée pour cet enregistrement.
- Vous sélectionnez Yes (Oui) pour Evaluate target health (Évaluer l'état de la cible) pour un enregistrement d'alias ou les enregistrements dans un groupe d'enregistrements d'alias de basculement, d'alias de géolocalisation, d'alias de routage basé sur IP, d'alias de latence ou d'alias pondérés. Si les enregistrements d'alias font référence à des enregistrements sans alias dans une même zone hébergée, vous devez spécifier les surveillances d'état pour les enregistrements référencés. Si vous associez une surveillance de l'état à un enregistrement d'alias et que vous sélectionnez également Yes (Oui) pour Evaluate Target Health (Évaluer l'état de la cible), les deux doivent être évalués à vrai. Pour de plus amples informations, veuillez consulter Que se passe-t-il lorsque vous associez une surveillance de l'état à un enregistrement d'alias ?.

Si vos surveillances de l'état spécifient le point de terminaison uniquement par nom de domaine, nous vous recommandons de créer une surveillance de l'état distincte pour chaque point de terminaison. Par exemple, créez une surveillance de l'état pour chaque serveur HTTP qui diffuse du contenu pour www.example.com. Pour la valeur du champ Domain name (Nom de domaine), indiquez le nom de domaine du serveur (par exemple, us-east-2-www.example.com), et non pas le nom des enregistrements (example.com).

> **Important**
>
> Dans cette configuration, si vous créez une vérification de l'état pour laquelle la valeur du champ Domain name (Nom de domaine) correspond au nom des enregistrements et si vous associez ensuite la vérification de l'état à ces enregistrements, les résultats de la vérification de l'état seront imprévisibles.

Pour les enregistrements d'alias basés sur IP, si un point de terminaison n'est pas en bon état, Route 53 recherche un enregistrement dans l'emplacement associé plus grand. Par exemple, supposons que vous disposez d'enregistrements pour un État des États-Unis, pour les États-Unis, pour l'Amérique du Nord et pour tous les emplacements (la valeur du champ Location [Emplacement] est Default [Par défaut]). Si le point de terminaison de l'enregistrement de l'État n'est pas sain, Route 53 vérifie les enregistrements pour les États-Unis, pour l'Amérique du Nord, ainsi que pour tous les emplacements, dans cet ordre, jusqu'à ce qu'il trouve un enregistrement comportant un point de terminaison sain. Si tous les enregistrements applicables sont défaillants, y compris l'enregistrement pour tous les emplacements, Route 53 répond à la requête DNS à l'aide de la valeur pour l'enregistrement de la région géographique la plus petite.

Évaluer l'état de la cible

Sélectionnez Yes (Oui) si vous voulez que Route 53 détermine s'il doit répondre aux requêtes DNS à l'aide de cet enregistrement en vérifiant l'état de la ressource spécifiée dans le champ Endpoint (Point de terminaison).

Remarques :

API Gateway personnalisé, régional APIs et optimisé pour les périphériques APIs

> Il n'y a aucune exigence spécifique pour la définition du champ Evaluate target health (Évaluer l'état de la cible) sur Yes (Oui) lorsque le point de terminaison est une API régionale personnalisée API Gateway ou une API optimisée pour la périphérie.

CloudFront distributions

Vous ne pouvez pas définir Evaluate target health sur Oui lorsque le point de terminaison est une CloudFront distribution.

Environnements Elastic Beanstalk comportant des sous-domaines régionalisés

Si vous spécifiez un environnement Elastic Beanstalk dans Endpoint et que celui-ci contient un équilibreur de charge ELB, Elastic Load Balancing achemine les requêtes uniquement vers les instances Amazon EC2 saines enregistrées auprès de l'équilibreur de charge. (Un environnement contient automatiquement un équilibreur de charge ELB s'il inclut plusieurs EC2 instances Amazon.) Si vous définissez Evaluate target health sur Oui et que les EC2 instances Amazon ne sont pas saines ou que l'équilibreur de charge lui-même est défaillant, Route 53 achemine les requêtes vers d'autres ressources disponibles qui sont saines, le cas échéant.

Si l'environnement contient une seule EC2 instance Amazon, il n'y a aucune exigence particulière.

Equilibreurs de charge ELB

Le comportement de la surveillance de l'état dépend du type de l'équilibreur de charge :

- Classic Load Balancers : si vous spécifiez un ELB Classic Load Balancer dans Endpoint, Elastic Load Balancing achemine les requêtes uniquement vers les instances EC2 Amazon saines enregistrées auprès de l'équilibreur de charge. Si vous définissez Evaluate target health sur Oui et qu'aucune EC2 instance n'est saine ou que l'équilibreur de charge lui-même est défaillant, Route 53 achemine les requêtes vers d'autres ressources.
- Équilibreurs de charge d'application et Network Load Balancer : si vous spécifiez un équilibreur de charge ELB d'application ou Network Load Balancer et que vous définissez Evaluate target health (Évaluer l'état de la cible) sur Yes (Oui), Route 53 achemine les requêtes vers l'équilibreur de charge en fonction de l'état des groupes cible associés à l'équilibreur de charge :
  - Pour qu'un équilibreur d'application ou un équilibreur Network Load Balancer soit considéré comme sain, chaque groupe cible contenant des cibles doit en contenir au moins une saine. Si un groupe cible contient uniquement des cibles qui ne sont pas saines, l'équilibreur de charge est considéré comme étant lui-même défectueux et Route 53 achemine les requêtes vers d'autres ressources.
  - Un groupe cible qui n'a pas de cibles enregistrées est considéré comme non sain.

> **Note**
>
> Lorsque vous créez un équilibreur de charge, vous configurez les paramètres des surveillances de l'état Elastic Load Balancing ; il ne s'agit pas de surveillances de l'état

Route 53, mais elles jouent le même rôle. Ne créez pas de bilans de santé Route 53 pour les EC2 instances que vous enregistrez auprès d'un équilibreur de charge ELB.

Compartiments S3

Il n'y a aucune exigence spécifique pour la définition du champ Evaluate target health (Évaluer l'état de la cible) sur Yes (Oui) lorsque le point de terminaison est un compartiment S3.

Points de terminaison de l'interface d'un VPC Amazon

Il n'y a aucune exigence spécifique pour la définition du champ Evaluate target health (Évaluer l'état de la cible) sur Yes (Oui) lorsque le point de terminaison est un point de terminaison d'interface d'un VPC Amazon.

Autres enregistrements dans la même zone hébergée

Si la AWS ressource que vous spécifiez dans Endpoint est un enregistrement ou un groupe d'enregistrements (par exemple, un groupe d'enregistrements pondérés) mais qu'il ne s'agit pas d'un autre enregistrement alias, nous vous recommandons d'associer un bilan de santé à tous les enregistrements du point de terminaison. Pour de plus amples informations, veuillez consulter Que se passe-t-il lorsque vous omettez des surveillances de l'état ?.

ID d'enregistrement

Saisissez une valeur qui identifie de manière unique cet enregistrement dans le groupe d'enregistrements basés sur l'IP.

Valeurs spécifiques pour les enregistrements de réponses multivaleur

Lorsque vous créez des enregistrements de réponse multivaleur, vous spécifiez les valeurs suivantes.

> **Note**
>
> La création d'enregistrements d'alias de réponse multivaleur n'est pas prise en charge.

Rubriques

- Stratégie de routage
- Nom de l'enregistrement
- Type de registre
- TTL (secondes)
- Valeur/acheminer le trafic vers
- Surveillance de l'état
- ID d'enregistrement

Stratégie de routage

Choisissez Multivalue answer (Réponse multivaleur).

Nom de l'enregistrement

Saisissez le nom de domaine ou de sous-domaine vers lequel vous souhaitez acheminer le trafic. La valeur par défaut est le nom de la zone hébergée.

> **Note**
>
> Si vous créez un enregistrement qui porte le même nom que la zone hébergée, n'entrez aucune valeur (par exemple, un symbole @) dans le champ Record name (Nom de l'enregistrement).

Entrez le même nom pour tous les enregistrements du groupe d'enregistrements multi-valeurs.

Pour plus d'informations sur les noms d'enregistrements, veuillez consulter Nom de l'enregistrement.

Type de registre

Type d'enregistrement DNS. Pour de plus amples informations, veuillez consulter Types d'enregistrements DNS pris en charge.

Sélectionnez n'importe quelle valeur à l'exception de NS ou CNAME.

Sélectionnez la même valeur pour tous les enregistrements du groupe d'enregistrements de réponse à valeurs multiples.

TTL (secondes)

Durée, en secondes, pendant laquelle vous voulez que les résolveurs DNS récursifs mettent en cache les informations relatives à cet enregistrement. Si vous spécifiez une valeur plus longue (par exemple, 172 800 secondes, soit deux jours), vous limitez le nombre d'appels que les résolveurs DNS récursifs doivent passer à Route 53 pour obtenir les dernières informations de cet enregistrement. Vous réduisez ainsi la latence et le montant de votre facture pour le service Route 53. Pour de plus amples informations, veuillez consulter Comment Amazon Route 53 achemine le trafic de votre domaine.

Cependant, si vous spécifiez une valeur de durée de vie plus longue, les modifications apportées à l'enregistrement (par exemple, une nouvelle adresse IP) mettent plus de temps à prendre effet, car les résolveurs récursifs utilisent les valeurs qui se trouvent dans leur cache pendant plus longtemps avant de demander les informations les plus récentes à Route 53. Si vous modifiez les paramètres d'un domaine ou d'un sous-domaine déjà utilisé, nous vous conseillons de spécifier initialement une valeur plus courte, par exemple 300 secondes, et d'augmenter la valeur une fois que vous avez vérifié que les nouveaux paramètres sont corrects.

Si vous associez cet enregistrement à une vérification de l'état, nous vous recommandons de spécifier une durée de vie de 60 secondes au maximum afin que les clients répondent rapidement aux modifications de l'état de santé.

> **Note**
>
> Si vous créez deux ou plusieurs enregistrements de réponse multivaleur qui ont le même nom et le même type, que vous utilisez la console et que vous spécifiez des valeurs différentes pour le TTL, Route 53 change la valeur du TTL pour tous les enregistrements à la dernière valeur que vous avez spécifiée.

Valeur/acheminer le trafic vers

Choisissez IP address or another value depending on the record type (Adresse IP ou autre valeur selon le type d'enregistrement). Entrez une valeur appropriée pour la valeur Record type (Type d'enregistrement). Si vous entrez plusieurs valeurs, entrez chacune d'entre elles sur une ligne séparée.

Vous pouvez acheminer le trafic vers, ou spécifier les valeurs suivantes :

- A — IPv4 adresse
- AAAA — adresse IPv6
- CAA : autorisation de l'autorité de certification
- MX : échange de courrier
- NAPTR : nom d'indicateur d'autorité
- PTR : indicateur
- SPF : cadre de la politique de l'envoyeur
- SRV : localisateur de service
- TXT : texte

Pour plus d'informations sur les valeurs ci-dessus, consultez valeurs communes pour Valeur/Acheminement du trafic vers.

Surveillance de l'état

Sélectionnez une surveillance de l'état si vous voulez que Route 53 vérifie l'état d'un point de terminaison spécifique et réponde aux requêtes DNS à l'aide de cet enregistrement uniquement lorsque le point de terminaison est sain.

Route 53 ne vérifie pas l'état du point de terminaison spécifié dans l'enregistrement, par exemple, le point de terminaison indiqué par l'adresse IP dans le champ Value (Valeur). Lorsque vous sélectionnez une surveillance de l'état pour un enregistrement, Route 53 vérifie l'état du point de terminaison que vous avez spécifié dans la surveillance de l'état. Pour plus d'informations sur la façon dont Route 53 détermine si un point de terminaison est sain, consultez Comment Amazon Route 53 détermine si une surveillance de l'état est saine.

L'association d'une surveillance de l'état à un enregistrement est utile uniquement lorsque Route 53 doit choisir entre plusieurs enregistrements pour répondre à une requête DNS et que vous souhaitez

que Route 53 base en partie son choix sur le statut d'une surveillance de l'état. Utilisez des surveillances de l'état uniquement dans les configurations suivantes :

- Vous vérifiez l'état de santé de tous les enregistrements d'un groupe d'enregistrements portant le même nom, le même type et la même politique de routage (tels que le basculement ou les enregistrements pondérés), et vous spécifiez un contrôle de santé IDs pour tous les enregistrements. Si la vérification de l'état d'un enregistrement spécifie un point de terminaison qui n'est pas sain, Route 53 cesse de répondre aux requêtes utilisant la valeur indiquée pour cet enregistrement.
- Vous sélectionnez Yes (Oui) pour Evaluate target health (Évaluer l'état de la cible) pour chercher un enregistrement d'alias ou les enregistrements dans un groupe d'enregistrements d'alias pondérés, d'alias de latence, d'alias de géolocalisation ou d'alias de basculement. Si les enregistrements d'alias font référence à des enregistrements sans alias dans une même zone hébergée, vous devez spécifier les surveillances d'état pour les enregistrements référencés. Si vous associez une surveillance de l'état à un enregistrement d'alias et que vous sélectionnez également Yes (Oui) pour Evaluate Target Health (Évaluer l'état de la cible), les deux doivent être évalués à vrai. Pour de plus amples informations, veuillez consulter Que se passe-t-il lorsque vous associez une surveillance de l'état à un enregistrement d'alias ?.

Si vos surveillances de l'état spécifient le point de terminaison uniquement par nom de domaine, nous vous recommandons de créer une surveillance de l'état distincte pour chaque point de terminaison. Par exemple, créez une surveillance de l'état pour chaque serveur HTTP qui diffuse du contenu pour www.example.com. Pour la valeur du champ Domain name (Nom de domaine), indiquez le nom de domaine du serveur (par exemple, us-east-2-www.example.com), et non pas le nom des enregistrements (example.com).

> **Important**
>
> Dans cette configuration, si vous créez une vérification de l'état pour laquelle la valeur du champ Domain name (Nom de domaine) correspond au nom des enregistrements et si vous associez ensuite la vérification de l'état à ces enregistrements, les résultats de la vérification de l'état seront imprévisibles.

ID d'enregistrement

Entrez une valeur qui identifie de manière unique cet enregistrement dans le groupe d'enregistrements de réponse à valeurs multiples.

Valeurs spécifiques aux enregistrements pondérés

Lorsque vous créez des enregistrements pondérés, vous spécifiez les valeurs suivantes.

Rubriques

- Stratégie de routage
- Nom de l'enregistrement
- Type de registre
- TTL (secondes)
- Valeur/acheminer le trafic vers
- Weight
- Surveillance de l'état
- ID d'enregistrement

Stratégie de routage

Sélectionnez Weighted (Pondéré).

Nom de l'enregistrement

Saisissez le nom de domaine ou de sous-domaine vers lequel vous souhaitez acheminer le trafic. La valeur par défaut est le nom de la zone hébergée.

> **Note**
>
> Si vous créez un enregistrement qui porte le même nom que la zone hébergée, n'entrez aucune valeur (par exemple, un symbole @) dans le champ Record name (Nom de l'enregistrement).

Entrez le même nom pour tous les enregistrements du groupe d'enregistrements pondérés.

Pour plus d'informations sur les noms d'enregistrements, veuillez consulter Nom de l'enregistrement.

Type de registre

Type d'enregistrement DNS. Pour de plus amples informations, veuillez consulter Types d'enregistrements DNS pris en charge.

Sélectionnez la même valeur pour tous les enregistrements du groupe d'enregistrements pondérés.

TTL (secondes)

Durée, en secondes, pendant laquelle vous voulez que les résolveurs DNS récursifs mettent en cache les informations relatives à cet enregistrement. Si vous spécifiez une valeur plus longue (par exemple, 172 800 secondes, soit deux jours), vous limitez le nombre d'appels que les résolveurs DNS récursifs doivent passer à Route 53 pour obtenir les dernières informations de cet enregistrement. Vous réduisez ainsi la latence et le montant de votre facture pour le service Route 53. Pour de plus amples informations, veuillez consulter Comment Amazon Route 53 achemine le trafic de votre domaine.

Cependant, si vous spécifiez une valeur de durée de vie plus longue, les modifications apportées à l'enregistrement (par exemple, une nouvelle adresse IP) mettent plus de temps à prendre effet, car les résolveurs récursifs utilisent les valeurs qui se trouvent dans leur cache pendant plus longtemps avant de demander les informations les plus récentes à Route 53. Si vous modifiez les paramètres d'un domaine ou d'un sous-domaine déjà utilisé, nous vous conseillons de spécifier initialement une valeur plus courte, par exemple 300 secondes, et d'augmenter la valeur une fois que vous avez vérifié que les nouveaux paramètres sont corrects.

Si vous associez cet enregistrement à une vérification de l'état, nous vous recommandons de spécifier une durée de vie de 60 secondes au maximum afin que les clients répondent rapidement aux modifications de l'état de santé.

Vous devez indiquer la même valeur dans le champ TTL (Durée de vie) pour tous les enregistrements de ce groupe d'enregistrements pondérés.

> **Note**
>
> Si vous créez plusieurs enregistrements pondérés qui possèdent le même nom et le même type, puis que vous spécifiez des valeurs différentes pour TTL (Durée de vie), Route 53 remplace la valeur de TTL de tous les enregistrements par la dernière valeur que vous avez spécifiée.

Si un groupe d'enregistrements pondérés inclut un ou plusieurs enregistrements d'alias pondérés qui acheminent le trafic vers un équilibreur de charge ELB, nous vous recommandons de spécifier une durée de vie de 60 secondes pour tous les enregistrements pondérés sans alias ayant les

mêmes nom et type. D'autres valeurs que 60 secondes (durée de vie pour les équilibreurs de charge) modifieront l'effet des valeurs que vous spécifiez pour le champ Weight (Poids).

Valeur/acheminer le trafic vers

Choisissez IP address or another value depending on the record type (Adresse IP ou autre valeur selon le type d'enregistrement). Entrez une valeur appropriée pour la valeur Record type (Type d'enregistrement). Pour tous les types à l'exception de CNAME, vous pouvez entrer plusieurs valeurs. Entrez chaque valeur sur une ligne distincte.

Vous pouvez acheminer le trafic vers, ou spécifier les valeurs suivantes :

- A — IPv4 adresse
- AAAA — adresse IPv6
- CAA : autorisation de l'autorité de certification
- CNAME : nom canonique
- MX : échange de courrier
- NAPTR : nom d'indicateur d'autorité
- PTR : indicateur
- SPF : cadre de la politique de l'envoyeur
- SRV : localisateur de service
- TXT : texte

Pour plus d'informations sur les valeurs ci-dessus, consultez valeurs communes pour Valeur/Acheminement du trafic vers.

Weight

Valeur qui détermine la proportion de requêtes DNS auxquelles Route 53 répond à l'aide de l'enregistrement actuel. Route 53 calcule la somme des pondérations pour les enregistrements qui ont la même combinaison de type et de nom DNS. Route 53 répond ensuite aux requêtes en fonction du rapport entre le poids d'une ressource et le total.

Vous ne pouvez pas créer des enregistrements qui ne sont pas de type pondéré en utilisant les mêmes valeurs pour les champs Record name (Nom de l'enregistrement) et Record type (Type d'enregistrement) que celles des enregistrements pondérés.

Entrez un entier compris entre 0 et 255. Pour désactiver le routage vers une ressource, définissez le champ Weight (Poids) sur 0. Si vous définissez le champ Weight (Poids) sur 0 pour tous les enregistrements du groupe, le trafic est acheminé vers toutes les ressources avec une probabilité égale. Ainsi, vous ne pouvez pas désactiver accidentellement le routage pour un groupe d'enregistrements pondérés.

La définition du champ Weight (Poids) sur 0 produit un autre effet lorsque vous associez des vérifications de l'état à des enregistrements pondérés. Pour de plus amples informations, veuillez consulter Choix des enregistrements par Amazon Route 53 lorsque la surveillance de l'état est configurée.

Surveillance de l'état

Sélectionnez une surveillance de l'état si vous voulez que Route 53 vérifie l'état d'un point de terminaison spécifique et réponde aux requêtes DNS à l'aide de cet enregistrement uniquement lorsque le point de terminaison est sain.

Route 53 ne vérifie pas l'état du point de terminaison spécifié dans l'enregistrement, par exemple, le point de terminaison indiqué par l'adresse IP dans le champ Value (Valeur). Lorsque vous sélectionnez une surveillance de l'état pour un enregistrement, Route 53 vérifie l'état du point de terminaison que vous avez spécifié dans la surveillance de l'état. Pour plus d'informations sur la façon dont Route 53 détermine si un point de terminaison est sain, consultez Comment Amazon Route 53 détermine si une surveillance de l'état est saine.

L'association d'une surveillance de l'état à un enregistrement est utile uniquement lorsque Route 53 doit choisir entre plusieurs enregistrements pour répondre à une requête DNS et que vous souhaitez que Route 53 base en partie son choix sur le statut d'une surveillance de l'état. Utilisez des surveillances de l'état uniquement dans les configurations suivantes :

- Vous vérifiez l'état de santé de tous les enregistrements d'un groupe d'enregistrements portant le même nom, le même type et la même politique de routage (tels que le basculement ou les enregistrements pondérés), et vous spécifiez un contrôle de santé IDs pour tous les enregistrements. Si la surveillance de l'état d'un enregistrement spécifie un point de terminaison qui n'est pas sain, Route 53 cesse de répondre aux requêtes utilisant la valeur indiquée pour cet enregistrement.
- Vous sélectionnez Yes (Oui) pour Evaluate target health (Évaluer l'état de la cible) pour un enregistrement d'alias ou les enregistrements dans un groupe d'enregistrements d'alias de basculement, d'alias de géolocalisation, d'alias de latence, d'alias basés sur IP, ou d'alias pondérés. Si les enregistrements d'alias font référence à des enregistrements sans alias dans

une même zone hébergée, vous devez spécifier les surveillances d'état pour les enregistrements référencés. Si vous associez une surveillance de l'état à un enregistrement d'alias et que vous sélectionnez également Yes (Oui) pour Evaluate Target Health (Évaluer l'état de la cible), les deux doivent être évalués à vrai. Pour de plus amples informations, veuillez consulter Que se passe-t-il lorsque vous associez une surveillance de l'état à un enregistrement d'alias ?.

Si vos surveillances de l'état spécifient le point de terminaison uniquement par nom de domaine, nous vous recommandons de créer une surveillance de l'état distincte pour chaque point de terminaison. Par exemple, créez une surveillance de l'état pour chaque serveur HTTP qui diffuse du contenu pour www.example.com. Pour la valeur du champ Domain name (Nom de domaine), indiquez le nom de domaine du serveur (par exemple, us-east-2-www.example.com), et non pas le nom des enregistrements (example.com).

> **Important**
>
> Dans cette configuration, si vous créez une vérification de l'état pour laquelle la valeur du champ Domain name (Nom de domaine) correspond au nom des enregistrements et si vous associez ensuite la vérification de l'état à ces enregistrements, les résultats de la vérification de l'état seront imprévisibles.

ID d'enregistrement

Entrez une valeur qui identifie de manière unique cet enregistrement dans le groupe d'enregistrements pondérés.

Valeurs spécifiques aux enregistrements d'alias pondérés

Lorsque vous créez des enregistrements d'alias pondérés, vous spécifiez les valeurs suivantes. Pour de plus amples informations, veuillez consulter Choix entre des enregistrements avec ou sans alias.

Rubriques

- Stratégie de routage
- Nom de l'enregistrement
- Type de registre
- Valeur/acheminer le trafic vers
- Weight
- Surveillance de l'état
- Évaluer l'état de la cible
- ID d'enregistrement

Stratégie de routage

Choisissez Weighted (Pondéré).

Nom de l'enregistrement

Saisissez le nom de domaine ou de sous-domaine vers lequel vous souhaitez acheminer le trafic. La valeur par défaut est le nom de la zone hébergée.

> **Note**
>
> Si vous créez un enregistrement qui porte le même nom que la zone hébergée, n'entrez aucune valeur (par exemple, un symbole @) dans le champ Name (Nom).

Entrez le même nom pour tous les enregistrements du groupe d'enregistrements pondérés.

Pour plus d'informations sur les noms d'enregistrements, veuillez consulter Nom de l'enregistrement

Type de registre

Type d'enregistrement DNS. Pour de plus amples informations, veuillez consulter Types d'enregistrements DNS pris en charge.

Sélectionnez la valeur applicable en fonction de la AWS ressource vers laquelle vous acheminez le trafic :

API régionale personnalisée API Gateway et API optimisée pour la périphérie

Sélectionnez A — IPv4 adresse.

Points de terminaison de l'interface d'un VPC Amazon

Sélectionnez A — IPv4 adresse.

CloudFront distribution

Sélectionnez A — IPv4 adresse.

Si cette option IPv6 est activée pour la distribution, créez deux enregistrements, l'un avec la valeur A — IPv4 adresse pour Type, et l'autre avec la valeur AAAA — IPv6 adresse.

Service App Runner

Sélectionnez A — IPv4 adresse

Environnement Elastic Beanstalk comportant des sous-domaines régionalisés

Sélectionnez A — IPv4 adresse

ELB load balancer

Sélectionnez A — IPv4 adresse ou AAAA — IPv6 adresse

Compartiment Amazon S3

Sélectionnez A — IPv4 adresse

OpenSearch Service

Sélectionnez A — IPv4 adresse ou AAAA — IPv6 adresse

Autre enregistrement de cette zone hébergée

Sélectionnez le type d'enregistrement pour lequel vous créez l'alias. Tous les types sont pris en charge, sauf NS et SOA.

> **Note**
>
> Si vous créez un enregistrement d'alias qui a le même nom que la zone hébergée (appelée aussi zone apex), vous ne pouvez pas acheminer le trafic vers un

enregistrement dont la valeur pour Type (Type) est CNAME. Cela est dû au fait que l'enregistrement d'alias doit être du même type que l'enregistrement vers lequel vous acheminez le trafic et que la création d'un enregistrement CNAME pour la zone apex n'est pas prise en charge, même pour un enregistrement d'alias.

Sélectionnez la même valeur pour tous les enregistrements du groupe d'enregistrements pondérés.

Valeur/acheminer le trafic vers

La valeur que vous choisissez dans la liste ou que vous saisissez dans le champ dépend de la AWS ressource vers laquelle vous acheminez le trafic.

Pour plus d'informations sur les AWS ressources que vous pouvez cibler, consultez les valeurs communes des enregistrements d'alias vers lesquels le trafic de valeurs/d'itinéraires est destiné.

Pour plus d'informations sur la configuration de Route 53 pour acheminer le trafic vers des AWS ressources spécifiques, consultezAcheminement du trafic Internet vers vos AWS ressources.

Weight

Valeur qui détermine la proportion de requêtes DNS auxquelles Route 53 répond à l'aide de l'enregistrement actuel. Route 53 calcule la somme des pondérations pour les enregistrements qui ont la même combinaison de type et de nom DNS. Route 53 répond ensuite aux requêtes en fonction du rapport entre le poids d'une ressource et le total.

Vous ne pouvez pas créer des enregistrements qui ne sont pas de type pondéré en utilisant les mêmes valeurs pour les champs Record name (Nom de l'enregistrement) et Record type (Type d'enregistrement) que celles des enregistrements pondérés.

Entrez un entier compris entre 0 et 255. Pour désactiver le routage vers une ressource, définissez le champ Weight (Poids) sur 0. Si vous définissez le champ Weight (Poids) sur 0 pour tous les enregistrements du groupe, le trafic est acheminé vers toutes les ressources avec une probabilité égale. Ainsi, vous ne pouvez pas désactiver accidentellement le routage pour un groupe d'enregistrements pondérés.

La définition du champ Weight (Poids) sur 0 produit un autre effet lorsque vous associez des vérifications de l'état à des enregistrements pondérés. Pour de plus amples informations, veuillez consulter Choix des enregistrements par Amazon Route 53 lorsque la surveillance de l'état est configurée.

Surveillance de l'état

Sélectionnez une surveillance de l'état si vous voulez que Route 53 vérifie l'état d'un point de terminaison spécifique et réponde aux requêtes DNS à l'aide de cet enregistrement uniquement lorsque le point de terminaison est sain.

Route 53 ne vérifie pas l'état du point de terminaison spécifié dans l'enregistrement, par exemple, le point de terminaison indiqué par l'adresse IP dans le champ Value (Valeur). Lorsque vous sélectionnez une surveillance de l'état pour un enregistrement, Route 53 vérifie l'état du point de terminaison que vous avez spécifié dans la surveillance de l'état. Pour plus d'informations sur la façon dont Route 53 détermine si un point de terminaison est sain, consultez Comment Amazon Route 53 détermine si une surveillance de l'état est saine.

L'association d'une surveillance de l'état à un enregistrement est utile uniquement lorsque Route 53 doit choisir entre plusieurs enregistrements pour répondre à une requête DNS et que vous souhaitez que Route 53 base en partie son choix sur le statut d'une surveillance de l'état. Utilisez des surveillances de l'état uniquement dans les configurations suivantes :

- Vous vérifiez l'état de santé de tous les enregistrements d'un groupe d'enregistrements portant le même nom, le même type et la même politique de routage (tels que le basculement ou les enregistrements pondérés), et vous spécifiez un contrôle de santé IDs pour tous les enregistrements. Si la surveillance de l'état d'un enregistrement spécifie un point de terminaison qui n'est pas sain, Route 53 cesse de répondre aux requêtes utilisant la valeur indiquée pour cet enregistrement.
- Vous sélectionnez Yes (Oui) pour Evaluate target health (Évaluer l'état de la cible) pour un enregistrement d'alias ou les enregistrements dans un groupe d'enregistrements d'alias de basculement, d'alias de géolocalisation, d'alias de latence, d'alias basés sur IP, ou d'alias pondérés. Si les enregistrements d'alias font référence à des enregistrements sans alias dans une même zone hébergée, vous devez spécifier les surveillances d'état pour les enregistrements référencés. Si vous associez une surveillance de l'état à un enregistrement d'alias et que vous sélectionnez également Yes (Oui) pour Evaluate Target Health (Évaluer l'état de la cible), les deux doivent être évalués à vrai. Pour de plus amples informations, veuillez consulter Que se passe-t-il lorsque vous associez une surveillance de l'état à un enregistrement d'alias ?.

Si vos surveillances de l'état spécifient le point de terminaison uniquement par nom de domaine, nous vous recommandons de créer une surveillance de l'état distincte pour chaque point de terminaison. Par exemple, créez une surveillance de l'état pour chaque serveur HTTP qui diffuse du contenu pour www.example.com. Pour la valeur du champ Domain name (Nom de domaine),

indiquez le nom de domaine du serveur (par exemple, us-east-2-www.example.com), et non pas le nom des enregistrements (example.com).

> **Important**
>
> Dans cette configuration, si vous créez une vérification de l'état pour laquelle la valeur du champ Domain name (Nom de domaine) correspond au nom des enregistrements et si vous associez ensuite la vérification de l'état à ces enregistrements, les résultats de la vérification de l'état seront imprévisibles.

Évaluer l'état de la cible

Sélectionnez Yes (Oui) si vous voulez que Route 53 détermine s'il doit répondre aux requêtes DNS à l'aide de cet enregistrement en vérifiant l'état de la ressource spécifiée dans le champ Endpoint (Point de terminaison).

Remarques :

API Gateway personnalisé, régional APIs et optimisé pour les périphériques APIs

Il n'y a aucune exigence spécifique pour la définition du champ Evaluate target health (Évaluer l'état de la cible) sur Yes (Oui) lorsque le point de terminaison est une API régionale personnalisée API Gateway ou une API optimisée pour la périphérie.

CloudFront distributions

Vous ne pouvez pas définir Evaluate target health sur Oui lorsque le point de terminaison est une CloudFront distribution.

Environnements Elastic Beanstalk comportant des sous-domaines régionalisés

Si vous spécifiez un environnement Elastic Beanstalk dans Endpoint et que celui-ci contient un équilibreur de charge ELB, Elastic Load Balancing achemine les requêtes uniquement vers les instances Amazon EC2 saines enregistrées auprès de l'équilibreur de charge. (Un environnement contient automatiquement un équilibreur de charge ELB s'il inclut plusieurs EC2 instances Amazon.) Si vous définissez Evaluate target health sur Oui et que les EC2 instances Amazon ne sont pas saines ou que l'équilibreur de charge lui-même ne fonctionne pas correctement, Route 53 achemine les requêtes vers d'autres ressources disponibles qui sont saines, le cas échéant.

Si l'environnement contient une seule EC2 instance Amazon, il n'y a aucune exigence particulière.

Equilibreurs de charge ELB

Le comportement de la surveillance de l'état dépend du type de l'équilibreur de charge :

- Classic Load Balancers : si vous spécifiez un ELB Classic Load Balancer dans Endpoint, Elastic Load Balancing achemine les requêtes uniquement vers les instances EC2 Amazon saines enregistrées auprès de l'équilibreur de charge. Si vous définissez Evaluate Target Health sur Oui et qu'aucune EC2 instance n'est saine ou que l'équilibreur de charge lui-même ne fonctionne pas correctement, Route 53 achemine les requêtes vers d'autres ressources.
- Équilibreurs de charge d'application et Network Load Balancer : si vous spécifiez un équilibreur de charge ELB d'application ou Network Load Balancer et que vous définissez Evaluate target health (Évaluer l'état de la cible) sur Yes (Oui), Route 53 achemine les requêtes vers l'équilibreur de charge en fonction de l'état des groupes cible associés à l'équilibreur de charge :
  - Pour qu'un équilibreur d'application ou un équilibreur Network Load Balancer soit considéré comme sain, chaque groupe cible contenant des cibles doit en contenir au moins une saine. Si un groupe cible contient uniquement des cibles qui ne sont pas saines, l'équilibreur de charge est considéré comme étant lui-même défectueux et Route 53 achemine les requêtes vers d'autres ressources.
  - Un groupe cible qui n'a pas de cibles enregistrées est considéré comme non sain.

> **Note**
>
> Lorsque vous créez un équilibreur de charge, vous configurez les paramètres des surveillances de l'état Elastic Load Balancing ; il ne s'agit pas de surveillances de l'état Route 53, mais elles jouent le même rôle. Ne créez pas de bilans de santé Route 53 pour les EC2 instances que vous enregistrez auprès d'un équilibreur de charge ELB.

Compartiments S3

Il n'y a aucune exigence spécifique pour la définition du champ Evaluate target health (Évaluer l'état de la cible) sur Yes (Oui) lorsque le point de terminaison est un compartiment S3.

Points de terminaison de l'interface d'un VPC Amazon

Il n'y a aucune exigence spécifique pour la définition du champ Evaluate target health (Évaluer l'état de la cible) sur Yes (Oui) lorsque le point de terminaison est un point de terminaison d'interface d'un VPC Amazon.

Autres enregistrements dans la même zone hébergée

Si la AWS ressource que vous spécifiez dans Endpoint est un enregistrement ou un groupe d'enregistrements (par exemple, un groupe d'enregistrements pondérés) mais qu'il ne s'agit pas d'un autre enregistrement alias, nous vous recommandons d'associer un bilan de santé à tous les enregistrements du point de terminaison. Pour de plus amples informations, veuillez consulter Que se passe-t-il lorsque vous omettez des surveillances de l'état ?.

ID d'enregistrement

Entrez une valeur qui identifie de manière unique cet enregistrement dans le groupe d'enregistrements pondérés.

Création d'enregistrements par importation d'un fichier de zone

Si vous migrez à partir d'un autre fournisseur de services DNS, et si votre fournisseur de services DNS actuel vous permet d'exporter vos paramètres DNS actuels dans un fichier de zone, vous pouvez rapidement créer tous les enregistrements pour une zone hébergée Amazon Route 53 en important un fichier de zone.

> **Note**
>
> Un fichier de zone utilise un format standard appelé BIND pour représenter les enregistrements au format texte. Pour plus d'informations sur le format d'un fichier de zone, consultez l'entrée Wikipedia Zone file. Des informations supplémentaires sont disponibles dans la section 3.6.1 RFC 1034, Noms de domaine — Concepts et installations et la section 5 RFC 1035, Noms de domaine — Implémentation et spécification.

Si vous souhaitez créer des enregistrements en important un fichier de zone, veuillez noter les points suivants :

- Le format du fichier de zone doit être conforme à la norme RFC.
- Le nom de domaine des enregistrements du fichier de zone doit correspondre au nom de la zone hébergée.
- Route 53 prend en charge les mots-clés `$ORIGIN` et `$TTL`. Si le fichier de zone comprend les mots-clés `$GENERATE` ou `$INCLUDE`, l'importation échoue et Route 53 renvoie une erreur.

- Lorsque vous importez le fichier de zone, Route 53 ignore l'enregistrement SOA dans le fichier de zone. Route 53 ignore également les enregistrements NS ayant le même nom que la zone hébergée.
- Vous pouvez importer un maximum de 1000 enregistrements.
- Si la zone hébergée contient déjà des enregistrements qui apparaissent dans le fichier de zone, le processus d'importation échoue et aucun enregistrement n'est créé.
- Nous vous recommandons de vérifier le contenu du fichier de zone pour vous assurer que les noms d'enregistrements incluent ou excluent un point final, le cas échéant :
  - Lorsque le nom d'un enregistrement du fichier de zone comprend un point final (`example.com.`), le processus d'importation l'interprète comme un nom de domaine complet et crée un enregistrement Route 53 avec le même nom.
  - Lorsque le nom d'un enregistrement du fichier de zone n'inclut pas de point final (`www`), le processus d'importation concatène ce nom avec le nom de domaine du fichier de zone (`example.com`) et crée un enregistrement Route 53 avec le nom concaténé (`www.example.com`).

  Si le processus d'exportation n'ajoute pas de point final aux noms de domaine complets d'un enregistrement, le processus d'importation Route 53 ajoute le nom de domaine au nom de l'enregistrement. Supposons par exemple que vous importez des enregistrements dans la zone hébergée `example.com` et que le nom d'un enregistrement MX dans le fichier de zone est `mail.example.com`, sans point final. Le processus d'importation Route 53 crée un enregistrement MX nommé `mail.example.com.example.com`.

  > **Important**
  >
  > Pour les enregistrements CNAME, MX, PTR et SRV, ce comportement s'applique également au nom de domaine qui est inclus dans la valeur RDATA. Supposons par exemple que vous avez un fichier de zone pour `example.com`. Si un enregistrement CNAME du fichier de zone (`support`, sans point final) comporte une valeur RDATA `www.example.com` (également sans point final), le processus d'importation crée un enregistrement Route 53 nommé `support.example.com` qui achemine le trafic vers `www.example.com.example.com`. Avant d'importer votre fichier de zone, consultez les valeurs RDATA et procédez à la mise à jour nécessaire.

Route 53 ne prend pas en charge l'exportation d'enregistrements vers un fichier de zone.

> **Note**
>
> Si vous créez un enregistrement qui porte le même nom que la zone hébergée, n'entrez aucune valeur (par exemple, un symbole @) dans le champ Name (Nom).

Pour créer des enregistrements par importation d'un fichier de zone

1. Obtenez un fichier de zone auprès du fournisseur de services DNS actuellement en charge du domaine. Les processus et la terminologie varient d'un fournisseur de service à l'autre. Reportez-vous à l'interface et la documentation du fournisseur pour obtenir des informations sur l'exportation ou l'enregistrement de vos données dans un fichier de zone ou dans un fichier BIND.

   Si le processus n'est pas évident, demandez au service client de votre fournisseur DNS actuel de vous communiquer les informations relatives à votre liste d'enregistrements ou à votre fichier de zone.
2. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
3. Dans le panneau de navigation, choisissez Zones hébergées.
4. Sur la page Hosted zones (Zones hébergées), créez une zone hébergée :
   a. Choisissez Create Hosted Zone (Créer une zone hébergée).
   b. Entrez le nom de votre domaine et, le cas échéant, un commentaire.
   c. Sélectionnez Create (Créer).
5. Choisissez Import Zone File (Importer un fichier de zone).
6. Dans le volet Import Zone File (Importer un fichier de zone), collez le contenu de votre fichier de zone dans la zone de texte Zone file (Fichier de zone).
7. Choisissez Import (Importer).

   > **Note**
   >
   > En fonction du nombre d'enregistrements dans votre fichier de zone, la création des enregistrements peut prendre quelques minutes.

8. Si vous utilisez un autre service DNS pour le domaine (ce qui est courant lorsque vous avez enregistré le domaine avec un autre bureau), migrez le service DNS vers Route 53. Lorsque cette étape est terminée, votre bureau d'enregistrement commence à identifier Route 53 en tant que service DNS en réponse aux requêtes DNS pour votre domaine, et les requêtes commencent à être envoyées vers des serveurs DNS Route 53. (En règle générale, un délai d'un jour ou deux est nécessaire avant que les requêtes DNS commencent à être acheminées vers Route 53, car les informations relatives à votre service DNS précédent sont mises en cache sur des résolveurs DNS pendant cette durée.) Pour de plus amples informations, veuillez consulter Configuration d'Amazon Route 53 en tant que service DNS d'un domaine existant.

Modification des enregistrements

La procédure suivante explique comment modifier des enregistrements à l'aide de la console Amazon Route 53. Pour plus d'informations sur la façon de modifier des enregistrements à l'aide de l'API Route 53, consultez ChangeResourceRecordSetsle manuel de référence de l'API Amazon Route 53.

> **Note**
>
> La propagation de vos registres modifiés sur les serveurs DNS Route 53 n'est pas immédiate. À l'heure actuelle, le seul moyen de vérifier que les modifications se sont propagées consiste à utiliser l'action GetChangeAPI. Les changements se propagent généralement sur tous les serveurs de Route 53 en 60 secondes.

Pour modifier des enregistrements à l'aide de la console Route 53

1. Si vous ne modifiez pas des enregistrements d'alias, passez à l'étape 2.

   Si vous modifiez des enregistrements d'alias qui acheminent le trafic vers un Classic Load Balancer Elastic Load Balancing, Application Load Balancer ou Network Load Balancer, et si vous avez créé votre zone hébergée Route 53 et votre équilibreur de charge à l'aide de différents comptes, exécutez la procédure Obtention du nom DNS d'un équilibreur de charge Elastic Load Balancing pour obtenir le nom DNS de l'équilibreur de charge.

   Si vous modifiez des enregistrements d'alias pour une autre AWS ressource, passez à l'étape 2.

2. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.

3. Dans le panneau de navigation, choisissez Zones hébergées.
4. Sur la page Hosted Zones (Zones hébergées), choisissez sur la ligne de la zone hébergée qui contient les enregistrements que vous souhaitez modifier.
5. Sélectionnez la ligne de l'enregistrement que vous voulez modifier, puis entrez vos modifications dans le panneau Edit record (Modifier l'enregistrement).
6. Entrez les valeurs applicables. Pour de plus amples informations, veuillez consulter Valeurs à spécifier lorsque vous créez ou modifiez des enregistrements Amazon Route 53.
7. Sélectionnez Save Changes (Enregistrer les modifications).
8. Si vous modifiez plusieurs enregistrements, répétez les étapes 5 à 7.

Suppression d'enregistrements

La procédure suivante explique comment supprimer des enregistrements à l'aide de la console Route 53. Pour plus d'informations sur la façon de supprimer des enregistrements à l'aide de l'API Route 53, consultez ChangeResourceRecordSetsla référence de l'API Amazon Route 53.

> **Note**
>
> La propagation de vos registres modifiés sur les serveurs DNS Route 53 n'est pas immédiate. À l'heure actuelle, le seul moyen de vérifier que les modifications se sont propagées consiste à utiliser l'action GetChangeAPI. Les changements se propagent généralement sur tous les serveurs de Route 53 en 60 secondes.

Pour supprimer des enregistrements

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Sur la page Hosted Zones (Zones hébergées), choisissez la ligne de la zone hébergée qui contient les enregistrements que vous souhaitez supprimer.
3. Dans la liste des enregistrements, sélectionnez l'enregistrement que vous voulez supprimer.

   Pour sélectionner plusieurs enregistrements consécutifs, sélectionnez la première ligne, maintenez la touche Maj, puis sélectionnez la dernière ligne. Pour sélectionner plusieurs enregistrements non consécutifs, choisissez la première ligne, maintenez la touche Ctrl enfoncée, puis choisissez les autres lignes.

Vous ne pouvez pas supprimer les registres dont la valeur est NS ou SOA pour le champ Type.

4. Sélectionnez Delete (Supprimer).
5. Choisissez Delete (Supprimer) pour fermer la boîte de dialogue.

Liste des enregistrements

La procédure suivante explique comment utiliser la console Amazon Route 53 pour répertorier les enregistrements d'une zone hébergée. Pour plus d'informations sur la façon de répertorier des enregistrements à l'aide de l'API Route 53, consultez ListResourceRecordSetsle manuel de référence de l'API Amazon Route 53.

Pour lister des enregistrements

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le panneau de navigation, choisissez Zones hébergées.
3. Sur la page Hosted Zones (Zones hébergées), choisissez le nom d'une zone hébergée.
4. Pour changer le mode de recherche, choisissez l'icône d'engrenage en haut à droite du tableau Enregistrements. Choisissez-en parmi :

   - Automatique

     Dans ce mode, le service utilise un filtre basé sur un certain nombre d'enregistrements. Complet pour moins de 2000 et rapide pour plus de 2000 enregistrements.
   - Complet

     Dans ce mode, tous les filtres de recherche sont disponibles, mais les performances de recherche peuvent être plus lentes.
   - Rapide

     Dans ce mode, certaines fonctionnalités avancées ne sont pas disponibles, mais les performances de recherche seront plus rapides.

Pour afficher uniquement les enregistrements sélectionnés, entrez les critères de recherche applicables au-dessus de la liste des enregistrements. En mode automatique, le comportement

de recherche varie selon que la zone hébergée contient jusqu'à 2000 enregistrements ou plus de 2 000 enregistrements :

Jusqu'à 2000 enregistrements et mode complet

- Pour afficher les enregistrements ayant des valeurs spécifiques, entrez une valeur dans la barre de recherche et appuyez sur Entrée. Par exemple, pour afficher les enregistrements dont l'adresse IP commence par 192.0, entrez cette valeur dans le champ Search (Recherche) et appuyez sur Entrée.
- Pour afficher uniquement les enregistrements ayant le même type d'enregistrement DNS, sélectionnez le Record type (Type d'enregistrement) dans la liste déroulante et saisissez le type d'enregistrement.
- Pour afficher uniquement les registres d'alias, sélectionnez Alias dans la liste déroulante, puis saisissez **`Yes`**.
- Pour afficher uniquement les enregistrements pondérés, sélectionnez Routing policy (Stratégie de routage) dans la liste déroulante, puis entrez **`WEIGHTED`**.

Plus de 2000 enregistrements et mode rapide

- Vous pouvez effectuer des recherches uniquement sur les noms d'enregistrement, et non sur les valeurs d'enregistrements. De même, vous ne pouvez pas filtrer en fonction du type d'enregistrement, ou sur l'alias ou sur les enregistrements pondérés.

  Pour ce faire, placez votre curseur dans la zone de texte Filtre, sélectionnez Propriétés, puis Nom de l'enregistrement.
- Pour les enregistrements ayant trois étiquettes (trois parties séparées par des points), lorsque vous saisissez une valeur dans le champ de recherche et appuyez sur Entrée, la console Route 53 effectue automatiquement une recherche de caractère générique sur la troisième étiquette à partir de la droite dans le nom d'enregistrement. Par exemple, supposons que la zone hébergée example.com contienne 100 enregistrements appelés record1.example.com jusqu'à record100.example.com. (Record1 est la troisième étiquette à partir de la droite.) Voici ce qui se produit lorsque vous effectuez une recherche sur les valeurs suivantes :
  - record1 : la console Route 53 recherche record1*. example.com, qui renvoie record1.example.com, record10.example.com jusqu'à record19.example.com et record100.example.com.
  - record1.example.com : comme dans l'exemple précédent, la console recherche record1*. example.com et renvoie les mêmes enregistrements.
  - 1 :: la console recherche 1*.example.com et ne renvoie aucun enregistrement.

- example : la console recherche example*.example.com et ne renvoie aucun enregistrement.
- example.com : dans cet exemple, la console n'effectue pas de recherche de caractère générique. Elle renvoie tous les enregistrements de la zone hébergée.
- Mode de recherche automatique : lorsque vous utilisez ce mode de recherche, vous devez d'abord fournir une propriété, comme le nom de l'enregistrement, pour pouvoir effectuer la recherche.

> **Note**
>
> Si la troisième étiquette à partir de la droite contient un ou plusieurs traits d'union (comme `third-label.example.com`), et si vous recherchez la partie de la troisième étiquette immédiatement avant le trait d'union (`third` dans cet exemple), Route 53 ne renverra aucun enregistrement. Au lieu de cela, incluez le trait d'union (recherchez `third-`) ou omettez le caractère situé immédiatement avant le trait d'union (recherchez `third`).

- Pour les enregistrements qui ont quatre étiquettes ou plus, vous devez spécifier le nom exact de l'enregistrement. Aucune recherche générique n'est prise en charge. Par exemple, si la zone hébergée inclut un enregistrement appelé label4.record1.example.com, vous pouvez trouver cet enregistrement uniquement si vous spécifiez label4.record1.example.com dans le champ de recherche.

Configuration de la signature DNSSEC dans Amazon Route 53

La signature DNSSEC (Domain Name System Security Extensions) permet aux résolveurs DNS de valider qu'une réponse DNS provient d'Amazon Route 53 et qu'elle n'a pas été altérée. Lorsque vous utilisez la signature DNSSEC, chaque réponse pour une zone hébergée est signée à l'aide du chiffrement par clé publique. Pour un aperçu du DNSSEC, consultez la section DNSSEC de AWS re:Invent 2021 - Amazon Route 53 : A year in review.

Dans ce chapitre, nous expliquons comment activer la signature DNSSEC pour Route 53, comment utiliser les clés de signature par clé (KSKs) et comment résoudre les problèmes. Vous pouvez utiliser la signature DNSSEC dans l'API AWS Management Console ou par programmation. Pour plus d'informations sur l'utilisation de la CLI ou SDKs sur l'utilisation de Route 53, consultezConfigurer Amazon Route 53.

Avant d'activer la signature DNSSEC, prenez les éléments suivants en considération :

- Pour éviter une panne de zone et éviter que votre domaine ne devienne indisponible, vous devez rapidement corriger et résoudre les erreurs DNSSEC. Nous vous recommandons vivement de configurer une CloudWatch alarme qui vous avertira chaque fois qu'une `DNSSECInternalFailure` `DNSSECKeySigningKeysNeedingAction` erreur est détectée. Pour de plus amples informations, veuillez consulter Surveillance des zones hébergées à l'aide d'Amazon CloudWatch.
- Il existe deux types de clés dans DNSSEC : une clé KSK et une clé ZSK. Dans la signature DNSSEC Route 53, chaque clé KSK est basée sur une clé asymétrique gérée par le client dans AWS KMS que vous possédez. Vous êtes responsable de la gestion des clés KSK, ce qui inclut la rotation, le cas échéant. La gestion des ZSK est assurée par Route 53.
- Lorsque vous activez la signature DNSSEC pour une zone hébergée, Route 53 limite la TTL à une semaine. Si vous définissez une TTL de plus d'une semaine pour les registres dans la zone hébergée, vous n'obtenez pas d'erreur. Cependant, la Route 53 applique une TTL d'une semaine pour les registres. Les registres dont la TTL est inférieure à une semaine et les registres dans d'autres zones hébergées pour lesquelles la signature DNSSEC n'est pas activée ne sont pas affectés.
- Lorsque vous utilisez la signature DNSSEC, les configurations multi-fournisseurs ne sont pas prises en charge. Si vous avez configuré des serveurs de noms en marque blanche (également appelés serveurs de noms personnalisés ou serveurs de noms privés), assurez-vous que ces serveurs de noms sont fournis par un seul fournisseur DNS.
- Certains fournisseurs de DNS ne prennent pas en charge les enregistrements DS (Delegation Signer) dans leur DNS officiel. Si votre zone parent est hébergée par un fournisseur DNS qui ne prend pas en charge les requêtes DS (sans définir d'indicateur AA dans la réponse aux requêtes DS), lorsque vous activez DNSSEC dans sa zone enfant, la zone enfant ne peut plus être résolue. Assurez-vous que votre fournisseur DNS prend en charge les enregistrements DS.
- Il peut être utile de configurer des autorisations IAM pour permettre à un autre utilisateur, outre le propriétaire de la zone, d'ajouter ou de supprimer des registres dans la zone. Par exemple, un propriétaire de zone peut ajouter une clé KSK et activer la signature, et peut également être responsable de la rotation des clés. Toutefois, une autre personne peut être responsable de l'utilisation d'autres registres pour la zone hébergée. Pour consulter un exemple de politique IAM, consultez Exemples d'autorisations pour un propriétaire d'enregistrement de domaine.
- Pour vérifier si le TLD prend en charge le protocole DNSSEC, consultez. Domaines que vous pouvez enregistrer avec Amazon Route 53

Rubriques

- Activation de la signature DNSSEC et établissement d'une chaîne d'approbation
- Désactivation de la signature DNSSEC
- Utilisation des clés gérées par le client pour DNSSEC
- Utilisation de clés de signature () KSKs
- Gestion des clés KMS et ZSK dans Route 53
- Preuves DNSSEC d'inexistence dans Route 53
- Résolution des problèmes de signature DNSSEC

Activation de la signature DNSSEC et établissement d'une chaîne d'approbation

Les étapes progressives s'appliquent au propriétaire de la zone hébergée et au responsable de la zone parent. Il peut s'agir de la même personne, mais si ce n'est pas le cas, le propriétaire de la zone doit en informer le responsable de la zone parent et collaborer avec celui-ci.

Nous vous recommandons de suivre les étapes décrites dans cet article pour signer et inclure votre zone dans la chaîne d'approbation. Les étapes suivantes réduiront le risque d'onboarding sur le protocole DNSSEC (Domain Name System Security Extensions).

> **Note**
>
> Assurez-vous de lire les prérequis avant de vous lancer dans Configuration de la signature DNSSEC dans Amazon Route 53.

Trois étapes permettent d'activer la signature DNSSEC, comme décrit dans les sections suivantes.

Rubriques

- Étape 1 : Préparer l'activation de la signature DNSSEC
- Étape 2 : Activer la signature DNSSEC et créer une clé KSK
- Étape 3 : Établir une chaîne d'approbation

Étape 1 : Préparer l'activation de la signature DNSSEC

Les étapes de préparation vous aident à réduire le risque d'onboarding à DNSSEC en contrôlant la disponibilité de la zone et en réduisant les temps d'attente entre l'activation de la signature et l'insertion du registre Delegation Signer (DS).

Pour se préparer à l'activation de la signature DNSSEC

1. Contrôlez la disponibilité de la zone.

   Vous pouvez contrôler la zone de disponibilité des noms de domaine. Cela peut vous aider à résoudre tous les problèmes pouvant justifier un retour à l'étape précédente après avoir activé la signature DNSSEC. Vous pouvez contrôler les noms de domaine ayant le plus de trafic à l'aide de la journalisation des requêtes. Pour plus d'informations sur la configuration de la journalisation des requêtes, consultez Surveillance d'Amazon Route 53.

   Vous pouvez effectuer la surveillance via un script shell ou via un service tiers. Il ne devrait toutefois pas s'agir du seul signal permettant de déterminer si une restauration est nécessaire. Vous recevrez peut-être également des commentaires de vos clients en raison de l'indisponibilité d'un domaine.

2. Réduisez la TTL maximale de la zone.

   La TTL maximale de la zone est le registre TTL le plus long de la zone. Dans l'exemple de zone ci-dessous, la TTL maximale de la zone est de 1 jour (86 400 secondes).

Nom	TTL	Classe de registre	Type de registre	Données de registre
exemple.com.	900	IN	SOA	ns1.exemple.com. hostmaster.exemple.com. 2002022401 10800 15 604800 300
exemple.com.	900	IN	NS	

Nom	TTL	Classe de registre	Type de registre	Données de registre
				ns1.exemple.com.
route53.exemple.com.	86400	IN	TXT	**some txt record**

La réduction de la TTL maximale de la zone permettra de réduire le temps d'attente entre l'activation de la signature et l'insertion du registre Delegation Signer (DS). Nous vous recommandons de réduire la TTL maximale de la zone à 1 heure (3 600 secondes). Cela vous permet de revenir en arrière après seulement une heure si un résolveur rencontre des problèmes avec la mise en cache des registres signés.

Restauration : annulez les modifications TTL.

3. Réduisez le champ SOA TTL and SOA minimum (Valeur TTL SOA et SOA minimale).

   Le champ SOA minimum (Valeur SOA minimale) est le dernier champ des données de registre SOA. Dans l'exemple de registre SOA suivant, le champ Minimum (Minimal) comporte une valeur de 5 minutes (300 secondes).

Nom	TTL	Classe de registre	Type de registre	Données de registre
exemple.com.	900	IN	SOA	ns1.exemple.com. hostmaster.exemple.com. 2002022401 10800 15 604800 300

Le champ SOA TTL and SOA minimum (Valeur TTL SOA et SOA minimale) détermine pendant combien de temps les résolveurs mémorisent les réponses négatives. Une fois que vous avez

activé la signature, les serveurs de noms Route 53 commencent à renvoyer des registres NSEC pour obtenir des réponses négatives. NSEC contient des informations que les résolveurs peuvent utiliser pour synthétiser une réponse négative. Si vous devez revenir en arrière, car les informations NSEC ont amené un résolveur à supposer une réponse négative pour un nom, il suffit d'attendre le maximum du champ SOA TTL and SOA minimum (Valeur TTL SOA et SOA minimale) pour que le résolveur arrête l'hypothèse.

Restauration : annulez les modifications de la source de noms (SOA, Start of Authority).

4. Assurez-vous que les modifications du champ TTL and SOA minimum (Valeur TTL et SOA minimale) sont appliquées.

   Utilisez-le GetChangepour vous assurer que les modifications que vous avez apportées jusqu'à présent ont été propagées à tous les serveurs DNS Route 53.

Étape 2 : Activer la signature DNSSEC et créer une clé KSK

Vous pouvez activer la signature DNSSEC et créer une clé de signature par clé (KSK) en utilisant AWS CLI ou sur la console Route 53.

- INTERFACE DE LIGNE DE COMMANDE (CLI)
- Console

Lorsque vous fournissez ou créez une clé KMS, plusieurs exigences s'appliquent. Pour de plus amples informations, veuillez consulter Utilisation des clés gérées par le client pour DNSSEC.

CLI

Vous pouvez utiliser une clé que vous possédez déjà ou en créer une en exécutant une commande AWS CLI telle que la suivante, en utilisant vos propres valeurs pour `hostedzone_id`, `cmk_arn`, `ksk_name` et `unique_string` (pour rendre la demande unique) :

```
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
```

Pour plus d'informations sur les clés gérées par le client, consultez Utilisation des clés gérées par le client pour DNSSEC. Voir aussi CreateKeySigningKey.

Pour activer la signature DNSSEC, exécutez une AWS CLI commande comme celle-ci, en utilisant votre propre valeur pour : `hostedzone_id`

```
aws --region us-east-1 route53 enable-hosted-zone-dnssec \
   --hosted-zone-id $hostedzone_id
```

Pour plus d'informations, consultez enable-hosted-zone-dnssecet EnableHostedZoneDNSSEC.

Console

Pour activer la signature DNSSEC et créer une clé KSK

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le panneau de navigation, choisissez Hosted zones (Zones hébergées), puis choisissez une zone hébergée pour laquelle vous souhaitez activer la signature DNSSEC.
3. Dans l'onglet DNSSEC signing (Signature DNSSEC), choisissez Enable DNSSEC signing (Activer la signature DNSSEC).

   > **Note**
   >
   > Si l'option de cette section est Disable DNSSEC signing (Désactiver la signature DNSSEC), vous avez déjà réalisé la première étape de l'activation de la signature DNSSEC. Assurez-vous d'établir une chaîne d'approbation pour la zone hébergée pour DNSSEC, ou assurez-vous qu'il en existe déjà une. Ensuite, vous avez terminé. Pour de plus amples informations, veuillez consulter Étape 3 : Établir une chaîne d'approbation.

4. Dans Key-signing key (KSK) creation [Création d'une clé de signature de clé (KSK)], choisissez Create new KSK (Créer une clé KSK) et sous Provide KSK name (Fournir un nom de clé KSK), entrez un nom pour la clé KSK que Route 53 créera pour vous. Le nom peut contenir des chiffres, des lettres et des traits de soulignement (_). Il doit être unique.
5. Sous Customer managed CMK (Clé CMK gérée par le client), choisissez la clé gérée par le client à utiliser par Route 53 lorsqu'il crée la clé KSK pour vous. Vous pouvez utiliser une clé gérée par le client existante qui s'applique à la signature DNSSEC, ou créer une nouvelle clé gérée par le client.

Lorsque vous fournissez ou créez une clé gérée par le client, plusieurs exigences s'appliquent. Pour plus d'informations, consultez Utilisation des clés gérées par le client pour DNSSEC.

6. Saisissez l'alias d'une clé gérée par le client existante. Si vous souhaitez utiliser une nouvelle clé gérée par le client, saisissez un alias pour la clé gérée par le client et Route 53 en créera un pour vous.

> **Note**
>
> Si vous choisissez que Route 53 crée une clé gérée par le client, sachez que des frais distincts s'appliquent pour chaque clé gérée par le client. Pour plus d'informations, consultez Tarification d'AWS Key Management Service.

7. Choisissez Enable DNSSEC signing (Activer la signature DNSSEC).

Une fois que vous avez activé la signature de zone, suivez les étapes ci-après (que vous utilisiez la console ou la CLI) :

1. Assurez-vous que la signature de zone est effective.

   Si vous l'avez utilisé AWS CLI, vous pouvez utiliser l'identifiant d'opération indiqué dans la sortie de l'`EnableHostedZoneDNSSEC()`appel pour exécuter get-change ou GetChangepour vous assurer que tous les serveurs DNS Route 53 signent les réponses (status `=INSYNC`).

2. Attendez au moins la TTL maximale de la zone précédente.

   Attendez que les résolveurs vident tous les registres non signés de leur cache. Pour ce faire, vous devez attendre au moins la TTL maximale de la zone précédente. Dans la zone `example.com` ci-dessus, le temps d'attente serait de 1 jour.

3. Contrôlez les rapports des problèmes de clients.

   Une fois que vous avez activé la signature de zone, vos clients remarqueront peut-être des problèmes liés aux périphériques réseau et aux résolveurs. La période de surveillance recommandée est de 2 semaines.

   Voici des exemples de problèmes que vous pourriez constater :

- Certains périphériques réseau peuvent limiter la taille de la réponse DNS à moins de 512 octets, ce qui est trop petit pour certaines réponses signées. Ces périphériques réseau doivent être reconfigurés pour autoriser des tailles plus grandes de réponses DNS.
- Certains périphériques réseau effectuent une inspection approfondie des réponses DNS et suppriment certains registres incompréhensibles, comme ceux utilisés pour DNSSEC. Ces périphériques doivent être reconfigurés.
- Les résolveurs de certains clients affirment qu'ils peuvent accepter une réponse UDP plus grande que celle prise en charge par leur réseau. Vous pouvez tester la capacité de votre réseau et configurer vos résolveurs de manière appropriée. Pour plus d'informations, consultez Serveur de test de taille de réponse DNS.

Annulation : appelez DisableHostedZoneDNSSEC puis annulez les étapes. Étape 1 : Préparer l'activation de la signature DNSSEC

Étape 3 : Établir une chaîne d'approbation

Après avoir activé la signature DNSSEC pour une zone hébergée dans Route 53, établissez une chaîne d'approbation pour la zone hébergée pour terminer la configuration de votre signature DNSSEC. Pour ce faire, créez un registre Delegation Signer dans la zone hébergée parent, pour votre zone hébergée, à l'aide des informations fournies par Route 53. Selon l'emplacement dans lequel votre domaine est membre, ajoutez le registre à la zone hébergée parent dans Route 53 ou dans un autre bureau d'enregistrement de domaine.

Pour établir une chaîne d'approbation pour la signature DNSSEC

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le panneau de navigation, choisissez Hosted zones (Zones hébergées), puis choisissez une zone hébergée pour laquelle vous souhaitez établir une chaîne d'approbation DNSSEC. Vous devez d'abord activer la signature DNSSEC.
3. Dans l'onglet DNSSEC signing (Signature DNSSEC), sous DNSSEC signing (Signature DNSSEC), choisissez View information to create DS record (Afficher les informations pour créer un registre DS).

> **Note**
>
> Si vous ne voyez pas View information to create DS record (Afficher les informations pour créer un registre DS) dans cette section, vous devez activer la signature DNSSEC avant d'établir la chaîne d'approbation. Choisissez Enable DNSSEC signing (Activer la signature DNSSEC) et effectuez les étapes, comme décrit dans Étape 2 : Activer la signature DNSSEC et créer une clé KSK, puis revenez à ces étapes pour établir la chaîne d'approbation.

4. Sous Establish a chain of trust (Établir une chaîne d'approbation), choisissez Route 53 registrar (Bureau d'enregistrement Route 53) ou Another domain registrar (Autre bureau d'enregistrement de domaine), en fonction de l'emplacement dans lequel votre domaine est membre.
5. Utiliser les valeurs fournies à partir de l'étape 3 pour créer un registre DS pour la zone hébergée parent dans Route 53. Si votre domaine n'est pas hébergé sur Route 53, utilisez les valeurs fournies pour créer un registre DS sur le site Web de votre bureau d'enregistrement de domaines.

   Établissez une chaîne de confiance pour la zone parent :

   - Si votre domaine est géré via Route 53, procédez comme suit :

     Assurez-vous de configurer l'algorithme de signature (ECDSAP256SHA256 et le type 13) et l'algorithme de synthèse (SHA-256 et type 2) corrects.

     Si Route 53 est votre bureau d'enregistrement, procédez comme suit dans la console Route 53 :

     1. Notez les valeurs Key type (Type de clé), Signing algorithm (Algorithme de signature) et Public key (Clé publique). Dans le panneau de navigation, choisissez Registered domains (Domaines membres).
     2. Sélectionnez un domaine, puis, dans l'onglet Clés DNSSEC, choisissez Ajouter une clé.
     3. Dans la boîte de dialogue Manage DNSSEC keys (Gérer les clés DNSSEC), choisissez le Key type (Type de clé) et l'Algorithm (Algorithme) appropriés au Route 53 registrar (Bureau d'enregistrement Route 53) dans les menus déroulants.
     4. Copiez la Public key (Clé publique) pour le bureau d'enregistrement Route 53. Dans la boîte de dialogue Manage DNSSEC keys (Gérer les clés DNSSEC), collez la valeur dans la zone Public key (Clé publique).

5. Choisissez Add (Ajouter).

   Route 53 ajoute le registre DS à la zone parent à partir de la clé publique. Par exemple, si votre domaine est `example.com`, le registre DS est ajouté à la zone DNS .com.

- Si votre domaine est géré sur un autre registre, suivez les instructions de la section Autre bureau d'enregistrement de domaines.

  Pour vous assurer que les étapes suivantes se déroulent correctement, présentez une TTL DS faible à la zone parent. Nous vous recommandons de définir la TTL DS sur 5 minutes (300 secondes) pour une récupération plus rapide si vous devez annuler vos modifications.

  - Établissez une chaîne de confiance pour la zone enfant :

    Si votre zone parent est administrée par un autre registre, contactez votre bureau d'enregistrement pour présenter le registre DS de votre zone. En règle générale, vous ne pourrez pas ajuster la TTL du registre DS.

  - Si votre zone parent est hébergée sur Route 53, contactez le propriétaire de la zone parent pour présenter le registre DS de votre zone.

    Fournissez `$ds_record_value` au propriétaire de la zone parent. Vous pouvez l'obtenir en cliquant sur Afficher les informations pour créer un enregistrement DS dans la console et en copiant le champ d'enregistrement DS, ou en appelant l'API GetDNSSEC et en récupérant la valeur du champ « » : DSRecord

    ```
    aws --region us-east-1 route53 get-dnssec
                --hosted-zone-id $hostedzone_id
    ```

    Le propriétaire de la zone parent peut insérer le registre via la console Route 53 ou la CLI.

    - Pour insérer l'enregistrement DS à l'aide de AWS CLI, le propriétaire de la zone parent crée et nomme un fichier JSON similaire à l'exemple suivant. Le propriétaire de la zone parent peut nommer le fichier de manière semblable : `inserting_ds.json`.

      ```
      {
          "HostedZoneId": "$parent_zone_id",
          "ChangeBatch": {
              "Comment": "Inserting DS for zone $zone_name",
              "Changes": [
                  {
                      "Action": "UPSERT",
      ```

```
                "ResourceRecordSet": {
                    "Name": "$zone_name",
                    "Type": "DS",
                    "TTL": 300,
                    "ResourceRecords": [
                        {
                            "Value": "$ds_record_value"
                        }
                    ]
                }
            }
        ]
    }
}
```

Ensuite, exécutez la commande suivante :

```
aws --region us-east-1 route53 change-resource-record-sets
            --cli-input-json file://inserting_ds.json
```

- Pour insérer le registre DS à l'aide de la console,

  Ouvrez la console Route 53 à l'adresse https://console.aws.amazon.com/route53/.

  Dans le panneau de navigation, choisissez Hosted zones (Zones hébergées), le nom de votre zone hébergée, puis le bouton Create record (Créer un registre). Assurez-vous de choisir le routage simple pour la Routing policy(Politique de routage).

  Dans le champ Nom de l'enregistrement, entrez le même nom que le`$zone_name`, sélectionnez DS dans le menu déroulant Type d'enregistrement, entrez la valeur de `$ds_record_value` dans le champ Valeur, puis choisissez Créer des enregistrements.

Restauration : supprimez le DS de la zone parent, attendez la TTL DS, puis annulez les étapes d'établissement de l'approbation. Si la zone parent est hébergée sur Route 53, le propriétaire de la zone parent peut passer `Action` de `UPSERT` à `DELETE` dans le fichier JSON, puis réexécuter l'exemple de CLI ci-dessus.

6. Attendez que les mises à jour se propagent, en fonction de la TTL pour vos registres de domaine.

Si la zone parent est sur le service DNS Route 53, le propriétaire de la zone parent peut confirmer la propagation complète via l'GetChangeAPI.

Sinon, vous pouvez rechercher périodiquement le registre DS dans la zone parent, puis attendre ensuite 10 minutes de plus pour augmenter la probabilité de propagation complète de l'insertion du registre DS. Notez que certains bureaux d'enregistrement ont planifié l'insertion de DS, par exemple une fois par jour.

Lorsque vous présentez le registre Delegation Signer (DS) dans la zone parent, les résolveurs validés qui ont récupéré le DS commenceront à valider les réponses à partir de la zone.

Pour vous assurer que les étapes d'établissement de l'approbation se déroulent correctement, renseignez les informations suivantes :

1. Trouvez la TTL NS maximale.

   2 jeux de registres NS sont associés à vos zones :

   - Registre NS de délégation : il s'agit du registre NS de votre zone détenu par la zone parent. Pour le trouver, exécutez les commandes Unix suivantes (si votre zone est exemple.com, la zone parent est com) :

     ```
     dig -t NS com
     ```

     Choisissez l'un des registres NS, puis exécutez les éléments suivants :

     ```
     dig @one of the NS records of your parent zone -t NS example.com
     ```

     Par exemple :

     ```
     dig @b.gtld-servers.net. -t NS example.com
     ```

   - Registre NS dans la zone : il s'agit du registre NS de votre zone. Pour le trouver, exécutez la commande Unix suivante :

     ```
     dig @one of the NS records of your zone -t NS example.com
     ```

     Par exemple :

     ```
     dig @ns-0000.awsdns-00.co.uk. -t NS example.com
     ```

Notez la TTL maximale pour les deux zones.

2. Attendez la TTL NS maximale.

   Avant l'insertion de DS, les résolveurs reçoivent une réponse signée, mais ne valident pas la signature. Lorsque le registre DS est inséré, les résolveurs ne le verront pas avant l'expiration du registre NS de la zone. Lorsque les résolveurs extraient à nouveau le registre NS, le registre DS est également renvoyé.

   Si votre client exécute un résolveur sur un hôte dont l'horloge n'est pas synchronisée, assurez-vous que l'horloge n'avance pas ni ne recule de 1 heure de l'heure correcte.

   Une fois cette étape terminée, tous les résolveurs compatibles avec DNSSEC valideront votre zone.

3. Observez la résolution des noms.

   Vous devez noter qu'il n'existe aucun problème avec les résolveurs qui valident votre zone. Assurez-vous également de prendre en compte le temps nécessaire à vos clients pour vous signaler les problèmes.

   Nous vous recommandons d'effectuer la surveillance pendant 2 semaines au maximum.

4. (Facultatif) Allongez le DS et le NS. TTLs

   Si la configuration vous convient, vous pouvez enregistrer les modifications de TTL et de SOA que vous avez apportées. Notez que Route 53 limite la TTL à une semaine pour les zones signées. Pour de plus amples informations, veuillez consulter Configuration de la signature DNSSEC dans Amazon Route 53.

   Si vous pouvez modifier la TTL DS, nous vous recommandons de la définir sur 1 heure.

Désactivation de la signature DNSSEC

Les étapes de désactivation de la signature DNSSEC dans Route 53 varient en fonction de la chaîne d'approbation dont votre zone hébergée fait partie.

Par exemple, il est possible que votre zone hébergée dispose d'une zone parent dotée d'un registre Delegation Signer (DS), ce qui constitue une partie d'une chaîne d'approbation. Il est également possible que votre zone hébergée soit elle-même une zone parent pour les zones enfant qui ont activé la signature DNSSEC, ce qui constitue une autre partie de la chaîne d'approbation. Étudiez

et déterminez la chaîne d'approbation complète de votre zone hébergée avant de désactiver la signature DNSSEC.

La chaîne d'approbation de votre zone hébergée qui active la signature DNSSEC doit être soigneusement annulée lorsque vous désactivez la signature. Pour supprimer votre zone hébergée de la chaîne d'approbation, supprimez tous les registres DS en place pour la chaîne d'approbation qui inclut cette zone hébergée. Cela signifie que vous devez effectuer les tâches suivantes, dans l'ordre :

1. Supprimez tous les registres DS que cette zone hébergée possède pour les zones enfant qui font partie d'une chaîne d'approbation.
2. Supprimez le registre DS de la zone parent. Ignorez cette étape si vous disposez d'une île d'approbation (aucun registre DS dans la zone parent et aucun registre DS pour les zones enfant dans cette zone).
3. Si vous ne parvenez pas à supprimer des enregistrements DS, afin de supprimer la zone de la chaîne d'approbation, supprimez les enregistrements NS de la zone parent. Pour de plus amples informations, veuillez consulter Ajout ou modification de serveurs de noms et d'enregistrements de type glue pour un domaine.

Les étapes progressives suivantes vous permettent de contrôler le caractère effectif des différentes étapes afin d'éviter les problèmes de disponibilité DNS dans votre zone.

Pour désactiver la signature DNSSEC

1. Contrôlez la disponibilité de la zone.

   Vous pouvez contrôler la zone de disponibilité des noms de domaine. Cela peut vous aider à résoudre tous les problèmes pouvant justifier un retour à l'étape précédente après avoir activé la signature DNSSEC. Vous pouvez contrôler les noms de domaine ayant le plus de trafic à l'aide de la journalisation des requêtes. Pour plus d'informations sur la configuration de la journalisation des requêtes, consultez Surveillance d'Amazon Route 53.

   La surveillance peut être effectuée via un script shell ou via un service payant. Il ne devrait toutefois pas s'agir du seul signal permettant de déterminer si une restauration est nécessaire. Vous recevrez peut-être également des commentaires de vos clients en raison de l'indisponibilité d'un domaine.
2. Trouvez la TTL DS actuelle.

   Pour ce faire, exécutez la commande Unix suivante :

```
dig -t DS example.com example.com
```

3. Trouvez la TTL NS maximale.

   2 jeux de registres NS sont associés à vos zones :

   - Registre NS de délégation : il s'agit du registre NS de votre zone détenu par la zone parent. Pour le trouver, exécutez les commandes Unix suivantes :

     Commencez par trouver le NS de votre zone parent (si votre zone est exemple.com, la zone parent est com) :

     ```
     dig -t NS com
     ```

     Choisissez l'un des registres NS, puis exécutez les éléments suivants :

     ```
     dig @one of the NS records of your parent zone -t NS example.com
     ```

     Par exemple :

     ```
     dig @b.gtld-servers.net. -t NS example.com
     ```

   - Registre NS dans la zone : il s'agit du registre NS de votre zone. Pour le trouver, exécutez la commande Unix suivante :

     ```
     dig @one of the NS records of your zone -t NS example.com
     ```

     Par exemple :

     ```
     dig @ns-0000.awsdns-00.co.uk. -t NS example.com
     ```

     Notez la TTL maximale pour les deux zones.

4. Supprimez le registre DS de la zone parent.

   Contactez le propriétaire de la zone parent pour supprimer le registre DS.

   Restauration : réinsérez l'enregistrement DS, vérifiez que l'insertion de DS est effective et attendez la TTL NS (et non DS) maximale avant que tous les résolveurs recommencent la validation.

5. Vérifiez que la suppression de DS est effective.

Si la zone parent est sur le service DNS Route 53, le propriétaire de la zone parent peut confirmer la propagation complète via l'GetChangeAPI.

Sinon, vous pouvez rechercher périodiquement le registre DS dans la zone parent, puis attendre ensuite 10 minutes de plus pour augmenter la probabilité de propagation complète de la suppression du registre DS. Notez que certains bureaux d'enregistrement ont planifié la suppression de DS, par exemple une fois par jour.

6. Attendez la TTL DS.

   Attendez que tous les résolveurs aient expiré le registre DS de leurs caches.

7. Désactivez la signature DNSSEC et la clé de signature de clé (KSK).

   - INTERFACE DE LIGNE DE COMMANDE (CLI)
   - Console

   CLI

   Appelez DisableHostedZoneDNSSEC et. DeactivateKeySigningKey APIs

   Par exemple :

```
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

   Pour désactiver la signature DNSSEC

   1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
   2. Dans le panneau de navigation, choisissez Hosted zones (Zones hébergées), puis choisissez une zone hébergée pour laquelle vous souhaitez désactiver la signature DNSSEC.

3. Dans l'onglet DNSSEC signing (Signature DNSSEC), choisissez Disable DNSSEC signing (Désactiver la signature DNSSEC).
4. Sur la page Disable DNSSEC signing (Désactiver la signature DNSSEC), choisissez l'une des options suivantes, selon votre scénario pour la zone pour laquelle vous désactivez la signature DNSSEC.
   - Parent zone only (Zone parent uniquement) : cette zone comporte une zone parent avec un registre DS. Dans ce scénario, vous devez supprimer le registre DS de la zone parent.
   - Child zones only (Zones enfants uniquement) : cette zone comporte un registre DS pour une chaîne d'approbation avec une ou plusieurs zones enfants. Dans ce scénario, vous devez supprimer les registres DS de la zone.
   - Parent and child zones (Zones parent et enfants) : cette zone comporte à la fois un registre DS pour une chaîne d'approbation avec une ou plusieurs zones enfants et une zone parent avec un registre DS. Dans ce scénario, procédez comme suit, dans l'ordre :
     a. Supprimez les registres DS de la zone.
     b. Supprimez le registre DS de la zone parent.

     Si vous disposez d'une île d'approbation, vous pouvez ignorer cette étape.
5. Déterminez la TTL pour chaque registre DS que vous supprimez à l'étape 4. Assurez-vous que la période TTL la plus longue a expiré.
6. Cochez cette case pour confirmer que vous avez effectué les étapes dans l'ordre indiqué.
7. Saisissez disable dans le champ, comme illustré, puis choisissez Disable (Désactiver).

Pour désactiver la clé de signature de clé (KSK)

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le panneau de navigation, choisissez Hosted zones (Zones hébergées), puis choisissez une zone hébergée pour laquelle vous souhaitez désactiver la la clé de signature de clé (KSK).
3. Dans la section Clés de signature par clé (KSKs), choisissez le KSK que vous souhaitez désactiver, puis sous Actions, choisissez Modifier le KSK, définissez le statut du KSK sur Inactif, puis sélectionnez Enregistrer le KSK.

Annulation : appel ActivateKeySigningKeyet EnableHostedZone APIsDNSSEC.

Par exemple :

```
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. Confirmez que la désactivation de la signature de la zone est effective.

   Utilisez l'identifiant de l'`EnableHostedZoneDNSSEC()`appel pour exécuter GetChangeafin de vous assurer que tous les serveurs DNS Route 53 ont cessé de signer les réponses (status `=INSYNC`).

9. Observez la résolution des noms.

   Vous devez observer qu'aucun problème n'entraîne la validation de votre zone par les résolveurs. Prévoyez 1 à 2 semaines pour prendre en compte le temps nécessaire à vos clients pour vous signaler les problèmes.

10. (Facultatif) Nettoyez.

    Si vous ne réactivez pas la signature, vous pouvez effectuer le nettoyage DeleteKeySigningKeyet supprimer la clé gérée KSKs par le client correspondante afin de réduire les coûts.

Utilisation des clés gérées par le client pour DNSSEC

Lorsque vous activez la signature DNSSEC dans Amazon Route 53, Route 53 crée une clé KSK pour vous. Pour créer un KSK, Route 53 doit utiliser une clé gérée par le client AWS Key Management Service qui prend en charge le protocole DNSSEC. Cette section décrit les détails et les exigences relatifs à la clé gérée par le client à connaître lorsque vous utilisez DNSSEC.

Gardez à l'esprit ce qui suit lorsque vous utilisez les clés gérées par le client pour DNSSEC :

- La clé gérée par le client que vous utilisez avec la signature DNSSEC doit se trouver dans la région USA Est (Virginie du Nord).
- La clé gérée par le client doit être un clé asymétrique gérée par le client dotée d'une spécification de clé ECC_NIST_P256. Ces clés gérées par le client sont uniquement utilisées aux fins de la signature et de la vérification. Pour obtenir de l'aide sur la création d'une clé asymétrique gérée par le client, consultez la section Création de clés asymétriques gérées par le client dans le guide du AWS Key Management Service développeur. Pour obtenir de l'aide pour trouver la configuration cryptographique d'une clé gérée par le client existante, consultez la section Affichage de la configuration cryptographique des clés gérées par le client dans le Guide du AWS Key Management Service développeur.
- Si vous créez vous-même une clé gérée par le client à utiliser avec DNSSEC dans Route 53, vous devez inclure des instructions de politique de clé spécifiques qui confèrent à Route 53 les autorisations requises. Route 53 doit pouvoir accéder à votre clé gérée par le client afin de pouvoir créer une clé KSK pour vous. Pour de plus amples informations, veuillez consulter Autorisations de clé gérées par le client Route 53 requises pour la signature DNSSEC.
- Route 53 peut créer une clé gérée par le client que vous pouvez utiliser AWS KMS pour la signature DNSSEC sans autorisations supplémentaires AWS KMS . Toutefois, vous devez disposer d'autorisations spécifiques si vous souhaitez modifier la clé après sa création. Les autorisations spécifiques dont vous devez disposer sont les suivantes : `kms:UpdateKeyDescription`, `kms:UpdateAlias` et `kms:PutKeyPolicy`.
- Vous devez savoir que des frais distincts s'appliquent pour chaque clé gérée par le client que vous possédez, que vous créiez la clé gérée par le client ou que Route 53 la crée pour vous. Pour en savoir plus, consultez Pricing AWS Key Management Service (Tarification).

Utilisation de clés de signature () KSKs

Lorsque vous activez la signature DNSSEC, Route 53 crée une clé KSK pour vous. Vous pouvez en avoir jusqu'à deux KSKs par zone hébergée dans Route 53. Après avoir activé la signature DNSSEC, vous pouvez ajouter, supprimer ou modifier votre. KSKs

Tenez compte des points suivants lorsque vous travaillez avec votre KSKs :

- Avant de pouvoir supprimer une clé KSK, vous devez modifier la clé KSK pour définir son statut sur Inactive (Inactif).

- Lorsque la signature DNSSEC est activée pour une zone hébergée, Route 53 limite la TTL à une semaine. Si vous définissez une TTL de plus d'une semaine pour les registres dans la zone hébergée, vous n'obtenez pas d'erreur, mais Route 53 applique une TTL d'une semaine.
- Pour éviter une panne de zone et éviter que votre domaine ne devienne indisponible, vous devez rapidement corriger et résoudre les erreurs DNSSEC. Nous vous recommandons vivement de configurer une CloudWatch alarme qui vous avertira chaque fois qu'une `DNSSECInternalFailure` `DNSSECKeySigningKeysNeedingAction` erreur est détectée. Pour de plus amples informations, veuillez consulter Surveillance des zones hébergées à l'aide d'Amazon CloudWatch.
- Les opérations KSK décrites dans cette section vous permettent de faire pivoter celles de KSKs votre zone. Pour plus d'informations et un step-by-step exemple, consultez la section Rotation des clés DNSSEC dans le billet de blog Configuration de la signature et de la validation DNSSEC avec Amazon Route 53.

Pour travailler avec KSKs dans le AWS Management Console, suivez les instructions des sections suivantes.

Ajout d'une clé KSK

Lorsque vous activez la signature DNSSEC, Route 53 crée une clé KSK pour vous. Vous pouvez également les ajouter KSKs séparément. Vous pouvez en avoir jusqu'à deux KSKs par zone hébergée dans Route 53.

Lorsque vous créez un KSK, vous devez fournir ou demander à Route 53 de créer une clé gérée par le client à utiliser avec le KSK. Lorsque vous fournissez ou créez une clé gérée par le client, plusieurs exigences s'appliquent. Pour de plus amples informations, veuillez consulter Utilisation des clés gérées par le client pour DNSSEC.

Procédez comme suit pour ajouter une clé KSK dans la AWS Management Console.

Pour ajouter une clé KSK

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le panneau de navigation, choisissez Hosted zones (Zones hébergées), puis choisissez une zone hébergée.
3. Dans l'onglet Signature DNSSEC, sous Clés de signature par clé (KSKs), choisissez Passer à l'affichage avancé, puis, sous Actions, choisissez Ajouter un KSK.

4. Sous KSK (Clé KSK), saisissez un nom pour la clé KSK que Route 53 créera pour vous. Le nom peut contenir des chiffres, des lettres et des traits de soulignement (_). Il doit être unique.
5. Entrez l'alias d'une clé gérée par le client qui s'applique à la signature DNSSEC, ou entrez un alias pour une nouvelle clé gérée par le client que Route 53 créera pour vous.

> **Note**
>
> Si vous choisissez que Route 53 crée une clé gérée par le client, sachez que des frais distincts s'appliquent pour chaque clé gérée par le client. Pour en savoir plus, consultez Pricing AWS Key Management Service (Tarification).

6. Choisissez Create KSK(Créer une clé KSK).

Modification d'une clé KSK

Vous pouvez modifier le statut d'une clé KSK sur Active (Actif) ou Inactive (Inactif). Lorsqu'une clé KSK est active, Route 53 l'utilise aux fins de la signature DNSSEC. Avant de pouvoir supprimer une clé KSK, vous devez modifier la clé KSK pour définir son statut sur Inactive (Inactif).

Procédez comme suit pour modifier une clé KSK dans la AWS Management Console.

Pour modifier une clé KSK

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le panneau de navigation, choisissez Hosted zones (Zones hébergées), puis choisissez une zone hébergée.
3. Dans l'onglet Signature DNSSEC, sous Clés de signature par clé (KSKs), choisissez Passer à l'affichage avancé, puis, sous Actions, choisissez Modifier le KSK.
4. Effectuez les mises à jour souhaitées sur la clé KSK, puis choisissez Save (Enregistrer).

Suppression d'une clé KSK

Avant de pouvoir supprimer une clé KSK, vous devez modifier la clé KSK pour définir son statut sur Inactive (Inactif).

Vous pouvez supprimer une clé KSK aux fins de la routine de rotation des clés. Il est recommandé de périodiquement effectuer la rotation des clés de chiffrement. Votre organisation peut disposer d'instructions standard concernant la fréquence de rotation des clés.

Procédez comme suit pour supprimer une clé KSK dans la AWS Management Console.

Pour supprimer une clé KSK

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le panneau de navigation, choisissez Hosted zones (Zones hébergées), puis choisissez une zone hébergée.
3. Dans l'onglet Signature DNSSEC, sous Clés de signature par clé (KSKs), choisissez Passer à l'affichage avancé, puis sous Actions, choisissez Supprimer le KSK.
4. Suivez les instructions pour confirmer la suppression de la clé KSK.

Gestion des clés KMS et ZSK dans Route 53

Cette section décrit la pratique actuelle utilisée par Route 53 pour vos zones activées de signature DNSSEC.

> **Note**
>
> Route 53 utilise la règle suivante qui peut changer. Tout changement futur ne réduira pas la posture de sécurité de votre zone ou de Route 53.

Comment Route 53 utilise les informations AWS KMS associées à votre KSK

Dans DNSSEC, le KSK est utilisé pour générer la signature d'enregistrement de ressources (RRSIG) pour le jeu d'enregistrements de ressources DNSKEY. Tous `ACTIVE` KSKs sont utilisés dans la génération RRSIG. Route 53 génère un RRSIG en appelant l'`Sign` AWS KMS API sur la clé KMS associée. Pour plus d'informations, consultez Sign (Signer) dans le AWS KMS Guide de l'API. Ils RRSIGs ne sont pas pris en compte dans le calcul de la limite d'enregistrement des ressources de la zone.

RRSIG a une expiration. Pour éviter qu'ils RRSIGs n'expirent, RRSIGs ils sont rafraîchis régulièrement en les régénérant tous les un à sept jours.

Ils RRSIGs sont également actualisés chaque fois que vous appelez l'un des numéros suivants APIs :

- ActivateKeySigningKey
- CreateKeySigningKey
- DeactivateKeySigningKey
- DeleteKeySigningKey
- DisableHostedZoneDNSSEC
- EnableHostedZoneDNSSEC

Chaque fois que Route 53 effectue une actualisation, nous en générons 15 RRSIGs pour couvrir les prochains jours au cas où la clé KMS associée deviendrait inaccessible. Pour l'estimation des coûts des clés KMS, vous pouvez supposer une actualisation régulière une fois par jour. Une clé KMS peut devenir inaccessible en raison de modifications involontaires apportées à la politique de clé KMS. La clé KMS inaccessible définira l'état du KSK associé à `ACTION_NEEDED`. Nous vous recommandons vivement de surveiller cette condition en configurant une CloudWatch alarme chaque fois qu'une `DNSSECKeySigningKeysNeedingAction` erreur est détectée, car la validation des résolveurs commencera à échouer aux recherches après l'expiration du dernier RRSIG. Pour de plus amples informations, veuillez consulter Surveillance des zones hébergées à l'aide d'Amazon CloudWatch.

Comment Route 53 gère la ZSK de votre zone

Chaque nouvelle zone hébergée avec la signature DNSSEC activée aura une `ACTIVE` clé de signature de zone (ZSK). La ZSK est générée séparément pour chaque zone hébergée et appartient à Route 53. L'algorithme clé actuel est ECDSAP256SHA256.

Nous commencerons à effectuer une rotation ZSK régulière sur la zone dans les 7 à 30 jours suivant le début de la signature. Actuellement, Route 53 utilise la méthode Pre-Publish Key Rollover (Renouvellement de la clé de signature de la zone de pré-publication). Pour plus d'informations, veuillez consulterPre-Publish Zone Signing Key Rollover (Renouvellement de la clé de signature de la zone de pré-publication). Cette méthode va introduire un autre ZSK dans la zone. La rotation sera répétée tous les 7 à 30 jours.

La Route 53 suspendra la rotation de la ZSK si l'un des KSK de la zone est en `ACTION_NEEDED` état, car Route 53 ne sera pas en mesure de régénérer les ensembles d'enregistrements de ressources RRSIGs pour DNSKEY afin de tenir compte des modifications apportées au ZSK de la zone. La rotation ZSK reprend automatiquement une fois que la condition est supprimée.

Preuves DNSSEC d'inexistence dans Route 53

> **Note**
>
> Route 53 utilise la règle suivante qui peut changer. Tout changement futur ne réduira pas la posture de sécurité de votre zone ou de Route 53.

Il existe trois types de preuves d'inexistence dans DNSSEC :

- Preuve d'inexistence d'un registre correspondant au nom de la requête.
- Preuve d'inexistence d'un type correspondant au type de la requête.
- Preuve d'existence d'un registre joker utilisé pour générer le registre en réponse.

Route 53 implémente la preuve d'inexistence d'un registre correspondant au nom de la requête à l'aide de la méthode BL. Pour plus d'informations, consultez BL. C'est une méthode qui produit une représentation compacte de la preuve et empêche la marche en zone.

Dans les cas où un enregistrement correspond au nom de la requête mais pas au type de requête (par exemple pour une requête pour web.example). com/AAAA but there is only web.example.com/ Apresent), nous renvoyons un enregistrement NSEC (next secure) minimal contenant tous les types d'enregistrements de ressources pris en charge.

Lorsque Route 53 synthétise une réponse à partir d'un registre joker, la réponse n'est pas accompagnée d'un enregistrement sécurisé suivant, ou d'un registre NSEC pour le caractère générique. Un tel registre NSEC est utilisé dans certaines implémentations, généralement celles effectuant une signature hors ligne, pour empêcher la réutilisation des signatures d'enregistrement de ressources (RRSIG) de la réponse pour usurper une réponse différente. Route 53 utilise la signature en ligne pour les enregistrements non DNSKey afin de générer des informations RRSIGs spécifiques à la réponse qui ne peuvent pas être réutilisées pour une autre réponse.

Résolution des problèmes de signature DNSSEC

Les informations contenues dans cette section peuvent vous aider à résoudre les problèmes liés à la signature DNSSEC, notamment à l'activation, à la désactivation et à vos clés de signature par clé (). KSKs

Activation de la signature DNSSEC

Assurez-vous d'avoir lu les prérequis dans Configuration de la signature DNSSEC dans Amazon Route 53 avant de commencer activer la signature DNSSEC.

Désactivation de la signature DNSSEC

Afin de désactiver la signature DNSSEC en toute sécurité, Route 53 vérifiera si la zone cible se trouve dans la chaîne d'approbation. Il vérifie si le parent de la zone cible possède des enregistrements NS de la zone cible et des enregistrements DS de la zone cible. Si la zone cible ne peut pas être résolue publiquement, par exemple si vous recevez une réponse SERVFAIL lors d'une requête pour NS et DS, Route 53 ne peut pas déterminer s'il est prudent de désactiver la signature DNSSEC. Vous pouvez contacter votre zone parent pour résoudre ces problèmes et réessayer de désactiver la signature DNSSEC ultérieurement.

Le statut de la clé KSK est Action needed (Action requise)

Un KSK peut changer son statut en Action nécessaire (ou `ACTION_NEEDED` en KeySigningKeystatut), lorsque Route 53 DNSSEC perd l'accès à un correspondant AWS KMS key (en raison d'une modification des autorisations ou AWS KMS key d'une suppression).

Si le statut d'un KSK est Action needed (Action requise), cela signifie qu'il finira par provoquer une panne de zone pour les clients utilisant des résolveurs de validation DNSSEC et que vous devez agir rapidement pour éviter qu'une zone de production ne devienne impossible à résoudre.

Pour corriger le problème, assurez-vous que la clé gérée par le client sur laquelle votre clé KSK est basée est activée et qu'elle dispose des autorisations appropriées. Pour plus d'informations sur les autorisations requises, consultez Autorisations de clé gérées par le client Route 53 requises pour la signature DNSSEC.

Après avoir corrigé le KSK, réactivez-le à l'aide de la console ou du AWS CLI, comme décrit dansÉtape 2 : Activer la signature DNSSEC et créer une clé KSK.

Pour éviter que ce problème ne se reproduise à l'avenir, pensez à ajouter une Amazon CloudWatch métrique pour suivre l'état du KSK, comme suggéré dansConfiguration de la signature DNSSEC dans Amazon Route 53.

Le statut de la clé KSK est Internal failure (Échec interne)

Lorsqu'un KSK présente un état de défaillance interne (ou `INTERNAL_FAILURE` un KeySigningKeyétat), vous ne pouvez pas travailler avec d'autres entités DNSSEC tant que le

problème n'est pas résolu. Vous devez prendre des mesures avant de pouvoir utiliser la signature DNSSEC, y compris avant d'utiliser cette clé KSK ou votre autre clé KSK.

Pour corriger le problème, essayez à nouveau d'activer ou de désactiver la clé KSK.

Pour corriger le problème lorsque vous travaillez avec le APIs, essayez d'activer la signature (EnableHostedZoneDNSSEC) ou de désactiver la signature (DisableHostedZoneDNSSEC).

Il est important que vous corrigiez rapidement les problèmes Internal failure (Échec interne). Vous ne pouvez pas apporter d'autres modifications à la zone hébergée tant que vous n'avez pas corrigé le problème, à l'exception des opérations visant à résoudre le problème Internal failure (Échec interne).

Utilisation AWS Cloud Map pour créer des dossiers et des bilans de santé

Si vous souhaitez acheminer le trafic Internet ou le trafic interne d'un VPC Amazon vers des composants d'application ou des microservices, vous pouvez utiliser AWS Cloud Map pour créer automatiquement des registres et, éventuellement, des surveillances d'états. Pour plus d'informations, consultez le Manuel du développeur AWS Cloud Map.

Contraintes et comportements DNS

La messagerie DNS est soumise à des facteurs qui ont une influence sur la façon dont vous créez et utilisez les zones hébergées et les enregistrements. Cette section explique ces facteurs.

Taille de réponse maximale

Pour respecter les normes DNS, la taille des réponses envoyées via UDP est limitée à 512 octets. Les réponses qui dépassent 512 octets sont tronquées et le résolveur doit émettre à nouveau la demande via TCP. Si le résolveur prend en charge EDNS0 (comme défini dans RFC 2671) et informe Amazon Route 53 de l'option EDNS0, Route 53 autorise les réponses d'une taille maximale de 4 096 octets via UDP, sans troncature.

Traitement de la section relative à l'autorité

Pour les requêtes réussies, Route 53 ajoute les registres de serveur de noms (NS) de la zone hébergée appropriée à la section Authority (Autorité) de la réponse DNS. Pour les noms introuvables

(réponses NXDOMAIN), Route 53 ajoute le registre de source de noms (SOA) (comme défini dans RFC 1035) de la zone hébergée appropriée à la section Authority (Autorité) de la réponse DNS.

Traitement de la section supplémentaire

Route 53 ajoute des registres à la section Additional (Supplémentaire). Si les enregistrements sont connus et appropriés, le service ajoute des enregistrements A ou AAAA à toutes les cibles d'un enregistrement MX, CNAME, NS ou SRV cité dans la section relative à la réponse. Pour obtenir plus d'informations sur ces types d'enregistrements DNS, consultez Types d'enregistrements DNS pris en charge.

Utiliser Traffic Flow pour acheminer le trafic DNS

Traffic Flow simplifie considérablement le processus de création et de gestion des enregistrements dans des configurations complexes et volumineuses.

La gestion des enregistrements connexes dans une zone hébergée peut s'avérer difficile dans les circonstances suivantes :

- Vous disposez de nombreuses ressources qui effectuent la même opération, telles que des serveurs Web qui gèrent le trafic pour le même domaine.
- Vous souhaitez créer une arborescence complexe d'enregistrements à l'aide d'enregistrements d'alias et d'une combinaison de stratégies de routage Route 53, telles que la latence, le basculement et la pondération.

Avantages de Traffic Flow

Pour faciliter le suivi des enregistrements et de leurs relations, Traffic Flow simplifie la création d'enregistrements DNS grâce aux fonctionnalités suivantes :

Visual editor (Éditeur visuel)

L'éditeur visuel Traffic Flow vous permet de créer des arborescences complexes d'enregistrements et de voir les relations entre les enregistrements. Par exemple, vous pouvez créer une configuration où les enregistrements d'alias de latence font référence aux enregistrements pondérés, et où les enregistrements pondérés font référence à vos ressources dans plusieurs Régions AWS. Chaque configuration est connue sous le nom de stratégie de trafic. Vous pouvez créer autant de stratégies de trafic que vous le souhaitez sans frais supplémentaires.

Gestion des versions

Vous pouvez créer plusieurs versions d'une stratégie de trafic afin de ne pas avoir à tout recommencer lorsque votre configuration change. Les anciennes versions continuent d'exister jusqu'à ce que vous les supprimiez ; la limite par défaut est de 1000 versions par stratégie de trafic. Vous pouvez éventuellement fournir une description pour chaque version.

Création et mise à jour automatiques des enregistrements

Une stratégie de trafic peut représenter des dizaines, voire des centaines d'enregistrements. Traffic Flow vous permet de créer automatiquement tous ces enregistrements en créant un enregistrement de politique de trafic. Vous spécifiez la zone hébergée et le nom de l'enregistrement à la racine de l'arborescence, tel que example.com ou www.example.com, et Route 53 crée automatiquement tous les autres enregistrements de l'arborescence. L'enregistrement racine (enregistrement de stratégie de trafic) apparaît dans la liste des enregistrements de votre zone hébergée ; tous les autres enregistrements sont masqués.

Lorsque vous créez une nouvelle version d'une stratégie de trafic, vous pouvez mettre à jour de manière sélective les enregistrements de stratégie de trafic que vous avez créés à l'aide de la version de stratégie de trafic précédente. Lorsque vous mettez à jour un enregistrement de stratégie de trafic, Route 53 met automatiquement à jour tous les autres enregistrements de l'arborescence. Vous pouvez également annuler rapidement les modifications en mettant à nouveau à jour un enregistrement de stratégie de trafic de manière à utiliser une version de stratégie de trafic précédente.

> **Note**
>
> Vous pouvez utiliser Traffic Flow pour créer des enregistrements uniquement dans les zones hébergées publiques.

Stratégie de routage par proximité géographique

Lorsque vous utilisez Traffic Flow, vous pouvez comprendre de manière plus intuitive comment le trafic est acheminé vers chacun de vos points de terminaison globaux en utilisant la carte de géoproximité de l'éditeur visuel Traffic Flow. Pour de plus amples informations, veuillez consulter Routage par géoproximité.

Réutilisation pour plusieurs enregistrements dans différentes zones hébergées

Vous pouvez utiliser une stratégie de trafic pour créer automatiquement des enregistrements dans plusieurs zones hébergées publiques. Par exemple, si vous utilisez les mêmes serveurs Web pour plusieurs noms de domaine, vous pouvez utiliser la même stratégie de trafic pour créer des enregistrements de stratégie de trafic dans les zones hébergées pour example.com, example.org et example.net.

Lorsqu'un client soumet une requête pour le nom de l'enregistrement racine, tel que example.com ou www.example.com, Route 53 répond à la requête en fonction de la configuration de la stratégie de trafic utilisée pour créer l'enregistrement de stratégie de trafic correspondant.

Des frais mensuels sont facturés pour chaque enregistrement de stratégie de trafic. Pour de plus amples informations, veuillez consulter la section « Flux de trafic » de Tarification d'Amazon Route 53.

Pour réduire ces frais, vous pouvez créer un ou plusieurs enregistrements d'alias dans une zone hébergée qui font référence à un enregistrement de stratégie de trafic dans cette zone hébergée. Par exemple, vous pouvez créer un enregistrement de stratégie de trafic pour example.com, puis créer un enregistrement d'alias pour www.example.com qui fait référence à l'enregistrement de stratégie de trafic.

Création et gestion des stratégies de trafic

Rubriques

- Création d'une stratégie de trafic
- Valeurs à spécifier lors de la création d'une stratégie de trafic
- Affichage d'une carte montrant l'effet des paramètres de proximité géographique
- Création de versions supplémentaires d'une stratégie de trafic
- Création d'une politique de trafic à l'aide d'un document JSON
- Affichage des versions de stratégie de trafic et des enregistrements de stratégie associés
- Suppression de versions de stratégie de trafic et de stratégies de trafic

Création d'une stratégie de trafic

Pour créer une stratégie de trafic, utilisez la procédure suivante.

> **Note**
>
> Nous mettons à jour la console Traffic Flow pour Route 53. Pendant la période de transition, vous pouvez continuer à utiliser l'ancienne console.

Choisissez l'onglet correspondant à la console que vous utilisez.

- Nouvelle console
- Ancienne console

New console

Pour créer une stratégie de trafic

1. Concevez votre configuration. Pour plus d'informations sur le fonctionnement des configurations de routage DNS complexes, consultez la section Configuration du basculement DNS de Création de bilans de santé pour Amazon Route 53 .
2. En fonction de la conception de votre configuration, créez les surveillances de l'état que vous souhaitez utiliser pour vos points de terminaison.
3. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
4. Dans le volet de navigation, choisissez Traffic policies (Stratégies de trafic).
5. Choisissez Create traffic policy (Créer une stratégie de trafic).
6. Entrez un nom et une description facultative, puis choisissez Next.
7. Dans l'éditeur, choisissez le type d'enregistrement de ressource DNS dans le volet Propriétés. Ce type sera attribué à tous les enregistrements de ressources que vous créez pour cette politique de trafic.

   Choisissez Confirmer. Pour de plus amples informations, veuillez consulter Valeurs à spécifier lors de la création d'une stratégie de trafic.
8. Dans la page de l'éditeur, choisissez Connect to, puis choisissez l'une des options suivantes : Nouvelle règle de routage, Nouveau point de terminaison, Règle de routage existante ou Point de terminaison existant. Si vous avez sélectionné une nouvelle règle de routage, dans le volet Propriétés, sélectionnez la règle de routage et choisissez Confirmer. Ensuite, dans le volet Propriétés, entrez les valeurs appropriées. Répétez ce processus jusqu'à ce que votre politique soit terminée. Pour plus d'informations sur les valeurs de chaque type de connexion, consultezValeurs à spécifier lors de la création d'une stratégie de trafic.

   Vous pouvez supprimer des règles, des points de terminaison et des branches d'une stratégie de trafic de différentes manières :

   - Pour supprimer une règle ou un point de terminaison, sélectionnez la règle ou le point de terminaison dans l'éditeur, puis choisissez Supprimer dans le volet Propriétés.

> **Important**
>
> Si vous supprimez une règle comportant des points de terminaison et des règles enfant, Amazon Route 53 supprime également tous les enfants.

- Si vous connectez deux règles à la même règle enfant ou point de terminaison et que vous souhaitez supprimer l'une des connexions, sélectionnez la connexion que vous souhaitez supprimer, puis cliquez sur Supprimer dans le volet Propriétés pour cette connexion.

9. Choisissez Create Policy (Créer une politique).
10. Sur la page Créer des enregistrements de politique, utilisez la nouvelle politique de trafic pour créer un ou plusieurs enregistrements de politique dans une zone hébergée. Pour de plus amples informations, veuillez consulter Valeurs à spécifier lors de la création ou de la mise à jour d'un enregistrement de stratégie. Vous pouvez également créer des enregistrements de stratégies ultérieurement, soit dans la même zone hébergée ou dans d'autres zones hébergées.

    Si vous ne souhaitez pas créer d'enregistrements de politique maintenant, choisissez Annuler, et la console affiche la liste des politiques de trafic et des enregistrements de politique que vous avez créés à l'aide du AWS compte actuel.
11. Si vous avez défini des paramètres pour les enregistrements de stratégie à l'étape précédente, choisissez Create policy records.

Old console

Pour créer une stratégie de trafic

1. Concevez votre configuration. Pour plus d'informations sur le fonctionnement des configurations de routage DNS complexes, consultez la section Configuration du basculement DNS de Création de bilans de santé pour Amazon Route 53 .
2. En fonction de la conception de votre configuration, créez les surveillances de l'état que vous souhaitez utiliser pour vos points de terminaison.
3. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
4. Dans le volet de navigation, choisissez Traffic policies (Stratégies de trafic).
5. Choisissez Create traffic policy (Créer une stratégie de trafic).

6. Sur la page Name policy (Nommer la stratégie), spécifiez les valeurs applicables. Pour de plus amples informations, veuillez consulter Valeurs à spécifier lors de la création d'une stratégie de trafic.
7. Choisissez Next (Suivant).
8. Sur la page Create traffic policy (Créer une stratégie de trafic) policy name (nom de la stratégie) v1, spécifiez les valeurs applicables. Pour de plus amples informations, veuillez consulter Valeurs à spécifier lors de la création d'une stratégie de trafic.

   Vous pouvez supprimer des règles, des points de terminaison et des branches d'une stratégie de trafic de différentes manières :

   - Pour supprimer une règle ou un point de terminaison, cliquez sur x dans le coin supérieur droit de la zone.

     > **Important**
     >
     > Si vous supprimez une règle comportant des points de terminaison et des règles enfant, Amazon Route 53 supprime également tous les enfants.

   - Si vous connectez deux règles à même point de terminaison ou à la même règle enfant et que vous souhaitez supprimer l'une des connexions, placez votre curseur sur la connexion à supprimer, puis cliquez sur le x correspondant à cette connexion.
9. Choisissez Create traffic policy (Créer une stratégie de trafic).
10. Facultatif : sur la page Create policy records with traffic policy (Créer des enregistrements de stratégie avec une stratégie de trafic), utilisez la nouvelle stratégie de trafic pour créer un ou plusieurs enregistrements dans une zone hébergée. Pour de plus amples informations, veuillez consulter Valeurs à spécifier lors de la création ou de la mise à jour d'un enregistrement de stratégie. Vous pouvez également créer des enregistrements de stratégies ultérieurement, soit dans la même zone hébergée ou dans d'autres zones hébergées.

    Si vous ne souhaitez pas créer d'enregistrements de politique maintenant, choisissez Ignorer cette étape, et la console affiche la liste des politiques de trafic et des enregistrements de politique que vous avez créés à l'aide du AWS compte actuel.
11. Si vous avez spécifié des paramètres pour les enregistrements de stratégie à l'étape précédente, choisissez Create policy record (Créer un enregistrement de stratégie).

Valeurs à spécifier lors de la création d'une stratégie de trafic

> **Note**
>
> Nous mettons à jour la console Traffic Flow pour Route 53. Pendant la période de transition, vous pouvez continuer à utiliser l'ancienne console. La liste suivante s'applique aux deux consoles, sauf indication contraire.

Lorsque vous créez une stratégie de trafic, vous spécifiez les valeurs suivantes.

-
-
-
-
-
-
-
-

Nom de la politique

Entrez un nom qui décrit la stratégie de trafic. Cette valeur s'affiche dans la liste des stratégies de trafic dans la console. Vous ne pouvez pas modifier le nom d'une stratégie de trafic après l'avoir créée.

Version

Cette valeur est automatiquement attribuée par Amazon Route 53 lorsque vous créez une stratégie de trafic ou une nouvelle version d'une stratégie existante.

Version description

Entrez une description qui s'applique à cette version de stratégie de trafic. Cette valeur s'affiche dans la liste des versions de stratégies de trafic dans la console.

Type DNS

Choisissez le type DNS que vous souhaitez qu'Amazon Route 53 attribue à tous les enregistrements lorsque vous créez un enregistrement de stratégie à l'aide de cette version de la stratégie de trafic. Pour obtenir une liste des types pris en charge, consultez Types d'enregistrements DNS pris en charge.

> **Important**
>
> Si vous créez une nouvelle version d'une stratégie de trafic existante, vous pouvez modifier le type DNS. Cependant, vous ne pouvez pas modifier un enregistrement de stratégie et choisir une version de stratégie de trafic dont le type DNS est différent de la version de stratégie de trafic utilisée pour créer l'enregistrement de stratégie. Par exemple, si vous avez créé un enregistrement de stratégie à l'aide d'une version de stratégie de trafic dont la valeur de DNS type est A, vous ne pouvez pas modifier l'enregistrement de stratégie et choisir une version de stratégie de trafic dont la valeur de DNS type n'est pas A.

Si vous souhaitez acheminer le trafic vers les AWS ressources suivantes, choisissez la valeur applicable :

- CloudFront distribution — Choisissez A : adresse IP au IPv4 format ou AAAA : adresse IP au IPv6 format.

  > **Note**
  >
  > CloudFront les points de terminaison alias ne prennent pas en charge l'évaluation de l'état de santé. Vous pouvez toutefois créer un bilan de santé pour surveiller les CloudFront terminaux. Pour de plus amples informations, veuillez consulter Création et mise à jour de surveillances de l'état.

- Équilibreur de charge d'application ELB — Choisissez soit A : adresse IP au IPv4 format, soit AAAA : adresse IP au format. IPv6
- Équilibreur de charge ELB Classic — Choisissez soit A : adresse IP au IPv4 format, soit AAAA : adresse IP au format. IPv6
- Équilibreur de charge réseau ELB — Choisissez soit A : adresse IP au IPv4 format, soit AAAA : adresse IP au format. IPv6
- Environnement Elastic Beanstalk : choisissez l'adresse IP A : dans le format. IPv4

- Compartiment Amazon S3 configuré en tant que point de terminaison de site Web : Choisissez A : adresse IP au IPv4 format.

Se connecter à

Choisissez la règle applicable ou le point de terminaison en fonction de la conception de votre configuration.

Règle de basculement

Choisissez cette option lorsque vous souhaitez configurer un basculement actif-passif, dans lequel une ressource se charge de l'ensemble du trafic lorsqu'elle est disponible et l'autre ressource se charge de l'ensemble du trafic lorsque la première ressource n'est pas disponible.

Pour de plus amples informations, veuillez consulter Basculement actif-passif.

> **Note**
>
> L'option Évaluer l'état de santé de la cible est cochée par défaut et elle évaluera l'état du point de terminaison cible vers lequel le trafic est acheminé via un enregistrement d'alias. Si votre terminal ne reçoit pas de trafic DNS via un enregistrement d'alias, décochez cette case et créez un bilan de santé si vous souhaitez surveiller l'état du terminal. Pour de plus amples informations, veuillez consulter Création et mise à jour de surveillances de l'état.

Règle de géolocalisation

Choisissez cette option lorsque vous souhaitez qu'Amazon Route 53 réponde aux requêtes DNS en fonction de l'emplacement de vos utilisateurs.

Pour de plus amples informations, veuillez consulter Routage de géolocalisation.

Lorsque vous choisissez la règle de géolocalisation, vous pouvez également sélectionner le pays ou l'État des États-Unis d'où proviennent les requêtes.

> **Note**
>
> L'option Évaluer l'état de santé de la cible est cochée par défaut et elle évaluera l'état du point de terminaison cible vers lequel le trafic est acheminé via un enregistrement d'alias.

Si votre terminal ne reçoit pas de trafic DNS via un enregistrement d'alias, décochez cette case et créez un bilan de santé si vous souhaitez surveiller l'état du terminal. Pour de plus amples informations, veuillez consulter Création et mise à jour de surveillances de l'état.

Règle de latence

Choisissez cette option lorsque vous disposez de ressources dans plusieurs centres de EC2 données Amazon qui exécutent la même fonction et que vous souhaitez que Route 53 réponde aux requêtes DNS avec les ressources offrant la meilleure latence.

Lorsque vous choisissez la règle de latence, vous choisissez également une Région AWS.

Pour de plus amples informations, veuillez consulter Routage basé sur la latence.

> **Note**
>
> L'option Évaluer l'état de santé de la cible est cochée par défaut et elle évaluera l'état du point de terminaison cible vers lequel le trafic est acheminé via un enregistrement d'alias. Si votre terminal ne reçoit pas de trafic DNS via un enregistrement d'alias, décochez cette case et créez un bilan de santé si vous souhaitez surveiller l'état du terminal. Pour de plus amples informations, veuillez consulter Création et mise à jour de surveillances de l'état.

Règle de proximité géographique

Choisissez cette option lorsque vous souhaitez que Route 53 réponde aux requêtes DNS en fonction de l'emplacement de vos ressources et, éventuellement, d'une valeur d'écart que vous spécifiez. Cette valeur d'écart vous permet de diriger davantage de trafic vers une ressource, ou au contraire de détourner le trafic d'une ressource.

Lorsque vous choisissez la règle de proximité géographique, saisissez les valeurs suivantes :

Emplacement du point de terminaison

Choisissez la valeur applicable :

- Personnalisé (entrez les coordonnées) — Si votre point de terminaison n'est pas une AWS ressource, choisissez Personnalisé (entrez les coordonnées).
- An Région AWS — Si votre point de terminaison est une AWS ressource, choisissez Région AWS celle dans laquelle vous avez créé la ressource.

- Une zone AWS locale : si votre point de terminaison est une AWS ressource, choisissez la zone AWS locale dans laquelle vous avez créé la ressource.

Si vous utilisez des Zones AWS Locales, vous devez d'abord les activer. Pour plus d'informations, consultez Premiers pas avec les zones locales dans le Guide de l'utilisateur des zones locales AWS .

Pour connaître les zones locales disponibles, consultez la section Emplacements des zones locales AWS.

Pour en savoir plus sur la différence entre les zones Régions AWS et les zones locales, consultez Régions et zones dans le guide de EC2 l'utilisateur Amazon.

> **Important**
>
> Une seule politique de routage par proximité géographique ne peut pas contenir deux emplacements ou plus situés géographiquement dans la même zone métropolitaine. En outre, certaines Régions AWS Zones Locales, telles que USA West (Oregon) et Portland, États-Unis, sont situées trop près les unes des autres pour être utilisées dans le cadre de la même politique de routage par géoproximité. Si vous avez besoin d'acheminer du trafic vers plusieurs emplacements dans la même zone métropolitaine, définissez plutôt une politique de routage par proximité géographique qui aboutit à une règle de routage pondéré (WRR) 50/50 pour deux points de terminaison différents de la zone, répartissant ainsi le trafic de manière égale entre ces points de terminaison.

Coordinates

Si vous avez choisi Personnalisé (entrer des coordonnées) pour Emplacement du point de terminaison, saisissez la latitude et la longitude de l'emplacement de la ressource. Remarques :

- La latitude représente la position au sud (valeur négative) ou au nord (valeur positive) de l'équateur. Les valeurs valides vont de -90 degrés à 90 degrés.
- La longitude représente la position à l'ouest (valeur négative) ou à l'est (valeur positive) du méridien de référence. Les valeurs valides vont de -180 degrés à 180 degrés.
- Pour connaître la latitude et la longitude, vous pouvez avoir recours à diverses applications de cartographie en ligne. Par exemple, dans Google Maps, l'URL d'un emplacement spécifie la latitude et la longitude :

https://www.google.com/maps/@ 47,6086111, - 122,3409953,20 z

- Nous acceptons une précision maximale de deux décimales, par exemple : 47,63. Si vous indiquez une valeur avec une plus grande précision, Route 53 tronque cette valeur en conservant deux chiffres après la virgule. Pour la latitude et la longitude au niveau de l'équateur, 0,01 degré correspond à environ 0,69 miles (1,11 km).

Écart

(Facultatif) Pour modifier la taille de la région géographique à partir de laquelle Route 53 achemine le trafic vers une ressource, spécifiez la valeur applicable pour l'écart :

- Pour étendre la taille de la région géographique à partir de laquelle Route 53 achemine le trafic vers une ressource, spécifiez un nombre entier positif compris entre 1 et 99 en tant que valeur d'écart. Route 53 diminue la taille des régions adjacentes.
- Pour réduire la taille de la région géographique à partir de laquelle Route 53 achemine le trafic vers une ressource, spécifiez une valeur d'écart négative comprise entre -1 et -99. Route 53 étend la taille des régions adjacentes.

> **Important**
>
> L'effet de la modification de la valeur de l'écart est relatif (basé sur l'emplacement des autres ressources), plutôt qu'absolu (basé sur la distance). En conséquence, l'impact des modifications est difficile à prévoir. Par exemple, selon l'emplacement de vos ressources, passer d'une valeur d'écart de 10 à 15 peut entraîner l'ajout ou le retrait d'un gros volume de trafic en provenance de l'agglomération de New York. Nous vous conseillons donc de modifier la valeur d'écart par petits incréments et d'évaluer les résultats avant de procéder à des changements supplémentaires, si nécessaire.

Pour de plus amples informations, veuillez consulter Routage par géoproximité.

> **Note**
>
> L'option Évaluer l'état de santé de la cible est cochée par défaut et elle évaluera l'état du point de terminaison cible vers lequel le trafic est acheminé via un enregistrement d'alias. Si votre terminal ne reçoit pas de trafic DNS via un enregistrement d'alias, décochez cette case et créez un bilan de santé si vous souhaitez surveiller l'état du terminal. Pour de plus amples informations, veuillez consulter Création et mise à jour de surveillances de l'état.

Règle de réponse multivaleur

Choisissez cette option lorsque vous souhaitez que Route 53 réponde aux requêtes DNS avec jusqu'à huit réponses saines sélectionnées approximativement de manière aléatoire.

Pour de plus amples informations, veuillez consulter Multivalue answer routing (Routage de réponse multivaleur).

> **Note**
>
> L'option Évaluer l'état de santé de la cible est cochée par défaut et elle évaluera l'état du point de terminaison cible vers lequel le trafic est acheminé via un enregistrement d'alias. Si votre terminal ne reçoit pas de trafic DNS via un enregistrement d'alias, décochez cette case et créez un bilan de santé si vous souhaitez surveiller l'état du terminal. Pour de plus amples informations, veuillez consulter Création et mise à jour de surveillances de l'état.

Règle pondérée

Choisissez cette option lorsque vous disposez de plusieurs ressources qui exécutent la même fonction (par exemple, des serveurs web qui servent le même site web) et que vous voulez que Route 53 achemine le trafic vers ces ressources dans la proportion que vous spécifiez (par exemple, 1/3 vers un serveur et 2/3 vers l'autre).

Lorsque vous choisissez Weighted rule (Règle pondérée), saisissez la pondération que vous souhaitez appliquer à cette règle.

Pour de plus amples informations, veuillez consulter Weighted routing (Routage pondéré).

> **Note**
>
> L'option Évaluer l'état de santé de la cible est cochée par défaut et elle évaluera l'état du point de terminaison cible vers lequel le trafic est acheminé via un enregistrement d'alias. Si votre terminal ne reçoit pas de trafic DNS via un enregistrement d'alias, décochez cette case et créez un bilan de santé si vous souhaitez surveiller l'état du terminal. Pour de plus amples informations, veuillez consulter Création et mise à jour de surveillances de l'état.

Point de terminaison

Choisissez cette option pour spécifier la ressource, telle qu'une CloudFront distribution ou un équilibreur de charge Elastic Load Balancing, vers laquelle vous souhaitez acheminer les requêtes DNS.

Règle existante

Choisissez cette option lorsque vous souhaitez acheminer les requêtes DNS vers une règle existante dans cette stratégie de trafic. Par exemple, vous pouvez créer deux ou plusieurs règles de géolocalisation qui acheminent les requêtes de différents pays vers la même règle de basculement. La règle de basculement peut ensuite acheminer les requêtes vers deux équilibreurs de charge Elastic Load Balancing.

Cette option n'est pas disponible si la stratégie de trafic n'inclut pas de règle.

Point de terminaison existant

Choisissez cette option lorsque vous souhaitez acheminer des requêtes DNS vers un point de terminaison existant. Par exemple, si vous disposez de deux règles de basculement, vous pouvez décider d'acheminer les requêtes DNS pour les deux options Sur le basculement (secondaires) vers le même équilibreur de charge Elastic Load Balancing.

Cette option n'est pas disponible si la stratégie de trafic n'inclut pas de point de terminaison.

Type de la valeur

Choisissez l'option applicable :

CloudFront distribution

Choisissez cette option si vous souhaitez acheminer le trafic vers une CloudFront distribution. L'option n'est disponible que si vous avez choisi A : adresse IP au IPv4 format pour le type DNS ou AAAA : adresse IP au IPv6 format pour le type DNS.

> **Note**
>
> CloudFront les points de terminaison alias ne prennent pas en charge l'évaluation de l'état de santé. Vous pouvez toutefois créer un bilan de santé pour surveiller les CloudFront terminaux. Pour de plus amples informations, veuillez consulter Création et mise à jour de surveillances de l'état.

Application Load Balancer ELB

Choisissez cette option si vous souhaitez acheminer le trafic vers un Application Load Balancer Elastic Load Balancing. L'option n'est disponible que si vous avez choisi le IPv4 format A : adresse IP ou AAAA : adresse IP au IPv6 format pour le type DNS.

Classic Load Balancer ELB

Choisissez cette option si vous souhaitez acheminer le trafic vers un Classic Load Balancer Elastic Load Balancing. L'option n'est disponible que si vous avez choisi le IPv4 format A : adresse IP ou AAAA : adresse IP au IPv6 format pour le type DNS.

Network Load Balancer ELB

Choisissez cette option si vous souhaitez acheminer le trafic vers un Network Load Balancer Elastic Load Balancing. L'option n'est disponible que si vous avez choisi le IPv4 format A : adresse IP ou AAAA : adresse IP au IPv6 format pour le type DNS.

Environnement Elastic Beanstalk

Choisissez cette option si vous souhaitez acheminer le trafic vers un environnement Elastic Beanstalk. L'option n'est disponible que si vous avez choisi le IPv4 format A : adresse IP pour le type DNS.

Point de terminaison de site Web S3

Choisissez cette option si vous souhaitez acheminer le trafic vers un compartiment Amazon S3 configuré comme point de terminaison d'un site web. L'option n'est disponible que si vous avez choisi le IPv4 format A : adresse IP pour le type DNS.

Valeur type DNS

Choisissez cette option si vous voulez que Route 53 réponde aux requêtes DNS à l'aide de la valeur du champ Value (Valeur). Par exemple, si vous avez choisi A comme valeur de DNS type (Type DNS) lorsque vous avez créé cette stratégie de trafic, cette option figure dans la liste Value type (Type de valeur) au format Type A value (Valeur de type A). Cela nécessite que vous saisissiez une adresse IP IPv4 au format dans le champ Valeur. Route 53 répond aux requêtes DNS qui sont acheminées vers ce point de terminaison avec l'adresse IP dans Value (Valeur).

Valeur

Choisissez ou entrez une valeur en fonction de l'option que vous avez choisie pour Value type (Type de valeur) :

CloudFront distribution

Choisissez une CloudFront distribution dans la liste des distributions associées au AWS compte courant.

Application Load Balancer ELB

Choisissez un équilibreur de charge de l'application Elastic Load Balancing dans la liste des équilibreurs de charge associés au compte courant AWS .

Classic Load Balancer ELB

Choisissez un équilibreur de charge Elastic Load Balancing Classic dans la liste des équilibreurs de charge associés au compte courant AWS .

Network Load Balancer ELB

Choisissez un équilibreur de charge Elastic Load Balancing Network dans la liste des équilibreurs de charge associés au compte courant AWS .

Environnement Elastic Beanstalk

Choisissez un environnement Elastic Beanstalk dans la liste des environnements associés au Compte AWS actuel.

Point de terminaison de site Web S3

Choisissez un compartiment Amazon S3 dans la liste des compartiments Amazon S3 configurés comme points de terminaison de site Web et associés au compte courant AWS .

> **Important**
>
> Lorsque vous créez un enregistrement de stratégie basé sur cette stratégie de trafic, le compartiment que vous choisissez ici doit correspondre au nom de domaine (par exemple, www.example.com) que vous spécifiez pour Policy record DNS name dans l'enregistrement de stratégie. Si les valeurs de Value (Valeur) et de Policy record DNS name (Nom DNS d'enregistrement de stratégie) ne correspondent pas, Amazon S3 ne répondra pas aux requêtes DNS pour le nom de domaine.

Valeur type DNS

Entrez une valeur correspondant à la valeur spécifiée pour DNS type (Type DNS) lorsque vous avez commencé cette stratégie de trafic. Par exemple, si vous avez choisi MX pour

DNS type (Type DNS), entrez deux valeurs : la priorité que vous souhaitez attribuer à un serveur de messagerie et le nom de domaine du serveur de messagerie, comme `10 sydney.mail.example.com`.

Pour obtenir plus d'informations sur le types DNS pris en charge, consultez Types d'enregistrements DNS pris en charge.

Clé (nouvelle console uniquement)

Entrez un nom convivial pour une règle de routage ou un point de terminaison pour Key. Cette valeur s'affiche sous la forme du nom d'un nœud dans l'éditeur.

Affichage d'une carte montrant l'effet des paramètres de proximité géographique

Une règle de géoproximité vous permet de spécifier les emplacements de vos ressources, à la fois dans des zones locales ou dans Régions AWS des zones locales, et, en utilisant la latitude et la longitude, dans des zones non AWS localisées. Lorsque vous créez une règle de proximité géographique, Route 53 achemine le trafic Internet vers la ressource qui est la plus proche de vos utilisateurs par défaut. Vous pouvez également choisir d'acheminer davantage ou moins de trafic vers une ressource en spécifiant un écart qui augmente ou réduit la zone géographique à partir de laquelle le trafic est acheminé vers une ressource. Pour plus d'informations sur le routage de proximité géographique, consultez Routage par géoproximité.

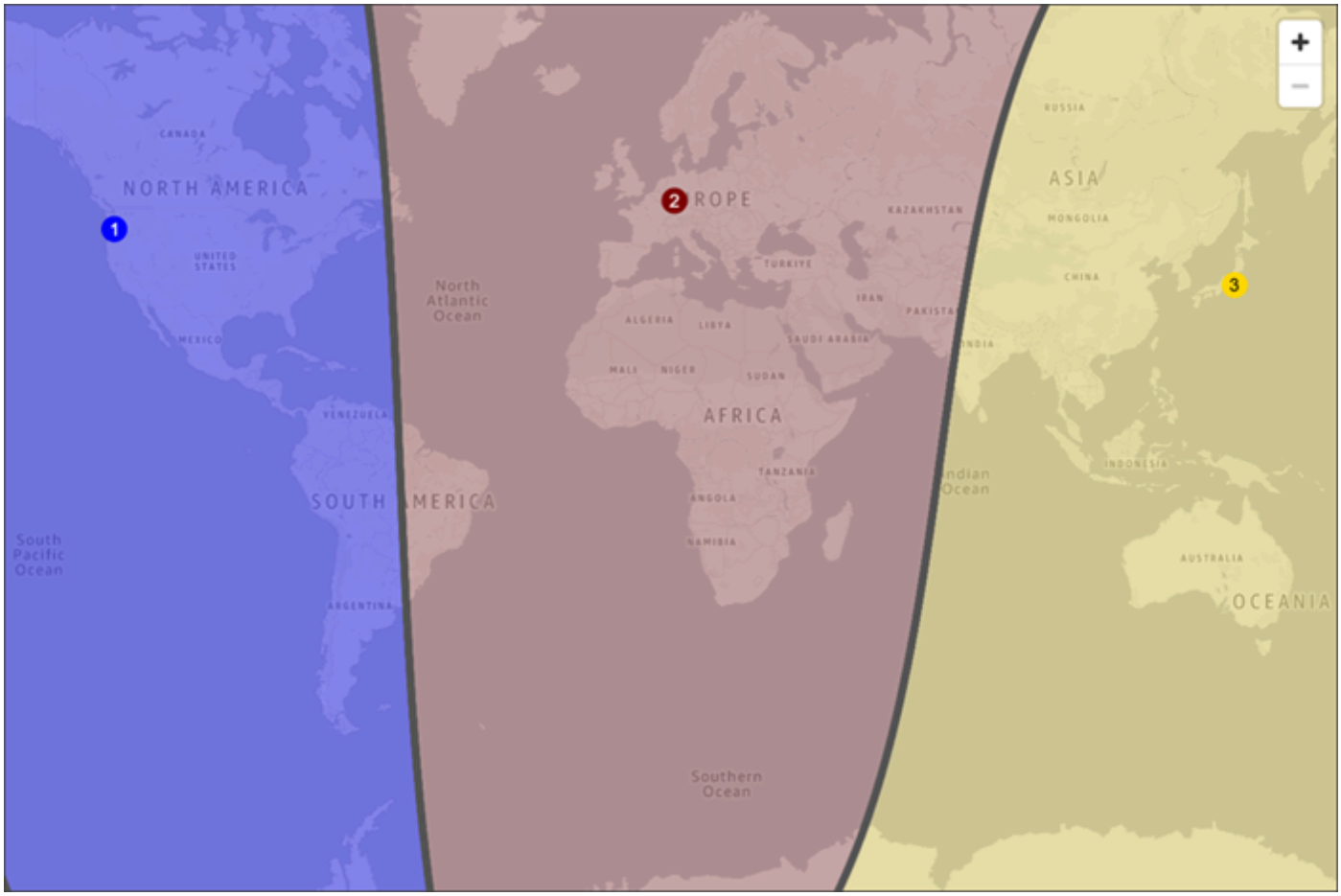
> **Note**
>
> Nous mettons à jour la console Traffic Flow pour Route 53. Pendant la période de transition, vous pouvez continuer à utiliser l'ancienne console.

Choisissez l'onglet correspondant à la console que vous utilisez.

- Nouvelle console
- Ancienne console

New console

Vous pouvez afficher une carte qui montre l'effet de vos paramètres actuels de proximité géographique. Par exemple, si vous avez des ressources dans les régions USA Ouest (Oregon), Europe (Francfort) et Asie-Pacifique (Tokyo), et si vous ne spécifiez pas d'écart, la carte ressemble à ceci.



La carte correspondant à une règle de géoproximité s'affiche automatiquement dans les propriétés et est mise à jour lorsque vous ajoutez ou supprimez des régions.

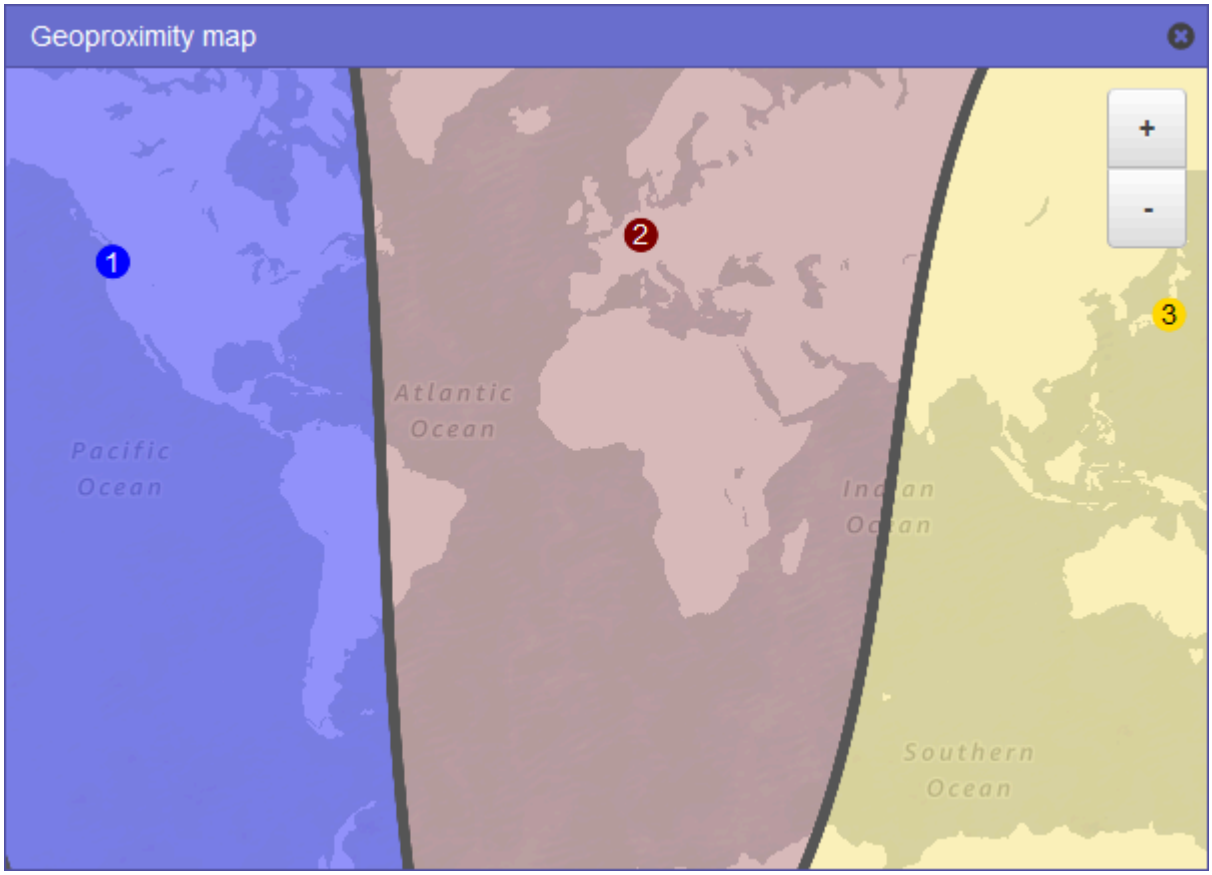
Remarques :

- La carte affiche une précision jusqu'à 16 kilomètres environ.
- La carte s'ajuste automatiquement lorsque vous ajoutez, modifiez ou supprimez des régions, ou lorsque vous modifiez le paramètre d'écart pour une région.
- Le numéro et la couleur d'une région dans chaque définition de règle correspondent aux numéros et aux couleurs sur la carte.

- Vous pouvez agrandir ou réduire l'affichage pour afficher plus ou moins de détails. Utilisez les boutons+et - sur la carte, un pavé tactile, ou la molette d'une souris pour modifier le niveau de zoom. Si vous ne voyez pas la région ou le numéro de région, vous pouvez agrandir le volet Propriétés pour qu'ils apparaissent.
- Vous pouvez déplacer la carte dans la fenêtre de carte pour afficher des zones spécifiques. Utilisez un pavé tactile, ou cliquez et faites glisser la carte avec une souris. Vous pouvez également déplacer la fenêtre de carte dans la fenêtre du navigateur.
- Si une stratégie contient plusieurs règles de proximité géographique, vous ne pouvez afficher la carte que pour une seule règle à la fois.

Old console

Vous pouvez afficher une carte qui montre l'effet de vos paramètres actuels de proximité géographique. Par exemple, si vous avez des ressources dans les régions USA Ouest (Oregon), Europe (Francfort) et Asie-Pacifique (Tokyo), et si vous ne spécifiez pas d'écart, la carte ressemble à ceci.



Pour afficher la carte pour une règle de proximité géographique, sélectionnez l'icône de graphique en regard de l'option Show geoproximity map (Afficher la carte de proximité géographique). (Cette icône s'affiche en haut de la règle.) Pour masquer la carte, sélectionnez à nouveau l'icône ou choisissez la x dans le coin supérieur droit de la carte.

Remarques :

- La carte affiche une précision jusqu'à 16 kilomètres environ.
- La carte s'ajuste automatiquement lorsque vous ajoutez, modifiez ou supprimez des régions, ou lorsque vous modifiez le paramètre d'écart pour une région.
- Le numéro et la couleur d'une région dans chaque définition de règle correspondent aux numéros et aux couleurs sur la carte.
- Vous pouvez agrandir ou réduire l'affichage pour afficher plus ou moins de détails. Utilisez les boutons+et - sur la carte, un pavé tactile, ou la molette d'une souris pour modifier le niveau de zoom.
- Vous pouvez déplacer la carte dans la fenêtre de carte pour afficher des zones spécifiques. Utilisez un pavé tactile, ou cliquez et faites glisser la carte avec une souris. Vous pouvez également déplacer la fenêtre de carte dans la fenêtre du navigateur.
- Si une stratégie contient plusieurs règles de proximité géographique, vous ne pouvez afficher la carte que pour une seule règle à la fois.

Création de versions supplémentaires d'une stratégie de trafic

Lorsque vous modifiez une stratégie de trafic, Amazon Route 53 crée automatiquement une autre version de la stratégie de trafic et conserve les versions précédentes, sauf si vous choisissez de les supprimer. La nouvelle version porte le même nom que la stratégie de trafic que vous modifiez. Un numéro de version incrémenté automatiquement par Route 53 permet de distinguer la nouvelle version de la version originale. Vous pouvez baser la nouvelle version d'une stratégie de trafic sur n'importe quelle version existante d'une stratégie de trafic portant le même nom.

Route 53 ne réutilise pas les numéros de version pour les nouvelles versions d'une stratégie de trafic donnée. Par exemple, si vous créez trois versions de MyTrafficPolicy, supprimez les deux dernières, puis créez une autre version, la nouvelle version est la version 4. En conservant les versions précédentes, Route 53 garantit la restauration à une configuration précédente si une nouvelle configuration n'achemine pas le trafic de la manière souhaitée.

Pour créer une nouvelle version de la stratégie de trafic, exécutez la procédure suivante.

> **Note**
>
> Nous mettons à jour la console Traffic Flow pour Route 53. Pendant la période de transition, vous pouvez continuer à utiliser l'ancienne console.

Choisissez l'onglet correspondant à la console que vous utilisez.

- Nouvelle console
- Ancienne console

New console

Pour créer une autre version d'une stratégie de trafic

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation, choisissez Traffic policies (Stratégies de trafic).
3. Choisissez le nom de la stratégie de trafic pour laquelle vous souhaitez créer une nouvelle version.
4. Dans le tableau Traffic policy versions (versions de stratégies de trafic) en haut de la page, cochez la case correspondant à la version de stratégie de trafic que vous souhaitez utiliser comme base pour la nouvelle version de stratégie de trafic.
5. Choisissez Edit policy as new version (Modifier la stratégie en tant que nouvelle version).
6. Dans la boîte de dialogue Modifier la politique en tant que nouvelle version, entrez une description pour la nouvelle version de la politique de trafic. Nous vous recommandons de spécifier une description qui différencie cette version des autres versions de la même stratégie de trafic. Lorsque vous créez un nouvel enregistrement de stratégie, la valeur que vous spécifiez s'affiche dans la liste des versions disponibles pour cette stratégie de trafic.
7. Choisissez Suivant.
8. Procédez à la mise à jour la configuration selon vos besoins. Pour de plus amples informations, veuillez consulter Valeurs à spécifier lors de la création d'une stratégie de trafic.

   Vous pouvez supprimer des règles, des points de terminaison et des branches d'une stratégie de trafic de différentes manières :

- Pour supprimer une règle ou un point de terminaison, choisissez-le dans l'éditeur, puis choisissez Supprimer dans le volet Propriétés.

> **Important**
>
> Si vous supprimez une règle comportant des points de terminaison et des règles enfant, Route 53 supprime également tous les enfants.

- Si vous connectez deux règles à la même règle enfant ou point de terminaison et que vous souhaitez supprimer l'une des connexions, sélectionnez la connexion que vous souhaitez supprimer, puis choisissez Supprimer dans le volet Propriétés.

9. Lorsque vous avez terminé les modifications, choisissez Save as new version (Enregistrer en tant que nouvelle version).
10. Facultatif : spécifiez les paramètres pour créer un ou plusieurs des enregistrements de stratégie dans une zone hébergée à l'aide de la nouvelle version de la stratégie de trafic. Pour de plus amples informations, veuillez consulter Valeurs à spécifier lors de la création ou de la mise à jour d'un enregistrement de stratégie. Vous pouvez également créer des enregistrements de stratégies ultérieurement, soit dans la même zone hébergée ou dans d'autres zones hébergées.

    Si vous ne souhaitez pas créer d'enregistrements de politique maintenant, choisissez Annuler, et la console affiche la liste des politiques de trafic et des enregistrements de politique que vous avez créés à l'aide du AWS compte actuel.
11. Si vous avez spécifié des paramètres pour les enregistrements de stratégie à l'étape précédente, choisissez Create policy record (Créer un enregistrement de stratégie).

Old console

Pour créer une autre version d'une stratégie de trafic

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation, choisissez Traffic policies (Stratégies de trafic).
3. Choisissez le nom de la stratégie de trafic pour laquelle vous souhaitez créer une nouvelle version.

4. Dans le tableau Traffic policy versions (versions de stratégies de trafic) en haut de la page, cochez la case correspondant à la version de stratégie de trafic que vous souhaitez utiliser comme base pour la nouvelle version de stratégie de trafic.
5. Choisissez Edit policy as new version (Modifier la stratégie en tant que nouvelle version).
6. Sur la page Update description (Mettre à jour la description), entrez une description pour la nouvelle version de stratégie de trafic. Nous vous recommandons de spécifier une description qui différencie cette version des autres versions de la même stratégie de trafic. Lorsque vous créez un nouvel enregistrement de stratégie, la valeur que vous spécifiez s'affiche dans la liste des versions disponibles pour cette stratégie de trafic.
7. Choisissez Suivant.
8. Procédez à la mise à jour la configuration selon vos besoins. Pour de plus amples informations, veuillez consulter Valeurs à spécifier lors de la création d'une stratégie de trafic.

   Vous pouvez supprimer des règles, des points de terminaison et des branches d'une stratégie de trafic de différentes manières :

   - Pour supprimer une règle ou un point de terminaison, cliquez sur x dans le coin supérieur droit de la zone.

     > **Important**
     >
     > Si vous supprimez une règle comportant des points de terminaison et des règles enfant, Route 53 supprime également tous les enfants.

   - Si vous connectez deux règles à même point de terminaison ou à la même règle enfant et que vous souhaitez supprimer l'une des connexions, placez votre curseur sur la connexion à supprimer, puis cliquez sur le x correspondant à cette connexion.
9. Lorsque vous avez terminé les modifications, choisissez Save as new version (Enregistrer en tant que nouvelle version).
10. Facultatif : spécifiez les paramètres pour créer un ou plusieurs des enregistrements de stratégie dans une zone hébergée à l'aide de la nouvelle version de la stratégie de trafic. Pour de plus amples informations, veuillez consulter Valeurs à spécifier lors de la création ou de la mise à jour d'un enregistrement de stratégie. Vous pouvez également créer des enregistrements de stratégies ultérieurement, soit dans la même zone hébergée ou dans d'autres zones hébergées.

Si vous ne souhaitez pas créer d'enregistrements de politique maintenant, choisissez Ignorer cette étape, et la console affiche la liste des politiques de trafic et des enregistrements de politique que vous avez créés à l'aide du AWS compte actuel.

11. Si vous avez spécifié des paramètres pour les enregistrements de stratégie à l'étape précédente, choisissez Create policy record (Créer un enregistrement de stratégie).

Création d'une politique de trafic à l'aide d'un document JSON

Vous pouvez créer une nouvelle stratégie de trafic ou une nouvelle version d'une stratégie existante en important un document au format JSON qui décrit tous les points de terminaison et règles que vous souhaitez inclure dans la règle de trafic. Pour plus d'informations sur le format de document JSON et pour consulter des exemples que vous pouvez copier et modifier, consultez Format de document de stratégie de trafic dans le document Référence de l'API Amazon Route 53.

Le moyen le plus simple d'obtenir le document au format JSON pour une version de politique de trafic existante consiste à utiliser la `get-traffic-policy` commande dans la CLI. AWS Pour plus d'informations, consultez get-traffic-policy dans la Référence des commandes de l'AWS CLI .

Le fichier JSON créé par la commande `get-traffic-policy` inclut des barres obliques inversées (\) comme caractères d'échappement. Avant d'importer le fichier JSON, remplacez toutes les barres obliques inversées par des caractères nuls.

> **Note**
>
> Nous mettons à jour la console Traffic Flow pour Route 53. Pendant la période de transition, vous pouvez continuer à utiliser l'ancienne console.

Choisissez l'onglet correspondant à la console que vous utilisez.

- Nouvelle console
- Ancienne console

New console

Pour créer une stratégie de trafic en important un document JSON

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Pour créer une nouvelle stratégie de trafic en important un document JSON, effectuez les opérations suivantes :
   a. Dans le volet de navigation, choisissez Traffic policies (Stratégies de trafic).
   b. Choisissez Create traffic policy (Créer une stratégie de trafic).
   c. Sur la page Name policy (Nommer la stratégie), spécifiez les valeurs applicables. Pour de plus amples informations, veuillez consulter Valeurs à spécifier lors de la création d'une stratégie de trafic.
   d. Passez à l'étape 4.
3. Pour créer une nouvelle version d'une stratégie de trafic existante en important un document JSON, procédez de la manière suivante :
   a. Dans le volet de navigation, choisissez Traffic policies (Stratégies de trafic).
   b. Choisissez le nom de la stratégie de trafic qui servira de base à la nouvelle version.
   c. Dans le tableau Traffic policy versions (Versions de stratégies de trafic), cochez la case correspondant à la version qui servira de base à la nouvelle version.
   d. Choisissez Edit policy as new version (Modifier la stratégie en tant que nouvelle version).
   e. Sur la page Update description (Mettre à jour la description), entrez une description de la nouvelle version.
   f. Passez à l'étape 4.
4. Choisissez Suivant.
5. Sur la page de l'éditeur, choisissez l'icône de l'éditeur json

   ( )

   dans le coin supérieur droit de l'éditeur.
6. Entrez une nouvelle stratégie de trafic, collez un exemple de stratégie de trafic ou collez une stratégie de trafic existante.

   Pour des exemples de politiques, consultez la section Exemples JSON de politique de flux de trafic.

7. Choisissez Mettre à jour.

Old console

Pour créer une stratégie de trafic en important un document JSON

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Pour créer une nouvelle stratégie de trafic en important un document JSON, effectuez les opérations suivantes :
   a. Dans le volet de navigation, choisissez Traffic policies (Stratégies de trafic).
   b. Choisissez Create traffic policy (Créer une stratégie de trafic).
   c. Sur la page Name policy (Nommer la stratégie), spécifiez les valeurs applicables. Pour de plus amples informations, veuillez consulter Valeurs à spécifier lors de la création d'une stratégie de trafic.
   d. Passez à l'étape 4.
3. Pour créer une nouvelle version d'une stratégie de trafic existante en important un document JSON, procédez de la manière suivante :
   a. Dans le volet de navigation, choisissez Traffic policies (Stratégies de trafic).
   b. Choisissez le nom de la stratégie de trafic qui servira de base à la nouvelle version.
   c. Dans le tableau Traffic policy versions (Versions de stratégies de trafic), cochez la case correspondant à la version qui servira de base à la nouvelle version.
   d. Choisissez Edit policy as new version (Modifier la stratégie en tant que nouvelle version).
   e. Sur la page Update description (Mettre à jour la description), entrez une description de la nouvelle version.
   f. Passez à l'étape 4.
4. Choisissez Suivant.
5. Choisissez Import traffic policy (Importer une stratégie de trafic).
6. Entrez une nouvelle stratégie de trafic, collez un exemple de stratégie de trafic ou collez une stratégie de trafic existante.

   Pour des exemples de politiques, consultez la section Exemples JSON de politique de flux de trafic

7. Choisissez Import traffic policy (Importer une stratégie de trafic).

Affichage des versions de stratégie de trafic et des enregistrements de stratégie associés

Vous pouvez afficher toutes les versions que vous avez créées pour une stratégie de trafic, ainsi que tous les enregistrements de stratégie que vous avez créés à l'aide de chacune des versions de la stratégie de trafic.

> **Note**
>
> Nous mettons à jour la console Traffic Flow pour Route 53. Pendant la période de transition, vous pouvez continuer à utiliser l'ancienne console.

Choisissez l'onglet correspondant à la console que vous utilisez.

- Nouvelle console
- Ancienne console

New console

Pour afficher les versions de la stratégie de trafic et les enregistrements de stratégie associés

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation, choisissez Traffic policies (Stratégies de trafic).
3. Choisissez le nom associé d'une politique de trafic.
4. Le tableau supérieur répertorie toutes les versions créées pour la stratégie de trafic. Le tableau comprend les informations suivantes :

   Version number

   Numéro de chaque version créée pour une stratégie de trafic. Si vous choisissez un numéro de version, la console affiche la configuration pour cette version.

Number of policy records

Nombre d'enregistrements de stratégie créés à l'aide de cette version de la stratégie de trafic.

Type DNS

Le type DNS que vous avez spécifié lorsque vous avez créé la version de la stratégie de trafic.

Descriptions des versions

La description que vous avez spécifiée lorsque vous avez créé la version de la stratégie de trafic.

5. Le tableau du bas répertorie tous les enregistrements de stratégie créés à l'aide des versions de stratégie de trafic de la table supérieure. Le tableau comprend les informations suivantes :

Nom du DNS

Noms DNS que vous avez associés à la stratégie de trafic.

Statut

Les valeurs possibles sont notamment les suivantes :

Applied

Route 53 a terminé la création ou la mise à jour d'un enregistrement de stratégie et des enregistrements correspondants.

Creating

Route 53 crée les enregistrements pour un nouvel enregistrement de stratégie.

Mise à jour

Vous avez mis à jour un enregistrement de stratégie et Route 53 est en train de créer un nouveau groupe d'enregistrements qui remplacera le groupe existant pour le nom DNS spécifié.

Deleting

Route 53 est en train de supprimer un enregistrement de stratégie et les enregistrements associés.

Failed

Route 53 n'a pas été en mesure de créer ou de mettre à jour l'enregistrement de stratégie et les enregistrements associés.

Type DNS

Type DNS de tous les enregistrements que Route 53 a créé pour cet enregistrement de stratégie. Lorsque vous modifiez un enregistrement de stratégie, vous devez spécifier une version de stratégie de trafic portant le même type DNS que celui de l'enregistrement de stratégie que vous modifiez.

Version

Indique la version de stratégie de trafic que vous avez utilisée pour créer l'enregistrement de stratégie.

TTL (en secondes)

Durée, en secondes, pendant laquelle vous voulez que les résolveurs DNS récursifs mettent en cache les informations relatives à cet enregistrement. Si vous spécifiez une valeur plus longue (par exemple, 172 800 secondes, ou deux jours), vous paierez moins pour le service Route 53, car les résolveurs récursifs envoient moins souvent de demandes à Route 53. Cependant, les modifications apportées aux enregistrements (par exemple, une nouvelle adresse IP) mettent plus de temps à prendre effet car les résolveurs récursifs utilisent les valeurs qui se trouvent dans leur cache pendant plus longtemps au lieu de demander les informations les plus récentes à Route 53.

Old console

Pour afficher les versions de la stratégie de trafic et les enregistrements de stratégie associés

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation, choisissez Traffic policies (Stratégies de trafic).
3. Choisissez le nom d'une stratégie de trafic.
4. Le tableau supérieur répertorie toutes les versions créées pour la stratégie de trafic. Le tableau comprend les informations suivantes :

Version number

Numéro de chaque version créée pour une stratégie de trafic. Si vous choisissez un numéro de version, la console affiche la configuration pour cette version.

Number of policy records

Nombre d'enregistrements de stratégie créés à l'aide de cette version de la stratégie de trafic.

Type DNS

Le type DNS que vous avez spécifié lorsque vous avez créé la version de la stratégie de trafic.

Version description

La description que vous avez spécifiée lorsque vous avez créé la version de la stratégie de trafic.

5. Le tableau du bas répertorie tous les enregistrements de stratégie créés à l'aide des versions de stratégie de trafic de la table supérieure. Le tableau comprend les informations suivantes :

Nom DNS de l'enregistrement de stratégie

Noms DNS que vous avez associés à la stratégie de trafic.

Statut

Les valeurs possibles sont notamment les suivantes :

Applied

Route 53 a terminé la création ou la mise à jour d'un enregistrement de stratégie et des enregistrements correspondants.

Creating

Route 53 crée les enregistrements pour un nouvel enregistrement de stratégie.

Mise à jour

Vous avez mis à jour un enregistrement de stratégie et Route 53 est en train de créer un nouveau groupe d'enregistrements qui remplacera le groupe existant pour le nom DNS spécifié.

Deleting

Route 53 est en train de supprimer un enregistrement de stratégie et les enregistrements associés.

Failed

Route 53 n'a pas été en mesure de créer ou de mettre à jour l'enregistrement de stratégie et les enregistrements associés.

Version used

Indique la version de stratégie de trafic que vous avez utilisée pour créer l'enregistrement de stratégie.

Type DNS

Type DNS de tous les enregistrements que Route 53 a créé pour cet enregistrement de stratégie. Lorsque vous modifiez un enregistrement de stratégie, vous devez spécifier une version de stratégie de trafic portant le même type DNS que celui de l'enregistrement de stratégie que vous modifiez.

TTL (en secondes)

Durée, en secondes, pendant laquelle vous voulez que les résolveurs DNS récursifs mettent en cache les informations relatives à cet enregistrement. Si vous spécifiez une valeur plus longue (par exemple, 172 800 secondes, ou deux jours), vous paierez moins pour le service Route 53, car les résolveurs récursifs envoient moins souvent de demandes à Route 53. Cependant, les modifications apportées aux enregistrements (par exemple, une nouvelle adresse IP) mettent plus de temps à prendre effet car les résolveurs récursifs utilisent les valeurs qui se trouvent dans leur cache pendant plus longtemps au lieu de demander les informations les plus récentes à Route 53.

Suppression de versions de stratégie de trafic et de stratégies de trafic

Pour supprimer une stratégie de trafic, vous devez supprimer toutes les versions (y compris la version originale) que vous avez créées pour la stratégie de trafic. En outre, pour supprimer une version de stratégie de trafic, vous devez supprimer tous les enregistrements de stratégie que vous avez créés à l'aide de la version de stratégie de trafic.

> **Important**
>
> Si vous supprimez des enregistrements de stratégie qu'Amazon Route 53 utilise pour répondre aux requêtes DNS, Route 53 cesse de répondre aux requêtes pour les noms DNS correspondants. Supposons par exemple que Route 53 utilise l'enregistrement de stratégie de www.example.com pour répondre aux requêtes DNS pour www.example.com et que vous supprimez l'enregistrement de stratégie, les utilisateurs ne pourront pas accéder à votre site web ou à une application web à l'aide du nom de domaine www.example.com.

Pour supprimer des versions d'une stratégie de trafic et, si besoin, une stratégie de trafic, procédez comme suit :

> **Note**
>
> Nous mettons à jour la console Traffic Flow pour Route 53. Pendant la période de transition, vous pouvez continuer à utiliser l'ancienne console.

Choisissez l'onglet correspondant à la console que vous utilisez.

- Nouvelle console
- Ancienne console

New console

Pour supprimer des versions de la stratégie de trafic et une stratégie de trafic

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation, choisissez Traffic policies (Stratégies de trafic).
3. Choisissez le nom associé de la politique de trafic dont vous souhaitez supprimer des versions de politique de trafic et que vous souhaitez éventuellement supprimer complètement.
4. Si les versions de politique de trafic que vous souhaitez supprimer dans le tableau supérieur apparaissent dans la colonne Version du tableau des enregistrements de politique, cochez les cases des enregistrements de politique correspondants dans le tableau inférieur.

Par exemple, si vous souhaitez supprimer la version 3 d'une stratégie de trafic, mais que l'un des enregistrements de stratégie de la table du bas a été créé à l'aide de la version 3, cochez la case correspondant à cet enregistrement de stratégie.

5. Choisissez Supprimer les enregistrements de stratégie, puis dans la boîte de dialogue Supprimer les enregistrements de stratégie, choisissez Confirmer.
6. Actualisez la page jusqu'à ce que les enregistrements de politique que vous avez supprimés n'apparaissent plus dans le tableau.
7. Dans la table supérieure, cochez les cases des versions de stratégie de trafic que vous souhaitez supprimer.
8. Sélectionnez Delete (Supprimer).
9. Si vous avez supprimé toutes les versions de la politique de trafic à l'étape précédente et que vous souhaitez également supprimer la politique de trafic, actualisez la page pour actualiser l'affichage jusqu'à ce que le tableau soit vide.
10. Dans le panneau de navigation, choisissez Traffic policies (Stratégies de trafic).
11. Dans la liste des stratégies de trafic, cochez la case correspondant à la stratégie de trafic que vous souhaitez supprimer.
12. Choisissez Delete traffic policy (Supprimer la stratégie de trafic).

Old console

Pour supprimer des versions de la stratégie de trafic et une stratégie de trafic

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation, choisissez Traffic policies (Stratégies de trafic).
3. Choisissez le nom de la stratégie de trafic pour laquelle vous souhaitez supprimer des versions ou que vous souhaitez supprimer complètement.
4. Si les versions de la stratégie de trafic que vous souhaitez supprimer dans la table supérieure figurent dans la colonne Version used (Version utilisée) de la table du bas, cochez les cases pour les enregistrements de stratégie correspondants dans la table du bas.

   Par exemple, si vous souhaitez supprimer la version 3 d'une stratégie de trafic, mais que l'un des enregistrements de stratégie de la table du bas a été créé à l'aide de la version 3, cochez la case correspondant à cet enregistrement de stratégie.

5. Choisissez Delete policy records (Supprimer des enregistrements de stratégie).
6. Cliquez sur le bouton d'actualisation de la table du bas pour actualiser l'affichage jusqu'à ce que les enregistrements de stratégie que vous avez supprimés n'apparaissent plus dans la table.
7. Dans la table supérieure, cochez les cases des versions de stratégie de trafic que vous souhaitez supprimer.
8. Choisissez Delete version (Supprimer la version).
9. Si vous avez supprimé toutes les versions de la stratégie de trafic à l'étape précédente et si vous voulez également supprimer la stratégie de trafic, cliquez sur le bouton d'actualisation de la table supérieure pour actualiser l'affichage jusqu'à ce que la table soit vide.
10. Dans le panneau de navigation, choisissez Traffic policies (Stratégies de trafic).
11. Dans la liste des stratégies de trafic, cochez la case correspondant à la stratégie de trafic que vous souhaitez supprimer.
12. Choisissez Delete traffic policy (Supprimer la stratégie de trafic).

Création et gestion des enregistrements de stratégie

Pour acheminer le trafic Internet vers les ressources spécifiées lorsque vous avez créé une stratégie de trafic, créez un ou plusieurs enregistrements de stratégie. Chaque enregistrement de stratégie identifie la zone hébergée dans laquelle vous souhaitez créer l'enregistrement de stratégie, ainsi que le nom de domaine ou de sous-domaine vers lequel vous souhaitez acheminer le trafic. Par exemple, si vous souhaitez acheminer du trafic pour www.example.com, vous spécifiez l'ID de la zone hébergée pour example.com, puis vous spécifiez www.example.com pour le Policy record DNS name (Nom DNS d'enregistrement de stratégie).

Si vous souhaitez utiliser la même stratégie de trafic pour acheminer le trafic pour plusieurs noms de domaine ou de sous-domaine, deux options s'offrent à vous :

- Vous pouvez créer un enregistrement de stratégie pour chaque nom de domaine ou de sous-domaine.
- Vous pouvez créer un enregistrement de stratégie, puis créer des enregistrements d'alias ou CNAME qui font référence à l'enregistrement de stratégie.

Par exemple, si vous souhaitez utiliser la même stratégie de trafic pour example.com, example.net et example.org, vous pouvez effectuer l'une des actions suivantes :

- Créez un enregistrement de stratégie pour chacun d'entre eux.
- Créez un enregistrement de stratégie pour l'un d'entre eux, puis créez des enregistrements CNAME dans les zones hébergées pour les deux autres. Dans les deux enregistrements CNAME, vous spécifiez le nom d'enregistrement pour lequel vous avez créé un enregistrement de stratégie.

Si vous souhaitez utiliser la même stratégie de trafic pour un domaine et ses sous-domaines, tels qu'exemple.com et www.exemple.com, vous pouvez créer un enregistrement de stratégie pour un des noms, puis créer des enregistrements d'alias pour le reste. Par exemple, vous pouvez créer un enregistrement de stratégie pour exemple.com, puis créer un enregistrement d'alias pour www.exemple.com possédant l'enregistrement exemple.com en tant que cible de l'alias.

> **Note**
>
> Des frais mensuels s'appliquent pour chaque enregistrement de stratégie créé. Si vous souhaitez utiliser la même stratégie de trafic pour plusieurs noms de domaine ou de sous-domaine, vous pouvez utiliser des enregistrements d'alias ou CNAME pour diminuer vos frais :
>
> - Si vous créez un enregistrement de stratégie et un ou plusieurs enregistrements CNAME faisant référence à l'enregistrement de stratégie, vous payez uniquement pour l'enregistrement de stratégie et pour les requêtes DNS pour les enregistrements CNAME.
> - Si vous créez un enregistrement de stratégie et un ou plusieurs enregistrements d'alias dans la même zone hébergée et faisant référence à l'enregistrement de stratégie, vous payez uniquement pour l'enregistrement de stratégie et pour les requêtes DNS pour les enregistrements d'alias.

Rubriques

- Création d'enregistrements de stratégie
- Valeurs à spécifier lors de la création ou de la mise à jour d'un enregistrement de stratégie
- Mise à jour d'enregistrements de stratégie
- Suppression d'enregistrements de stratégie

Création d'enregistrements de stratégie

Pour créer un enregistrement de stratégie, utilisez la procédure suivante.

> **Important**
>
> Pour chaque enregistrement de stratégie que vous créez, des frais mensuels s'appliquent. Si vous supprimez ultérieurement l'enregistrement de la stratégie, les frais sont calculés au prorata. Pour de plus amples informations, veuillez consulter la section « Flux de trafic » de la page Tarification d'Amazon Route 53.

> **Note**
>
> Nous mettons à jour la console Traffic Flow pour Route 53. Pendant la période de transition, vous pouvez continuer à utiliser l'ancienne console.

Choisissez l'onglet correspondant à la console que vous utilisez.

- Nouvelle console
- Ancienne console

New console

Pour créer un enregistrement de stratégie

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation, choisissez Policy records (Enregistrements de stratégies).
3. Sur la page Policy records (Enregistrements de stratégies), choisissez Create policy records (Créer des enregistrements de stratégies).
4. Sur la page Create policy records (Créer des enregistrements de stratégies), spécifiez les valeurs applicables. Pour de plus amples informations, veuillez consulter Valeurs à spécifier lors de la création ou de la mise à jour d'un enregistrement de stratégie.
5. Pour ajouter des enregistrements supplémentaires à la même zone hébergée, choisissez Ajouter un enregistrement de politique.
6. Choisissez Create policy records (Créer des enregistrements de stratégies).

   Plusieurs minutes peuvent être nécessaires pour que l'état de l'enregistrement de stratégie créé s'affiche comme Appliqué.

7. Si vous souhaitez créer des enregistrements de stratégie dans une autre zone hébergée, répétez les étapes 3 à 5.

> **Note**
>
> Si l'état de l'enregistrement de stratégie est Échec, cliquez sur le bouton d'information situé à côté de l'état pour obtenir plus d'informations sur l'échec. Si vous avez besoin d'une aide supplémentaire et que vous souhaitez contacter le AWS support technique, consultez l'article Comment puis-je obtenir une assistance technique AWS ?

Old console

Pour créer un enregistrement de stratégie

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation, choisissez Policy records (Enregistrements de stratégies).
3. Sur la page Policy records (Enregistrements de stratégies), choisissez Create policy records (Créer des enregistrements de stratégies).
4. Sur la page Create policy records (Créer des enregistrements de stratégies), spécifiez les valeurs applicables. Pour de plus amples informations, veuillez consulter Valeurs à spécifier lors de la création ou de la mise à jour d'un enregistrement de stratégie.
5. Choisissez Create policy records (Créer des enregistrements de stratégies).

   Plusieurs minutes peuvent être nécessaires pour que l'état de l'enregistrement de stratégie créé s'affiche comme Appliqué.
6. Si vous souhaitez créer des enregistrements de stratégie dans une autre zone hébergée, répétez les étapes 3 à 5.

> **Note**
>
> Si l'état de l'enregistrement de stratégie est Échec, cliquez sur le bouton d'information situé à côté de l'état pour obtenir plus d'informations sur l'échec. Si vous avez besoin

d'une aide supplémentaire et que vous souhaitez contacter le AWS support technique, consultez l'article Comment puis-je obtenir une assistance technique AWS ?

Valeurs à spécifier lors de la création ou de la mise à jour d'un enregistrement de stratégie

> **Note**
>
> Nous mettons à jour la console Traffic Flow pour Route 53. Pendant la période de transition, vous pouvez continuer à utiliser l'ancienne console. La liste suivante s'applique aux deux consoles, sauf indication contraire.

Lorsque vous créez ou mettez à jour un enregistrement de stratégie, vous spécifiez les valeurs suivantes

- Traffic policy
- Version
- Hosted zone
- Policy record DNS name
- TTL

Stratégie de trafic

Choisissez la stratégie de trafic dont vous souhaitez utiliser la configuration pour cet enregistrement de stratégie.

Version

Choisissez la version de la stratégie de trafic dont vous souhaitez utiliser la configuration pour cet enregistrement de stratégie.

Si vous mettez à jour un enregistrement de stratégie existant, vous devez choisir une version dont le type DNS correspond au type DNS actuel de l'enregistrement de stratégie. Par exemple, si le type DNS de l'enregistrement de stratégie est A, vous devez choisir une version dont le type DNS est A.

Zone hébergée

Choisissez la zone hébergée dans laquelle vous souhaitez créer un enregistrement de stratégie à l'aide de la stratégie de trafic et de la version spécifiées. Vous ne pouvez pas modifier la valeur de Hosted zone (Zone hébergée) après avoir créé un enregistrement de stratégie.

Nom DNS (nouvelle console), nom DNS de l'enregistrement de politique (ancienne console)

Lorsque vous créez un enregistrement de stratégie, entrez le nom de domaine ou le nom de sous-domaine pour lequel vous souhaitez que Route 53 réponde aux requêtes DNS à l'aide de la configuration de la stratégie de trafic et de la version spécifiées.

Pour utiliser la même configuration pour plusieurs noms de domaine ou noms de sous-domaines dans la zone hébergée spécifiée, choisissez Ajouter un enregistrement de stratégie (nouvelle console) ou Ajouter un autre enregistrement de politique (ancienne console), puis entrez le nom de domaine ou le nom de sous-domaine et le TTL applicables.

Vous ne pouvez pas modifier la valeur de Policy record DNS name (Nom DNS d'enregistrement de stratégie) après avoir créé un enregistrement de stratégie.

TTL (en secondes)

Entrez la durée, en secondes, pendant laquelle vous voulez que les résolveurs DNS récursifs mettent en cache les informations relatives à cet enregistrement. Si vous spécifiez une valeur plus longue (par exemple, 172 800 secondes, ou deux jours), vous paierez moins pour le service Route 53, car les résolveurs récursifs envoient moins souvent de demandes à Route 53. Cependant, les modifications apportées aux enregistrements (par exemple, une nouvelle adresse IP) mettent plus de temps à prendre effet car les résolveurs récursifs utilisent les valeurs qui se trouvent dans leur cache pendant plus longtemps au lieu de demander les informations les plus récentes à Route 53.

Mise à jour d'enregistrements de stratégie

Pour mettre à jour les paramètres d'un enregistrement de stratégie, exécutez la procédure suivante.

> **Note**
>
> Nous mettons à jour la console Traffic Flow pour Route 53. Pendant la période de transition, vous pouvez continuer à utiliser l'ancienne console.

Choisissez l'onglet correspondant à la console que vous utilisez.

- Nouvelle console
- Ancienne console

New console

Pour mettre à jour un enregistrement de stratégie

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation, choisissez Policy records (Enregistrements de stratégies).
3. Sur la page Enregistrements de stratégie, cochez la case correspondant à l'enregistrement de stratégie que vous souhaitez mettre à jour, puis choisissez Modifier.
4. Dans la page Edit policy record (Modifier un enregistrement de stratégie), spécifiez les valeurs applicables. Pour de plus amples informations, veuillez consulter Valeurs à spécifier lors de la création ou de la mise à jour d'un enregistrement de stratégie.
5. Choisissez Edit policy record (Modifier un enregistrement de stratégie).

   Plusieurs minutes peuvent être nécessaires pour que l'état de l'enregistrement de stratégie créé s'affiche comme Appliqué.
6. Si vous souhaitez mettre à jour un autre enregistrement de stratégie, répétez les étapes 3 à 5.

> **Note**
>
> Si l'état de l'enregistrement de stratégie est Échec, cliquez sur le bouton d'information situé à côté de l'état pour obtenir plus d'informations sur l'échec. Si vous avez besoin d'une aide supplémentaire et que vous souhaitez contacter le AWS support technique, consultez l'article Comment puis-je obtenir une assistance technique AWS ?

Old console

Pour mettre à jour un enregistrement de stratégie

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation, choisissez Policy records (Enregistrements de stratégies).
3. Dans la page Policy records (Enregistrements de stratégie) , cochez la case de l'enregistrement de stratégie que vous souhaitez mettre à jour, puis sélectionnez Edit policy record (Modifier un enregistrement de stratégie).
4. Dans la page Edit policy record (Modifier un enregistrement de stratégie), spécifiez les valeurs applicables. Pour de plus amples informations, veuillez consulter Valeurs à spécifier lors de la création ou de la mise à jour d'un enregistrement de stratégie.
5. Choisissez Edit policy record (Modifier un enregistrement de stratégie).

   Plusieurs minutes peuvent être nécessaires pour que l'état de l'enregistrement de stratégie créé s'affiche comme Appliqué.
6. Si vous souhaitez mettre à jour un autre enregistrement de stratégie, répétez les étapes 3 à 5.

> **Note**
>
> Si l'état de l'enregistrement de stratégie est Échec, cliquez sur le bouton d'information situé à côté de l'état pour obtenir plus d'informations sur l'échec. Si vous avez besoin d'une aide supplémentaire et que vous souhaitez contacter le AWS support technique, consultez l'article Comment puis-je obtenir une assistance technique AWS ?

Suppression d'enregistrements de stratégie

Pour supprimer des enregistrements de stratégie, exécutez la procédure suivante.

> **Important**
>
> Si vous supprimez des enregistrements de stratégie qu'Amazon Route 53 utilise pour répondre aux requêtes DNS, Route 53 cesse de répondre aux requêtes pour les noms DNS correspondants. Supposons par exemple que Route 53 utilise l'enregistrement de stratégie

de www.example.com pour répondre aux requêtes DNS pour www.example.com et que vous supprimez l'enregistrement de stratégie, les utilisateurs ne pourront pas accéder à votre site web ou à une application web à l'aide du nom de domaine www.example.com.

> **Note**
>
> Nous mettons à jour la console Traffic Flow pour Route 53. Pendant la période de transition, vous pouvez continuer à utiliser l'ancienne console.

Choisissez l'onglet correspondant à la console que vous utilisez.

- Nouvelle console
- Ancienne console

New console

Pour supprimer un enregistrement de stratégie

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation, choisissez Policy records (Enregistrements de stratégies).
3. Sur la page Enregistrements de stratégie, cochez les cases correspondant aux enregistrements de stratégie que vous souhaitez supprimer, puis choisissez Supprimer.
4. Dans la boîte de dialogue Supprimer l'enregistrement de politique, choisissez Confirmer.

   Patientez quelques minutes et actualisez la page pour vous assurer que l'enregistrement de stratégie disparaît de la liste.

Old console

Pour supprimer un enregistrement de stratégie

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation, choisissez Policy records (Enregistrements de stratégies).

3. Dans la page Policy records (Enregistrements de stratégie), cochez les cases des enregistrements de stratégie que vous souhaitez supprimer, puis sélectionnez Delete policy record (Supprimer un enregistrement de stratégie).

   Patientez quelques minutes et actualisez la page pour vous assurer que l'enregistrement de stratégie disparaît de la liste.

Qu'est-ce que c'est Amazon Route 53 Resolver ?

Amazon Route 53 Resolver répond de manière récursive aux requêtes DNS provenant AWS des ressources relatives aux archives publiques, aux noms DNS spécifiques à Amazon VPC et aux zones hébergées privées Amazon Route 53, et est disponible par défaut dans tous les domaines. VPCs

> **Note**
>
> Amazon Route 53 Resolver était auparavant appelé serveur DNS Amazon, mais a été renommé lorsque les règles Resolver et les points de terminaison entrants et sortants ont été introduits. Pour plus d'informations, veuillez consulter Serveur Amazon DNS dans le Guide de l'utilisateur Amazon Virtual Private Cloud.

Un VPC Amazon se connecte à un Route 53 Resolver à une adresse IP VPC+2. Cette adresse VPC +2 se connecte à un Route 53 Resolver situé dans une zone de disponibilité.

Un Route 53 Resolver répond automatiquement aux requêtes DNS pour :

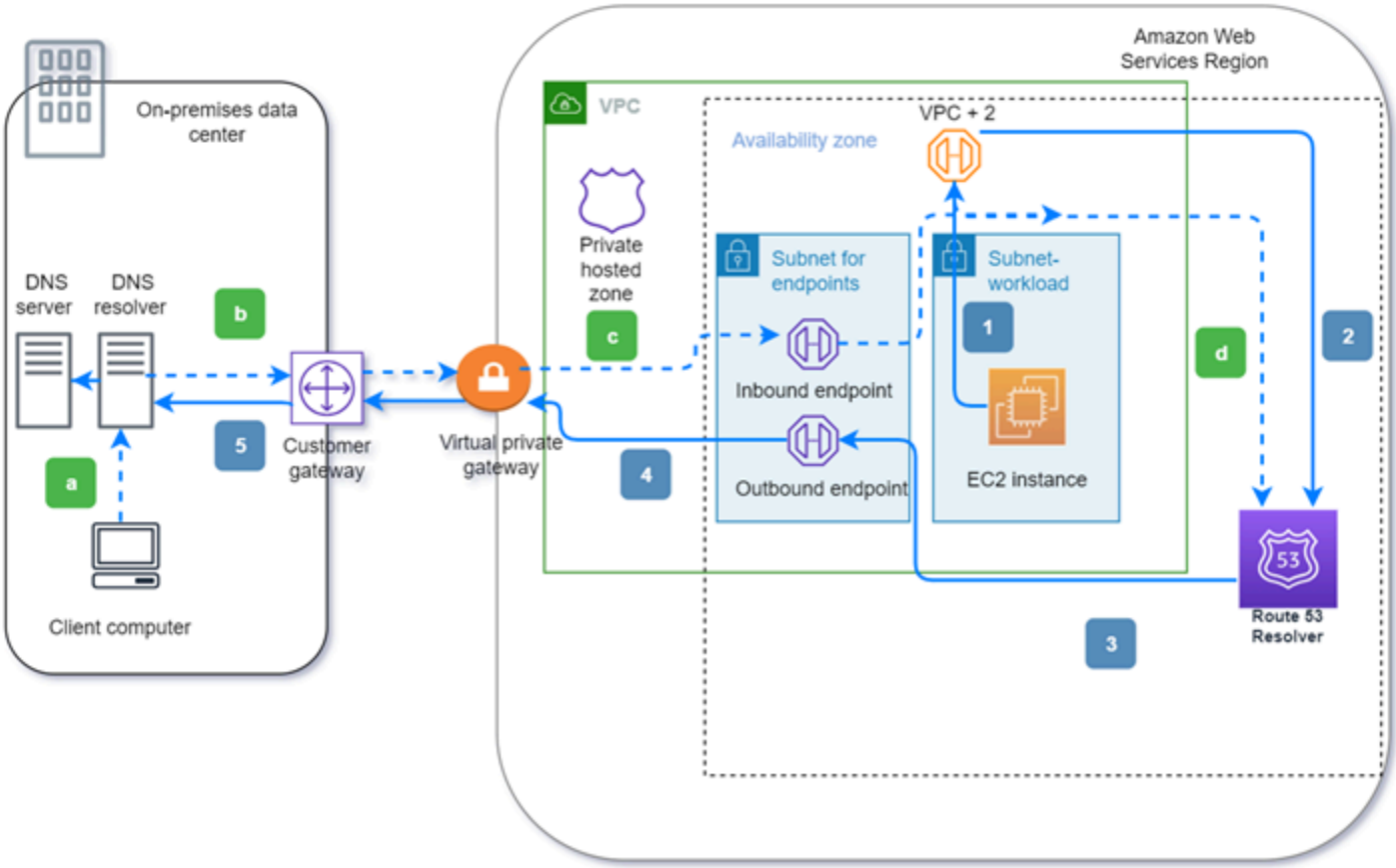
- Noms de domaine VPC locaux pour les EC2 instances (par exemple, ec2-192-0-2-44.compute-1.amazonaws.com).
- Enregistrements dans des zones hébergées privées (par exemple, acme.exemple.com).
- Pour les noms de domaine publics, Route 53 Resolver effectue des recherches récursives sur les serveurs de noms publics sur Internet.

Si vos charges de travail exploitent à la fois les ressources locales VPCs et les ressources locales, vous devez également résoudre les enregistrements DNS hébergés sur site. De même, ces ressources locales peuvent avoir besoin de résoudre les noms hébergés sur AWS. Grâce aux points de terminaison du résolveur et aux règles de transfert conditionnel, vous pouvez résoudre les requêtes DNS entre vos ressources locales et VPCs créer une configuration de cloud hybride via VPN ou Direct Connect (DX). En particulier :

- Les points de terminaison du Résolveur entrants autorisent les requêtes DNS vers votre VPC à partir de votre réseau sur site ou d'un autre VPC.

- Les points de terminaison du Résolveur sortants autorisent les requêtes DNS depuis votre VPC vers votre réseau sur site ou vers un autre VPC.
- Les règles du Résolveur vous permettent de créer une règle de réacheminement pour chaque nom de domaine et de spécifier le nom du domaine pour lequel vous souhaitez réacheminer les requêtes DNS depuis votre VPC vers un résolveur DNS sur site et depuis votre site vers votre VPC. Les règles sont appliquées directement à votre VPC et peuvent être partagées entre plusieurs comptes.

Le schéma suivant montre la résolution DNS hybride avec les points de terminaison du Résolveur. Notez que le diagramme est simplifié pour n'afficher qu'une seule zone de disponibilité.



Le diagramme suivant illustre les étapes suivantes :

Sortant (flèches pleines 1–5) :

1. Une EC2 instance Amazon doit résoudre une requête DNS sur le domaine internal.example.com. Le serveur DNS faisant autorité se trouve dans le centre de données sur site. Cette requête DNS est envoyée au VPC+2 du VPC qui se connecte à Route 53 Resolver.

2. Une règle de réacheminement Route 53 Resolver est configurée pour transférer les requêtes vers internal.exemple.com dans le centre de données sur site.
3. La requête est transmise à un point de terminaison sortant.
4. Le point de terminaison sortant transmet la requête au résolveur DNS local via une connexion privée entre AWS et le centre de données. La connexion peut être l'une AWS Direct Connect ou l'autre AWS Site-to-Site VPN, décrite comme une passerelle privée virtuelle.
5. Le résolveur DNS local résout la requête DNS pour internal.example.com et renvoie la réponse à l' EC2 instance Amazon via le même chemin en sens inverse.

Entrant (flèches pointillées a—d) :

a. Un client du centre de données sur site doit résoudre une requête DNS vers une AWS ressource pour le domaine dev.example.com. Il envoie la requête au résolveur DNS sur site.
b. Le résolveur DNS sur site dispose d'une règle de transfert qui dirige les requêtes vers dev.exemple.com vers un point de terminaison entrant.
c. La requête arrive au point de terminaison entrant via une connexion privée, telle que AWS Direct Connect ou AWS Site-to-Site VPN décrite comme une passerelle virtuelle.
d. Le point de terminaison entrant envoie la requête à Route 53 Resolver, et Route 53 Resolver résout la requête DNS pour dev.example.com et renvoie la réponse au client via le même chemin en sens inverse.

Rubriques

- Résolution des requêtes DNS entre VPCs et votre réseau
- Disponibilité et évolutivité du résolveur Route 53
- Mise en route avec Route 53 Resolver
- Transférer les requêtes DNS entrantes vers votre VPCs
- Réacheminement des requêtes DNS sortantes vers votre réseau
- Tutoriel sur les règles de délégation Resolver
- Activation de la validation DNSSEC dans Amazon Route 53

Résolution des requêtes DNS entre VPCs et votre réseau

Resolver contient en outre des points de terminaison que vous configurez pour répondre aux requêtes DNS depuis et vers votre environnement sur site.

> **Note**
>
> La transmission de requêtes DNS privées à toute adresse VPC CIDR + 2 à partir de vos serveurs DNS sur site n'est pas prise en charge et peut entraîner des résultats instables. À la place, nous vous recommandons d'utiliser un point de terminaison entrant Resolver.

Vous pouvez également intégrer la résolution DNS entre Resolver et les résolveurs DNS sur votre réseau en configurant des règles de réacheminement. Votre réseau peut inclure tous les réseaux accessibles depuis votre VPC, par exemple :

- Le VPC lui-même
- Un autre VPC appairé
- Un réseau sur site connecté à une passerelle VPN ou AWS à AWS Direct Connect une passerelle de traduction d'adresses réseau (NAT)

Avant de commencer à transférer des requêtes, vous créez les points de terminaison entrants et and/or sortants du résolveur dans le VPC connecté. Ces points de terminaison fournissent un chemin pour les requêtes entrantes ou sortantes :

Point de terminaison entrant : les résolveurs DNS de votre réseau peuvent réacheminer des requêtes DNS vers Route 53 Resolver via ce point de terminaison

> Il existe deux types de points de terminaison entrants : un point de terminaison entrant par défaut qui transmet aux adresses IP et un point de terminaison entrant de délégation qui délègue l'autorité d'un sous-domaine hébergé dans la zone hébergée privée Route 53 au résolveur Route 53. Les points de terminaison entrants permettent à vos résolveurs DNS de résoudre facilement les noms de domaine pour des AWS ressources telles que des EC2 instances ou des enregistrements dans une zone hébergée privée Route 53. Pour de plus amples informations, veuillez consulter Comment les résolveurs DNS de votre réseau réacheminent les requêtes DNS vers les points de terminaison Route 53 Resolver.

Point de terminaison sortant : Resolver réachemine de manière conditionnelle les requêtes aux résolveurs de votre réseau via ce point de terminaison

Pour réacheminer les requêtes sélectionnées, créez des règles Resolver qui spécifient les noms de domaine pour les requêtes DNS que vous souhaitez réacheminer (par exemple, exemple.com) et les adresses IP des résolveurs DNS de votre réseau vers lesquels vous voulez réacheminer les requêtes. Si une requête correspond à plusieurs règles (exemple.com, acme.exemple.com), Resolver choisit la règle ayant la correspondance la plus spécifique (acme.exemple.com) et réachemine la requête vers les adresses IP que vous avez indiquées dans cette règle. Il existe trois types de règles : les règles directes, les règles de système et les règles de délégation. Pour de plus amples informations, veuillez consulter Comment le point de terminaison Route 53 Resolver transfère les requêtes DNS de vous VPCs vers votre réseau.

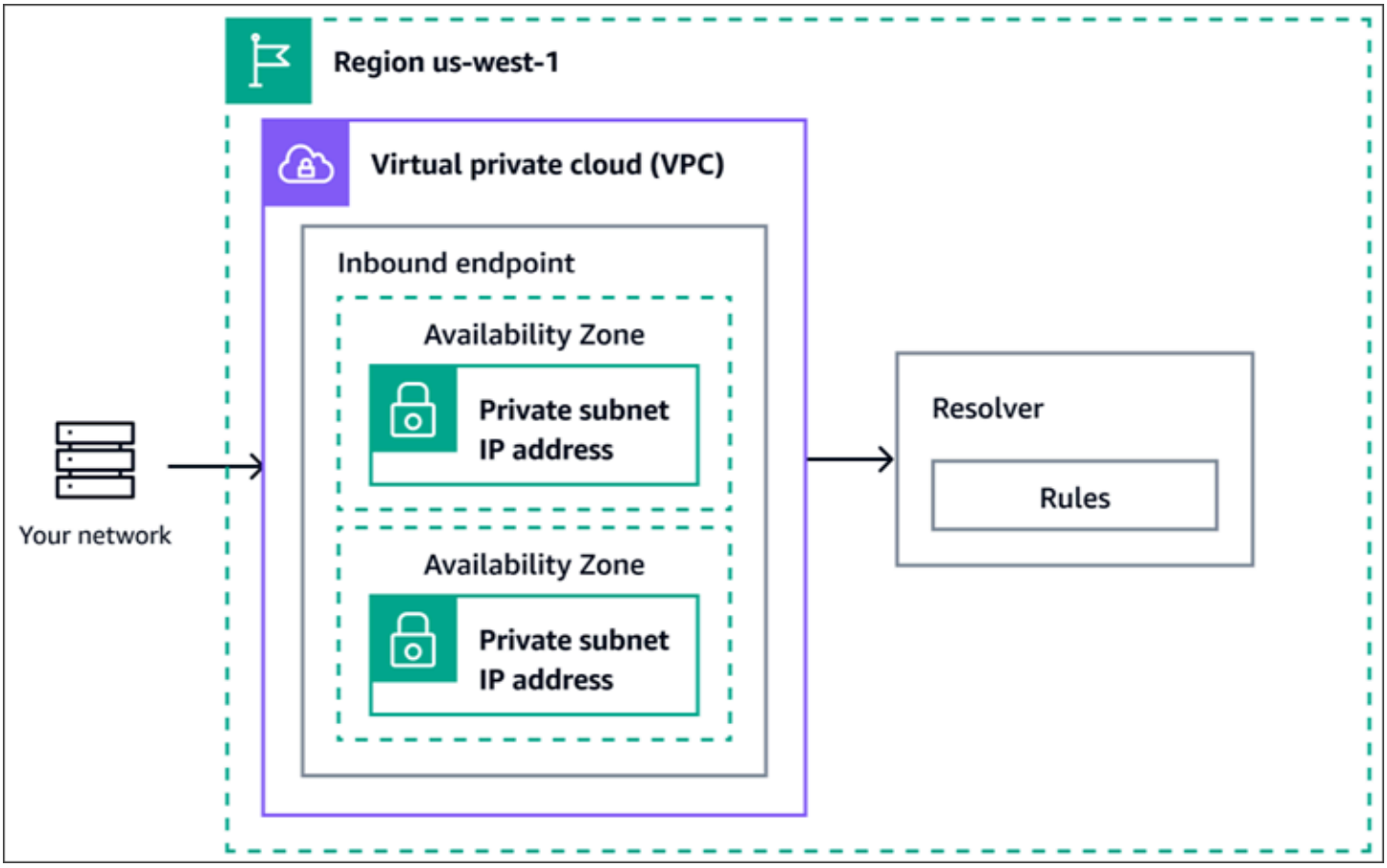
Comme Amazon VPC, Resolver est régional. Dans chaque région où vous vous trouvez VPCs, vous pouvez choisir de transférer les requêtes de votre réseau VPCs vers votre réseau (requêtes sortantes), de votre réseau vers votre VPCs (requêtes entrantes), ou les deux.

Vous ne pouvez pas créer de points de terminaison de résolveur dans un VPC dont vous n'êtes pas le propriétaire. Seul le propriétaire du VPC peut créer des ressources de niveau VPC telles que des points de terminaison entrants.

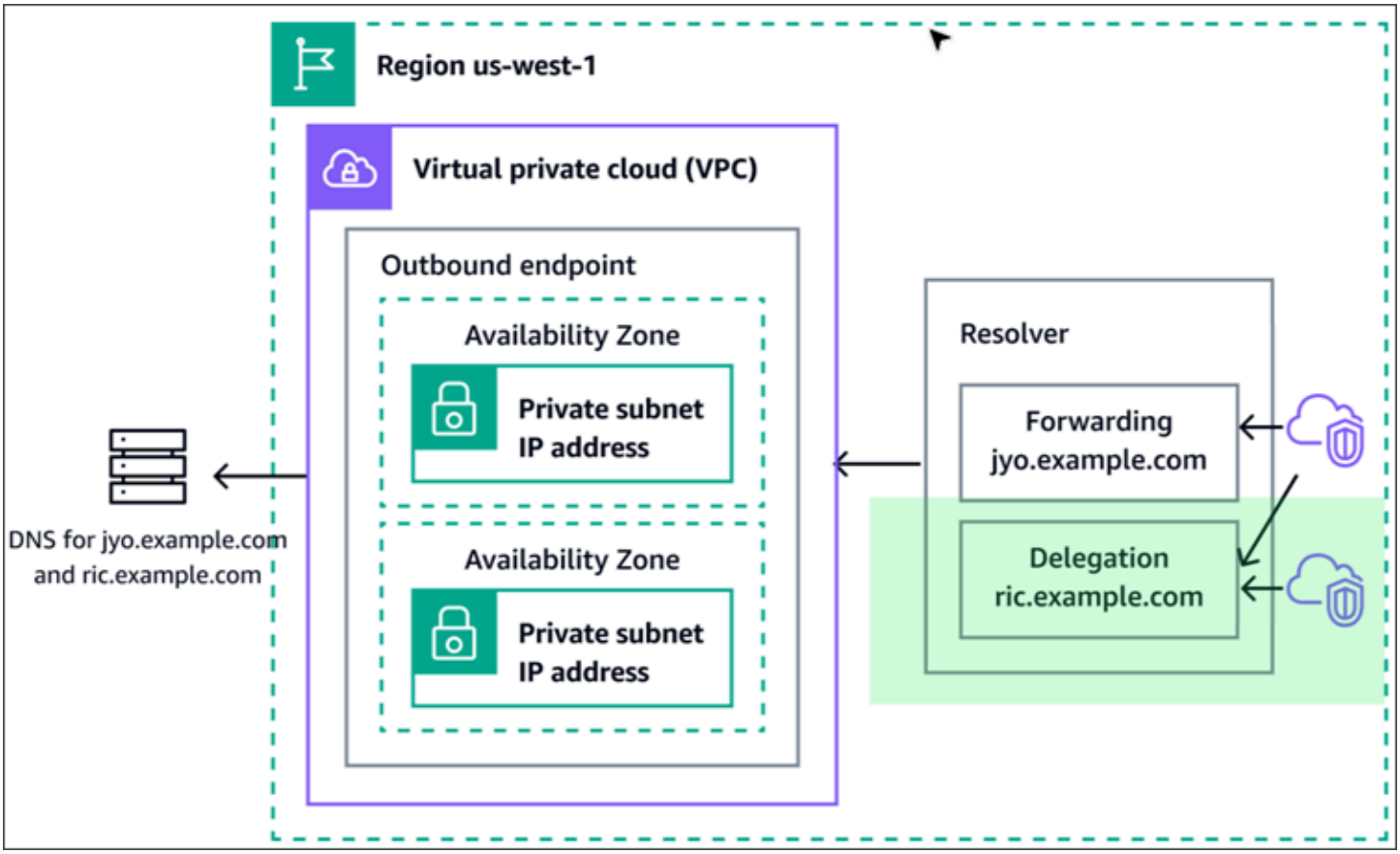
> **Note**
>
> Lorsque vous créez un point de terminaison Resolver, vous ne pouvez pas indquer un VPC doté de l'attribut de location d'instance défini sur `dedicated`. Pour plus d'informations, veuillez consulter .

Pour utiliser le réacheminement entrant ou sortant, créez un point de terminaison Resolver dans votre VPC. Dans le cadre de la définition d'un point de terminaison, vous spécifiez les adresses IP, ou délégation DNS, vers lesquelles vous souhaitez transférer les requêtes DNS entrantes ou les adresses IP dont vous souhaitez que les requêtes sortantes proviennent. Pour chaque adresse IP et délégation que vous spécifiez, Resolver crée automatiquement une interface VPC Elastic network.

Le diagramme suivant montre le chemin d'une requête DNS à partir d'un résolveur DNS sur votre réseau vers les points de terminaison Route 53 Resolver.



Le schéma suivant montre le chemin d'une requête DNS depuis une EC2 instance de l'un de vous VPCs vers un résolveur DNS de votre réseau. Le domaine jyo.example.com utilise une règle de transfert, tandis que le sous-domaine ric.example.com a délégué l'autorité de transfert à Route 53 Resolver.



Pour une présentation des interfaces réseau VPC, veuillez consulter Interfaces réseau Elastic dans le Guide de l'utilisateur Amazon VPC.

Rubriques

- Comment les résolveurs DNS de votre réseau réacheminent les requêtes DNS vers les points de terminaison Route 53 Resolver
- Comment le point de terminaison Route 53 Resolver transfère les requêtes DNS de vous VPCs vers votre réseau
- Considérations lors de la création de points de terminaison entrants et sortants

Comment les résolveurs DNS de votre réseau réacheminent les requêtes DNS vers les points de terminaison Route 53 Resolver

Pour transférer les requêtes DNS de votre réseau vers Route 53 Resolver, vous devez créer des points de terminaison entrants dans une région. AWS Il existe deux catégories de points de terminaison entrants : les points par défaut et les points de terminaison délégués.

Étapes de création de points de terminaison entrants par défaut

1. Vous créez un point de terminaison entrant du résolveur Route 53 par défaut dans un VPC et vous spécifiez les adresses IP auxquelles les résolveurs de votre réseau transmettent les requêtes DNS. Pour obtenir des instructions, consultez Configuration du réacheminement entrant.

   Pour chaque adresse IP que vous indiquez pour le point de terminaison entrant, Resolver crée une interface réseau Elastic VPC dans le VPC dans lequel vous avez créé le point de terminaison entrant.
2. Configurez les résolveurs sur votre réseau pour réacheminer les requêtes DNS pour les noms de domaine applicables vers les adresses IP indiquées dans le point de terminaison entrant. Pour de plus amples informations, veuillez consulter Considérations lors de la création de points de terminaison entrants et sortants.

Voici comment Resolver résout les requêtes DNS provenant de votre réseau via un point de terminaison entrant par défaut :

1. Un navigateur web ou une autre application de votre réseau envoie une requête DNS pour un nom de domaine que vous avez réacheminé vers Resolver.
2. Un résolveur de votre réseau réachemine la requête vers les adresses IP de votre point de terminaison entrant.
3. Le point de terminaison entrant réachemine la requête vers Resolver.
4. Resolver obtient la valeur applicable pour le nom de domaine dans la requête DNS, soit en interne ou en effectuant une recherche récursive sur les serveurs de noms publics.
5. Le résolveur renvoie la valeur au point de terminaison entrant.
6. Le point de terminaison entrant renvoie la valeur au résolveur de votre réseau.
7. Le résolveur de votre réseau renvoie la valeur à l'application.
8. À l'aide de la valeur renvoyée par Resolver, l'application envoie une demande, par exemple une demande pour un objet dans un compartiment Amazon S3.

Étapes de création de points de terminaison entrants de délégation

1. Vous créez un point de terminaison entrant Route 53 Resolver de délégation dans un VPC. Pour obtenir des instructions, consultez Configuration du réacheminement entrant.

Pour chaque adresse IP que vous indiquez pour le point de terminaison entrant, Resolver crée une interface réseau Elastic VPC dans le VPC dans lequel vous avez créé le point de terminaison entrant.

2. Vous configurez des résolveurs sur votre réseau pour déléguer les requêtes DNS pour les noms de domaine applicables à Route 53 Resolver. Pour les enregistrements Glue, vous devez saisir les adresses IP des points de terminaison entrants. Pour de plus amples informations, veuillez consulter Considérations lors de la création de points de terminaison entrants et sortants.

Voici comment Resolver résout les requêtes DNS provenant de votre réseau via un point de terminaison entrant de délégation :

1. Comme condition préalable, vous devez déléguer le sous-domaine hébergé dans la zone hébergée privée depuis le local. Comme vous déléguez le sous-domaine via le point de terminaison de délégation entrant, vous utilisez les adresses IP du point de terminaison entrant comme enregistrements de référence pour le sous-domaine délégué.

   > **Note**
   >
   > Vous devrez peut-être également inclure les enregistrements de colle pour vous assurer que la requête DNS peut être résolue. Si vous déléguez un sous-domaine à des serveurs de noms situés dans la même zone que le domaine parent, des enregistrements collés sont nécessaires.

2. Un navigateur Web ou une autre application de votre réseau envoie une requête DNS pour un nom de domaine que vous avez délégué au résolveur Route 53.
3. Un résolveur de votre réseau réachemine la requête vers les adresses IP de votre point de terminaison entrant.
4. Le point de terminaison entrant délègue la requête à Resolver.
5. Le résolveur renvoie l'adresse de la AWS ressource depuis la zone hébergée privée vers le point de terminaison entrant.
6. Le point de terminaison entrant renvoie la valeur au résolveur de votre réseau.
7. Le résolveur de votre réseau renvoie la valeur à l'application.
8. À l'aide de la valeur renvoyée par Resolver, l'application envoie une demande, par exemple une demande pour un objet dans un compartiment Amazon S3.

La création d'un point de terminaison entrant ne modifie pas le comportement de Resolver, elle fournit simplement un chemin entre un emplacement extérieur au AWS réseau et Resolver.

Comment le point de terminaison Route 53 Resolver transfère les requêtes DNS de vous VPCs vers votre réseau

Lorsque vous souhaitez transférer des requêtes DNS depuis les EC2 instances d'une ou de plusieurs instances VPCs d'une AWS région vers votre réseau, vous devez effectuer les étapes suivantes.

1. Créez un point de terminaison sortant Route 53 Resolver dans un VPC et spécifiez plusieurs valeurs :
   - Le VPC par lequel vous voulez que les requêtes DNS transitent lors de leur transfert vers les résolveurs de votre réseau.
   - Un groupe de sécurité VPC

   Pour chaque adresse IP que vous spécifiez pour le point de terminaison sortant, Resolver crée une interface réseau Elastic Amazon VPC dans le VPC que vous indiquez. Pour de plus amples informations, veuillez consulter Considérations lors de la création de points de terminaison entrants et sortants.
2. Vous créez une ou plusieurs règles, qui spécifient les noms de domaine des requêtes DNS que vous souhaitez déléguer à Resolver pour les transférer, ou que Resolver transfère aux résolveurs de votre réseau. Pour les règles de transfert, vous spécifiez également les adresses IP des résolveurs. Pour de plus amples informations, veuillez consulter Utilisation de règles pour contrôler les requêtes qui sont réacheminées vers votre réseau.
3. Vous associez chaque règle à celle VPCs pour laquelle vous souhaitez transférer les requêtes DNS vers votre réseau.

Utilisation de règles pour contrôler les requêtes qui sont réacheminées vers votre réseau

Les règles déterminent les requêtes DNS que le point de terminaison Route 53 Resolver réachemine vers les résolveurs DNS de votre réseau, et les requêtes que Resolver traite directement.

Vous pouvez classer les règles de deux façons. Par exemple, par l'auteur des règles :

- Règles définies automatiquement — Resolver crée automatiquement des règles définies automatiquement et associe les règles à vos. VPCs La plupart de ces règles s'appliquent aux noms

de domaine AWS spécifiques pour lesquels Resolver répond aux requêtes. Pour de plus amples informations, veuillez consulter Noms de domaine pour lesquels Resolver crée des règles système autodéfinies.

- Règles personnalisées : vous créez des règles personnalisées et vous les associez à VPCs. Actuellement, vous pouvez créer deux types de règles personnalisées : les règles de transfert conditionnelles, également appelées règles de transfert, et les règles de délégation. Les règles de transfert obligent Resolver à transférer les requêtes DNS de vous VPCs vers les adresses IP des résolveurs DNS de votre réseau.

  Si vous créez une règle de réacheminement pour le même domaine qu'une règle autodéfinie, Resolver réachemine les requêtes pour ce nom de domaine vers les résolveurs DNS de votre réseau selon les paramètres de la règle de réacheminement.

  Les règles de délégation transmettent les requêtes DNS avec les enregistrements de délégation figurant dans la règle de délégation qui correspondent aux enregistrements NS en réponse aux résolveurs de votre réseau.

Les règles peuvent aussi être classées selon leur action :

- Règles de réacheminement conditionnel - Vous créez des règles de réacheminement conditionnel (également appelées règles de réacheminement) lorsque vous souhaitez réacheminer les requêtes DNS pour des noms de domaine indiqués vers les résolveurs DNS de votre réseau.
- Règles système - Les règles système conduisent Resolver à remplacer de façon sélective le comportement défini dans une règle de réacheminement. Lorsque vous créez une règle système, Resolver résout les requêtes DNS pour les sous-domaines indiqués, qui seraient sinon résolues par les résolveurs DNS de votre réseau.

  Par défaut, les règles de réacheminement s'appliquent à un nom de domaine et à tous ses sous-domaines. Si vous souhaitez réacheminer les requêtes d'un domaine vers un résolveur de votre réseau, mais pas celles de certains sous-domaines, créez une règle système pour les sous-domaines. Par exemple, si vous créez une règle de réacheminement pour exemple.com, mais que vous ne voulez pas réacheminer les requêtes pour acme.exemple.com, créez une règle système et indiquez acme.exemple.com pour le nom de domaine.
- Règle récursive - Resolver crée automatiquement une règle récursive nommée Internet Resolver (Résolveur Internet). Avec cette règle, Route 53 Resolver agit en tant que résolveur récursif pour tous les noms de domaine pour lesquels vous n'avez pas créé de règles personnalisées et pour lesquels Resolver n'a pas créé de règles autodéfinies. Pour plus d'informations sur la façon de

remplacer ce comportement, consultez la section « Réacheminement de toutes les requêtes vers votre réseau » dans la suite de cette rubrique.

Vous pouvez créer des règles personnalisées qui s'appliquent à des noms de domaine spécifiques (le vôtre ou la plupart des noms de AWS domaine), aux noms de AWS domaines publics ou à tous les noms de domaine.

Réacheminement de requêtes pour des noms de domaines spécifiques vers votre réseau

Pour réacheminer les requêtes pour un nom de domaine spécifique, par exemple exemple.com, vers votre réseau, créez une règle et spécifiez ce nom de domaine. Pour les règles de transfert, vous spécifiez également les adresses IP des résolveurs DNS de votre réseau auxquels vous souhaitez transférer les requêtes ou, pour les règles de délégation, vous créez l'enregistrement de délégation pour lequel vous souhaitez déléguer l'autorité à des résolveurs sur site. Vous associez ensuite chaque règle à celle VPCs pour laquelle vous souhaitez transférer les requêtes DNS vers votre réseau. Par exemple, vous pouvez créer des règles distinctes pour exemple.com, exemple.org et exemple.net. Vous pouvez ensuite associer les règles VPCs à celles d'une AWS région dans n'importe quelle combinaison.

Réacheminement des requêtes pour amazonaws.com vers votre réseau

Le nom de domaine amazonaws.com est le nom de domaine public pour les AWS ressources telles que les EC2 instances et les compartiments S3. Si vous souhaitez transférer des requêtes pour amazonaws.com vers votre réseau, créez une règle, spécifiez amazonaws.com pour le nom de domaine et spécifiez Forward ou Delegation pour le type de règle en fonction de la méthode que vous souhaitez utiliser.

> **Note**
>
> Resolver ne réachemine pas automatiquement les requêtes DNS pour certains sous-domaines amazonaws.com, même si vous créez une règle de réacheminement pour amazonaws.com. Pour plus d'informations, veuillez consulter Noms de domaine pour lesquels Resolver crée des règles système autodéfinies. Pour plus d'informations sur la façon de remplacer ce comportement, consultez la section "Réacheminement de toutes les requêtes vers votre réseau" ci-dessous.

Réacheminement de toutes les requêtes vers votre réseau

Si vous souhaitez transférer toutes les requêtes vers votre réseau, vous devez créer une règle, en spécifiant «. » (point) pour le nom de domaine, et associez la règle à VPCs celle pour laquelle vous souhaitez transférer toutes les requêtes DNS vers votre réseau. Le résolveur ne transmet toujours pas toutes les requêtes DNS à votre réseau, car l'utilisation d'un résolveur DNS extérieur AWS perturberait certaines fonctionnalités. Par exemple, certains noms de AWS domaine internes comportent des plages d'adresses IP internes qui ne sont pas accessibles de l'extérieur AWS. Pour obtenir la liste des noms de domaine pour lesquels les requêtes ne sont pas réacheminées vers votre réseau lorsque vous créez une règle pour « . », consultez Noms de domaine pour lesquels Resolver crée des règles système autodéfinies.

Toutefois, les règles système autodéfinies pour le DNS inverse peuvent être désactivées, ce qui permet à la règle « . » de transférer toutes les requêtes DNS inverses vers votre réseau. Pour plus d'informations sur la désactivation des règles autodéfinies, veuillez consulter Règles de transfert pour les requêtes DNS inverses dans Resolver.

Si vous souhaitez essayer de réacheminer les requêtes DNS pour tous les noms de domaine vers votre réseau, y compris les noms de domaine exclus du réacheminement par défaut, vous pouvez créer une règle « . » et effectuer l'une des actions suivantes :

- Définissez l'indicateur `enableDnsHostnames` pour le VPC sur `false`
- Créez des règles pour les noms de domaine répertoriés dans Noms de domaine pour lesquels Resolver crée des règles système autodéfinies

> **Important**
>
> Si vous réacheminez tous les noms de domaine vers votre réseau, y compris les noms de domaine que Resolver exclut lorsque vous créez une règle « . », certaines fonctionnalités peuvent cesser de fonctionner.

Comment Resolver détermine si le nom de domaine d'une requête correspond aux règles

Route 53 Resolver compare le nom de domaine de la requête DNS au nom de domaine des règles associées au VPC dont la requête provient. Resolver considère que les noms de domaine correspondent dans les cas suivants :

- Les noms de domaine sont identiques.
- Le nom de domaine de la requête est un sous-domaine du nom de domaine de la règle.

Par exemple, si le nom de domaine de la règle est acme.exemple.com, Resolver considère que les noms de domaine suivants identifiés dans une requête DNS correspondent :

- acme.exemple.com
- zenith.acme.exemple.com

Les noms de domaine suivants ne correspondent pas :

- exemple.com
- nadir.exemple.com

Si le nom de domaine d'une requête correspond au nom de domaine de plusieurs règles (par exemple exemple.com et www.exemple.com), Resolver achemine les requêtes DNS sortantes à l'aide de la règle qui contient le nom de domaine le plus spécifique (www.exemple.com).

Comment Resolver détermine la destination du réacheminement des requêtes DNS

Lorsqu'une application exécutée sur une EC2 instance dans un VPC envoie une requête DNS, Route 53 Resolver exécute les étapes suivantes :

1. Resolver vérifie les noms de domaine dans les règles.

   Si le nom de domaine d'une requête correspond au nom de domaine d'une règle de transfert par défaut, Resolver transmet la requête à l'adresse IP que vous avez spécifiée lors de la création du point de terminaison sortant. Le point de terminaison sortant transmet ensuite la requête aux adresses IP des résolveurs de votre réseau, que vous avez spécifiées lorsque vous avez créé la règle.

   Si l'enregistrement de délégation en réponse correspond à la règle de délégation, le résolveur délègue l'autorité aux résolveurs sur site via le point de terminaison sortant associé à la règle de délégation.

   Pour de plus amples informations, veuillez consulter Comment Resolver détermine si le nom de domaine d'une requête correspond aux règles.
2. Le point de terminaison Resolver réachemine les requêtes DNS en fonction des paramètres de la règle « . ».

Si le nom de domaine d'une requête ne correspond pas au nom de domaine des autres règles, Resolver réachemine la requête en fonction des paramètres de la règle autodéfinie « . » (point). La règle des points s'applique à tous les noms de domaine, à l'exception de certains noms de domaine AWS internes et de certains noms d'enregistrement dans des zones hébergées privées. Cette règle conduit Resolver à réacheminer les requêtes DNS vers des serveurs de noms publics si les noms de domaine des requêtes ne correspondent à aucun nom des règles de réacheminement personnalisées. Si vous voulez transférer toutes les requêtes vers les résolveurs DNS de votre réseau, vous pouvez créer une règle de réacheminement personnalisée. Spécifiez « . » pour le nom de domaine, Forwarding (Réacheminement) pour le Type (Type), ainsi que les adresses IP des résolveurs.

3. Resolver renvoie la réponse à l'application qui a envoyé la requête.

Utilisation des règles dans plusieurs régions

Route 53 Resolver étant un service régional, les objets que vous créez dans une AWS région ne sont disponibles que dans cette région. Pour utiliser la même règle dans plusieurs régions, vous devez créer la règle dans chaque région.

Le AWS compte qui a créé une règle peut partager la règle avec d'autres AWS comptes. Pour de plus amples informations, veuillez consulter Partage des règles du résolveur avec d'autres AWS comptes et utilisation de règles partagées.

Noms de domaine pour lesquels Resolver crée des règles système autodéfinies

Resolver crée automatiquement des règles systèmes autodéfinies, qui définissent la façon dont les requêtes sont résolues par défaut pour les domaines sélectionnés :

- Pour les zones hébergées privées et pour les noms de EC2 domaine spécifiques à Amazon (tels que compute.amazonaws.com et compute.internal), les règles définies automatiquement garantissent que vos zones et EC2 instances hébergées privées continuent de se résoudre si vous créez des règles de transfert conditionnel pour des noms de domaine moins spécifiques tels que « ». (point) ou « com ».
- Pour les noms de domaines publiquement réservés (comme localhost et 10.in-addr.arpa), les bonnes pratiques DNS recommandent que les réponses aux requêtes soient fournies en local au lieu d'être réacheminées vers les serveurs de noms publics. Voir RFC 6303, Locally Served DNS Zones (RFC 6303, zones DNS servies en local).

> **Note**
>
> Si vous créez une règle de réacheminement conditionnel pour « . » (point) ou « com », nous vous recommandons de créer également une règle système pour amazonaws.com. (Avec les règles système, Resolver résoud localement les requêtes DNS pour des domaines et sous-domaines spécifiques). La création de cette règle système améliore les performances, réduit le nombre de requêtes qui sont réacheminées vers votre réseau et diminue les frais de Resolver.

Si vous souhaitez remplacer une règle autodéfinie, vous pouvez créer une règle de réacheminement conditionnel pour le même nom de domaine.

Vous pouvez également désactiver certaines règles définies automatiquement. Pour de plus amples informations, veuillez consulter Règles de transfert pour les requêtes DNS inverses dans Resolver.

Resolver crée les règles autodéfinies suivantes.

Règles pour les zones hébergées privées

Pour chaque zone hébergée privée que vous associez à un VPC, Resolver crée une règle et l'associe au VPC. Si vous associez la zone hébergée privée à plusieurs VPCs, Resolver associe la règle à la même VPCs zone.

La règle dispose d'un type Forward (Réacheminer).

Règles relatives aux différents noms de domaine AWS internes

Toutes les règles pour les noms de domaine internes de cette section sont de type Forward (Réacheminer). Resolver réachemine les requêtes DNS pour ces noms de domaine vers les serveurs de noms faisant autorité pour le VPC.

> **Note**
>
> Resolver crée la plupart de ces règles lorsque vous définissez l'indicateur `enableDnsHostnames` pour un VPC sur `true`. Resolver crée les règles, même si vous n'utilisez pas les points de terminaison Resolver.

Resolver crée les règles autodéfinies suivantes et les associe au VPC lorsque vous définissez l'indicateur `enableDnsHostnames` pour le VPC sur `true` :

- *Region-name*.compute.internal, par exemple, eu-west-1.compute.internal. La région us-east-1 n'utilise pas ce nom de domaine.
- *Region-name*.calculer. *amazon-domain-name*, par exemple, eu-west-1.compute.amazonaws.com ou cn-north-1.compute.amazonaws.com.cn. La région us-east-1 n'utilise pas ce nom de domaine.
- ec2.internal. Seule la région us-east-1 utilise ce nom de domaine.
- compute-1.internal. Seule la région us-east-1 utilise ce nom de domaine.
- compute-1.amazonaws.com. Seule la région us-east-1 utilise ce nom de domaine.

Les règles autodéfinies suivantes servent à la recherche DNS inverse pour les règles que Resolver crée lorsque vous définissez l'indicateur `enableDnsHostnames` pour le VPC sur `true`.

- 10.in-addr.arpa
- 16.172.in-addr.arpa via 31.172.in-addr.arpa
- 168.192.in-addr.arpa
- 254.169.254.169.in-addr.arpa
- Règles pour chacune des plages d'adresses CIDR pour le VPC. Par exemple, pour un VPC ayant une plage d'adresses CIDR de 10.0.0.0/23, Resolver crée les règles suivantes :
  - 0.0.10.in-addr.arpa
  - 1.0.10.in-addr.arpa

Les règles autodéfinies suivantes, pour les domaines associés à localhost, sont également créées et associées à un VPC lorsque vous définissez l'indicateur `enableDnsHostnames` pour le VPC sur `true` :

- localhost
- localdomain
- 127.in-addr.arpa
- 1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa
- 0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa

Resolver crée les règles autodéfinies suivantes et les associe à votre VPC lorsque vous connectez le VPC à un autre VPC via une passerelle de transit ou un appairage de VPC, et avec la prise en charge de DNS activée :

- La recherche DNS inverse pour les plages d'adresses IP du VPC appairé, par exemple, 0.192.in-addr.arpa

Si vous ajoutez un bloc IPv4 CIDR à un VPC, Resolver ajoute une règle définie automatiquement pour la nouvelle plage d'adresses IP.

- Si l'autre VPC est dans une autre région, les noms de domaine suivants :
  - *Region-name*.compute.interne. La région us-east-1 n'utilise pas ce nom de domaine.
  - *Region-name*.calculer. *amazon-domain-name*. La région us-east-1 n'utilise pas ce nom de domaine.
  - ec2.internal. Seule la région us-east-1 utilise ce nom de domaine.
  - compute-1.amazonaws.com. Seule la région us-east-1 utilise ce nom de domaine.

Une règle pour tous les autres domaines

Resolver crée une règle « . » (point) qui s'applique à tous les noms de domaine qui ne sont pas indiqués plus haut dans cette rubrique. La règle « . » dispose d'un type Recursive (Récursif), ce qui signifie que la règle conduit Resolver à agir en tant que résolveur récursif.

Considérations lors de la création de points de terminaison entrants et sortants

Avant de créer des points de terminaison de résolution entrants et sortants dans une AWS région, prenez en compte les points suivants.

Rubriques

- Nombre de points de terminaison entrants et sortants dans chaque région
- Utilisation du même VPC pour les points de terminaison entrants et sortants
- Points de terminaison entrants et zones hébergées privées
- Appairage de VPC
- Adresses IP dans des sous-réseaux partagés
- Connexion entre votre réseau et le terminal dans VPCs lequel vous créez des points de terminaison
- Lorsque vous partagez des règles, vous partagez également des points de terminaison sortants
- Choisir des protocoles pour les points de terminaison
- Utilisation d'un résolveur configuré pour la location d'instance dédiée VPCs

Nombre de points de terminaison entrants et sortants dans chaque région

Lorsque vous souhaitez intégrer le DNS d'une AWS région VPCs au DNS de votre réseau, vous avez généralement besoin d'un point de terminaison entrant Resolver (pour les requêtes DNS que vous transférez vers votre VPCs) et d'un point de terminaison sortant (pour les requêtes que vous transférez de votre VPCs vers votre réseau). Vous pouvez créer plusieurs points de terminaison entrants et sortants, mais un seul point de terminaison entrant ou sortant suffit pour traiter les requêtes DNS dans l'une ou l'autre direction. Remarques :

- Pour chaque point de terminaison Resolver, vous spécifiez deux ou plusieurs adresses IP dans différentes zones de disponibilité. Chaque adresse IP dans un point de terminaison peut traiter un grand nombre de requêtes DNS par seconde. (Pour le nombre maximum actuel de requêtes par seconde et par adresse IP dans un point de terminaison, consultez Quotas sur Route 53 Resolver.) Si vous voulez que Resolver traite plus de requêtes, vous pouvez ajouter d'autres adresses IP à votre point de terminaison existant, au lieu d'ajouter un autre point de terminaison.
- La tarification de Resolver est basée sur le nombre d'adresses IP dans vos points de terminaison et sur le nombre de requêtes DNS traitées par le point de terminaison. Chaque point de terminaison inclut un minimum de deux adresses IP. Pour en savoir plus sur la tarification de Resolver, veuillez consulter Tarification Amazon Route 53.
- Chaque règle spécifie le point de terminaison sortant à partir duquel les requêtes DNS sont transférées. Si vous créez plusieurs points de terminaison sortants au sein d'une région AWS et que vous souhaitez associer certaines ou toutes les règles Resolver avec chaque VPC, vous devez créer plusieurs copies de ces règles.

Utilisation du même VPC pour les points de terminaison entrants et sortants

Vous pouvez créer des points de terminaison entrants et sortants dans le même VPC ou dans un autre VPCs dans la même région.

Pour de plus amples informations, veuillez consulter Bonnes pratiques relatives à Amazon Route 53.

Points de terminaison entrants et zones hébergées privées

Si vous voulez que Resolver résolve les requêtes DNS entrantes à l'aide de registres dans une zone hébergée privée, associez la zone hébergée privée avec le VPC dans lequel vous avez créé le point de terminaison entrant. Pour plus d'informations sur l'association de zones hébergées privées à VPCs, consultezUtilisation des zones hébergées privées.

Appairage de VPC

Vous pouvez utiliser n'importe quel VPC d'une AWS région pour un point de terminaison entrant ou sortant, que le VPC que vous choisissez soit apparié ou non à un autre. VPCs Pour en savoir plus, consultez Amazon Virtual Private Cloud VPC Peering.

Adresses IP dans des sous-réseaux partagés

Lorsque vous créez un point de terminaison entrant ou sortant, vous pouvez spécifier une adresse IP dans un sous-réseau partagé uniquement si le compte actuel a créé le VPC. Si un autre compte crée un VPC et partage un sous-réseau dans le VPC avec votre compte, vous ne pouvez pas spécifier d'adresse IP dans ce sous-réseau. Pour plus d'informations sur les sous-réseaux partagés, consultez la section Travailler avec le partage VPCs dans le guide de l'utilisateur Amazon VPC.

Connexion entre votre réseau et le terminal dans VPCs lequel vous créez des points de terminaison

Vous devez disposer de l'une des connexions suivantes entre votre réseau et le point de terminaison dans VPCs lequel vous créez :

- Points de terminaison entrants - Vous devez configurer une connexion AWS Direct Connect ou une connexion VPN entre votre réseau et chaque VPC pour lequel vous créez un point de terminaison entrant.
- Points de terminaison sortants - Vous devez configurer une connexion AWS Direct Connect, une connexion VPN ou une passerelle de traduction d'adresse réseau (NAT) entre votre réseau et chaque VPC pour lequel vous créez un point de terminaison sortant.

Lorsque vous partagez des règles, vous partagez également des points de terminaison sortants

Lorsque vous créez une règle, vous spécifiez le point de terminaison sortant que vous voulez que Resolver utilise pour réacheminer les requêtes DNS vers votre réseau. Si vous partagez la règle avec un autre AWS compte, vous partagez également indirectement le point de terminaison sortant que vous spécifiez dans la règle. Si vous avez utilisé plusieurs AWS comptes pour créer un compte VPCs dans une AWS région, vous pouvez effectuer les opérations suivantes :

- Créer un point de terminaison sortant dans la région.
- Créez des règles à l'aide d'un seul AWS compte.

- Partagez les règles avec tous les AWS comptes créés VPCs dans la région.

Cela vous permet d'utiliser un point de terminaison sortant dans une région pour transférer des requêtes DNS à votre réseau à partir de plusieurs, VPCs même si VPCs elles ont été créées à l'aide de AWS comptes différents.

Choisir des protocoles pour les points de terminaison

Les protocoles de point de terminaison déterminent la manière dont les données sont transmises à un point de terminaison entrant et à partir d'un point de terminaison sortant. Le chiffrement des requêtes DNS pour le trafic VPC n'est pas nécessaire, car chaque flux de paquets sur le réseau est autorisé individuellement selon une règle permettant de valider la source et la destination correctes avant d'être transmis et livré. Il est hautement improbable que des informations passent arbitrairement d'une entité à l'autre sans l'autorisation spécifique de l'entité émettrice et réceptrice. Si un paquet est acheminé vers une destination sans règle qui lui correspond, le paquet est abandonné. Pour plus d'informations, consultez Fonctionnalités VPC.

Les protocoles disponibles sont :

- Do53 : DNS sur le port 53. Les données sont relayées à l'aide du Route 53 Resolver sans chiffrement supplémentaire. Bien que les données ne puissent pas être lues par des tiers, elles peuvent être consultées au sein des AWS réseaux. Utilise UDP ou TCP pour envoyer les paquets. Do53 est principalement utilisé pour le trafic au sein d'Amazon et entre Amazon VPCs. Il s'agit actuellement du seul protocole disponible pour les points de terminaison entrants de délégation.
- DoH : Les données sont transmises via une session HTTPS chiffrée. Le DoH ajoute un niveau de sécurité supplémentaire selon lequel les données ne peuvent pas être déchiffrées par des utilisateurs non autorisés et ne peuvent être lues par personne d'autre que le destinataire prévu. Non disponible pour les points de terminaison entrants de délégation.
- DOH-FIPS : Les données sont transmises via une session HTTPS chiffrée conforme à la norme de chiffrement FIPS 140-2. Pris en charge uniquement pour les points de terminaison entrants. Pour plus d'informations, veuillez consulter FIPS PUB 140-2. Non disponible pour les points de terminaison entrants de délégation.

Pour un point de terminaison entrant de type Forward, vous pouvez appliquer les protocoles comme suit :

- Do53 et DoH en combinaison.

- Do53 et DoH-FIPS en combinaison.
- Do53 uniquement.
- DoH uniquement.
- DoH-FIPS uniquement.
- Aucun, qui est traité comme Do53.

Pour un point de terminaison sortant, vous pouvez appliquer les protocoles comme suit :

- Do53 et DoH en combinaison.
- Do53 uniquement.
- DoH uniquement.
- Aucun, qui est traité comme Do53.

Voir aussi Valeurs à spécifier lors de la création ou de la modification de points de terminaison entrants et Valeurs à spécifier lors de la création ou de la modification de points de terminaison sortants.

Utilisation d'un résolveur configuré pour la location d'instance dédiée VPCs

Lorsque vous créez un point de terminaison Resolver, vous ne pouvez pas indiquer un VPC doté de l'attribut de location d'instance défini sur `dedicated`. Resolver ne s'exécute pas sur un matériel à utilisateur unique.

Vous pouvez toujours utiliser Resolver pour résoudre les requêtes DNS provenant d'un VPC. Créez au moins un VPC doté de l'attribut de location d'instance défini sur `default`, et spécifiez ce VPC lorsque vous créez des points de terminaison entrants et sortants.

Lorsque vous créez une règle de réacheminement, vous pouvez l'associer à n'importe quel VPC, quelle que soit la valeur de l'attribut de location d'instance.

Disponibilité et évolutivité du résolveur Route 53

Amazon Route 53 Resolver, exécuté sur l'adresse Amazon VPC CIDR + 2 et fd00:ec2 : :253, est disponible par défaut dans tous les domaines et répond de manière récursive aux requêtes DNS concernant les enregistrements publics VPCs, les noms DNS spécifiques à Amazon VPC et les zones hébergées privées Route 53. Le résolveur Route 53 comprend deux composants hautement

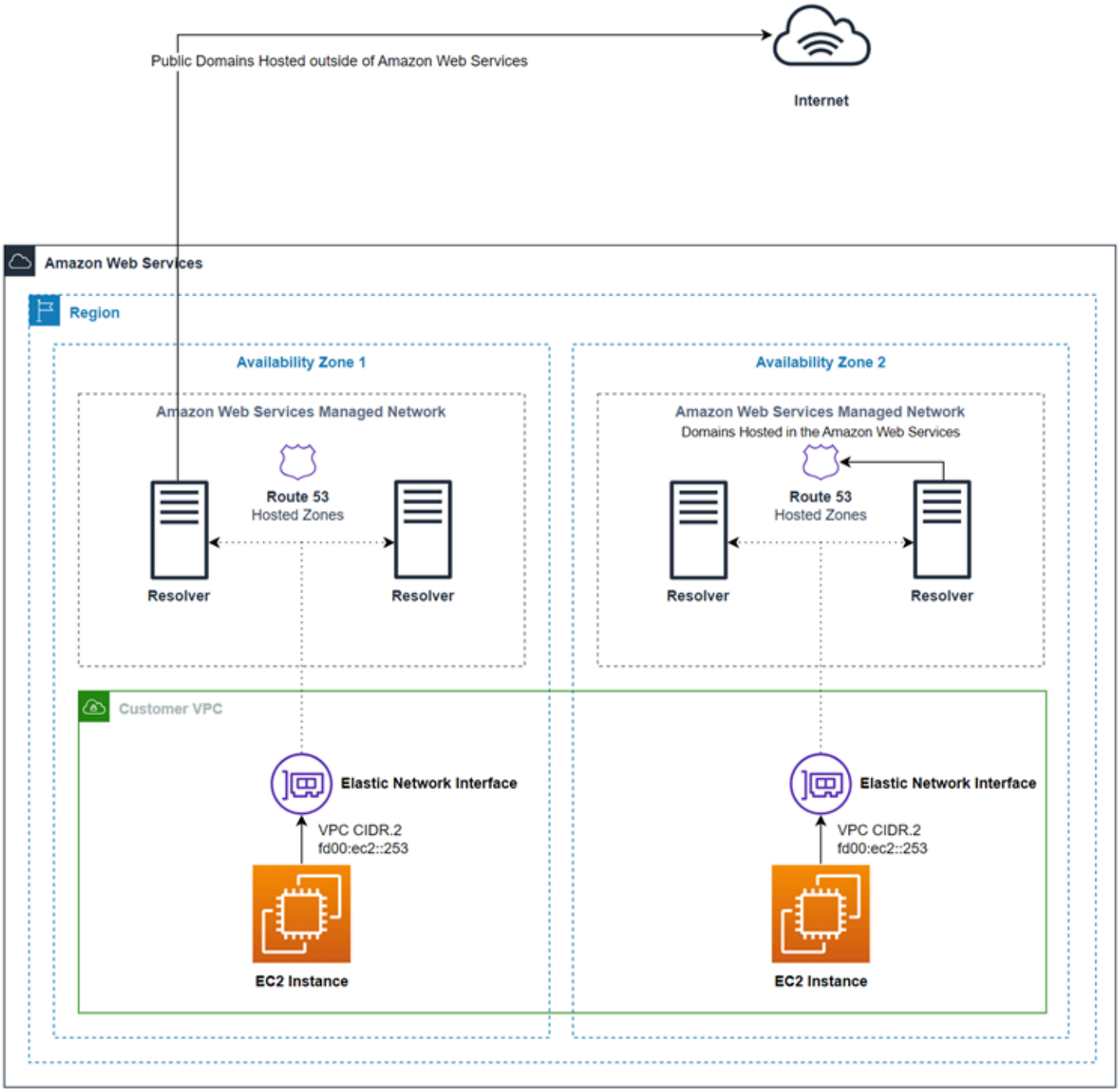
disponibles, transparents pour les utilisateurs : le service Nitro Resolver et le parc de résolveurs zonaux. Le service Nitro Resolver est un service qui s'exécute sur la carte Nitro sur les instances Nitro et dans Dom0 sur les instances d'ancienne génération, et qui consomme les paquets adressés au résolveur Route 53 localement sur le serveur hôte. Pour plus d'informations, consultez La conception de la sécurité du système AWS Nitro.

Le service Nitro Resolver contient un cache local qui peut aider à réduire la latence en répondant aux requêtes répétées effectuées sur une courte période par une instance. Lorsque le service Nitro Resolver reçoit une requête pour laquelle il n'a pas de réponse mise en cache, il la transmet au parc de résolveurs zonaux, un parc de résolveurs à haute disponibilité situé généralement dans la même zone de disponibilité que l'instance. En cas de défaillance du traitement des requêtes par les serveurs de noms en amont ou par d'autres composants du chemin, le service Nitro Resolver est souvent en mesure de gérer ces défaillances de manière transparente sans impact sur les charges de travail exécutées sur l'instance. En outre, si le résolveur rencontre des délais d'attente, des connexions refusées ou des SERVFAILS provenant des serveurs de noms du domaine, il peut répondre par une réponse mise en cache au-delà de la valeur Time-To-Live (TTL) afin d'améliorer la disponibilité. Les requêtes entre le service Nitro Resolver et la flotte de Zonal Resolver sont limitées à un réseau étroitement contrôlé en dehors du VPC du client, qui est inaccessible aux clients et soumis à des contrôles de sécurité rigoureux. En gérant les requêtes entre le service Nitro Resolver et le parc Zonal Resolver en dehors du VPC, les clients ne peuvent pas intercepter les requêtes DNS au sein de leur VPC. Les requêtes destinées à des serveurs de noms extérieurs AWS traverseront l'Internet public, en provenance d'adresses IP publiques appartenant au parc de résolveurs zonaux. Nous ne prenons pas en charge l'attribut EDNS0-client Subnet aujourd'hui, ce qui signifie que toutes les requêtes destinées aux serveurs de noms DNS publics n'incluent pas d'informations sur l'adresse IP du client d'origine.

Le service Nitro Resolver fait partie des services Link-Local de l'instance. Les services Link-Local incluent Route 53 Resolver, Amazon Time Service (NTP), Instance Metadata Service (IMDS) et Windows Licensing Service (pour les instances Windows). Ces services s'adaptent à chaque interface réseau élastique que vous créez dans votre VPC, et chaque interface réseau autorise 1 024 paquets par seconde (PPS) destinés aux services Link-Local. Les paquets dépassant cette limite sont rejetés. Vous pouvez déterminer si vous avez dépassé cette limite à partir de la `linklocal_allowance_exceeded` valeur renvoyée par ethtool. Pour plus d'informations sur l'outil ethtool, consultez la section Surveiller les performances du réseau pour votre EC2 instance Amazon dans le guide de l' EC2 utilisateur Amazon. Cette métrique peut également être rapportée aux CloudWatch métriques par l' CloudWatchagent. Étant donné que le résolveur Route 53 est implémenté par interface réseau, il évolue et devient plus fiable à mesure que vous ajoutez des

instances dans davantage de zones de disponibilité. Il n'existe aucune limite globale par VPC quant au nombre de requêtes. Le résolveur Route 53 peut donc évoluer dans les limites d'un VPC, qui est intrinsèquement basé sur l'utilisation des adresses réseau (NAU). Pour plus d'informations, consultez la section Utilisation des adresses réseau pour votre VPC dans le guide de l'utilisateur Amazon Virtual Private Cloud.

Le schéma suivant montre une vue d'ensemble de la façon dont Route 53 Resolver résout les requêtes DNS dans les zones de disponibilité.



Mise en route avec Route 53 Resolver

La console Route 53 Resolver inclut un assistant qui vous guide tout au long des étapes suivantes pour démarrer avec Resolver :

- Créer des points de terminaison : entrant, sortant ou les deux.

- Pour les points de terminaison sortants, créez une ou plusieurs règles de réacheminement, qui spécifient les noms de domaine pour lesquels vous souhaitez réacheminer les requêtes DNS vers votre réseau.
- Si vous avez créé un point de terminaison sortant, choisissez le VPC auquel vous voulez associer ces règles.

Pour configurer Route 53 Resolver à l'aide de l'assistant

1. Connectez-vous à la console Resolver AWS Management Console et ouvrez-la à https://console.aws.amazon.com/route53resolver/l'adresse.
2. Sur la page Welcome to Route 53 Revolver (Bienvenue sur Route 53 Resolver), choisissez Configure endpoints (Configurer des points de terminaison).
3. Dans la barre de navigation, choisissez la région dans laquelle vous voulez créer un point de terminaison Resolver.
4. Dans Basic configuration (Configuration de base), choisissez la direction d'acheminement des requêtes DNS :
   - Inbound and outbound (Entrant et sortant) : l'assistant vous guide à travers les paramètres qui vous permettent à la fois de réacheminer les requêtes DNS à partir des résolveurs de votre réseau vers Resolver dans un VPC, et de réacheminer les requêtes indiquées (par exemple, exemple.com ou exemple.net) à partir d'un VPC vers les résolveurs de votre réseau.
   - Inbound only (Entrant uniquement) : l'assistant vous guide à travers les paramètres qui vous permettent de réacheminer les requêtes DNS à partir des résolveurs de votre réseau vers Resolver dans un VPC.
   - Outbound only (Sortant uniquement) : l'assistant vous guide à travers les paramètres qui vous permettent d'acheminer des requêtes spécifiques à partir d'un VPC vers des résolveurs de votre réseau.
5. Choisissez Suivant.
6. Si vous avez choisi Inbound and outbound (Entrant et sortant) ou Inbound only (Entrant uniquement), entrez les valeurs applicables pour configurer un point de terminaison entrant. Passez ensuite à l'étape 7. Pour plus d'informations, veuillez consulter Valeurs à spécifier lors de la création ou de la modification de points de terminaison entrants.

   Si vous avez choisi Outbound only (Sortant uniquement), passez directement à l'étape 7.

7. Entrez les valeurs applicables pour configurer un point de terminaison sortant. Pour plus d'informations, veuillez consulter Valeurs à spécifier lors de la création ou de la modification de points de terminaison sortants.
8. Si vous avez choisi Inbound and outbound (Entrant et sortant) ou Outbound only (Sortant uniquement), entrez les valeurs applicables pour créer une règle. Pour plus d'informations, veuillez consulter Valeurs à spécifier lors de la création ou de la modification de règles.
9. Sur la page Review and create (Vérifier et créer), vérifiez que les paramètres que vous avez indiqués sur les pages précédentes sont corrects. Si nécessaire, choisissez Edit (Modifier) pour la section applicable et mettez à jour les paramètres. Lorsque vous êtes satisfait de vos paramètres, choisissez Submit (Envoyer).

   > **Note**
   >
   > Créer un point de terminaison sortant prend une minute ou deux. Vous ne pouvez pas créer d'autre point de terminaison sortant avant d'avoir créé le premier.

10. Si vous souhaitez créer d'autres règles, consultez Gestion des règles de réacheminement.
11. Si vous avez créé un point de terminaison entrant, configurez les résolveurs DNS sur votre réseau pour réacheminer les requêtes DNS applicables vers les adresses IP de votre point de terminaison entrant. Pour plus d'informations, consultez la documentation de votre application DNS.

Transférer les requêtes DNS entrantes vers votre VPCs

Pour réacheminer les requêtes DNS à partir de votre réseau vers Resolver, créez un point de terminaison entrant. Un point de terminaison entrant spécifie les adresses IP (à partir de la page d'adresses IP disponibles pour votre VPC) vers lesquelles vous souhaitez que les résolveurs DNS de votre réseau transfèrent les requêtes DNS. Ces adresses IP ne sont pas des adresses IP publiques. Par conséquent, pour chaque point de terminaison entrant, vous devez connecter votre VPC à votre réseau à l'aide AWS Direct Connect d'une connexion ou d'une connexion VPN.

Lorsque vous implémentez la délégation entrante, vous déléguez l'autorité DNS pour un sous-domaine de votre infrastructure DNS locale à Route 53 Resolver. Pour configurer correctement cette délégation, vous devez utiliser les adresses IP du point de terminaison entrant comme enregistrements collés (enregistrements NS) sur votre serveur de noms local pour le sous-domaine délégué. Par exemple, si vous déléguez le sous-domaine « aws.example.com » à Route 53 Resolver

via un point de terminaison de délégation entrant avec les adresses IP 10.0.1.100 et 10.0.1.101, vous devez créer des enregistrements NS sur votre serveur DNS local pointant « aws.example.com » vers ces adresses IP. Cela garantit que les requêtes DNS pour le sous-domaine délégué sont correctement acheminées vers le résolveur Route 53 via le point de terminaison entrant, ce qui permet au résolveur de répondre avec des enregistrements provenant de la zone hébergée privée associée.

Configuration du réacheminement entrant

Pour créer un point de terminaison entrant, utilisez la procédure suivante.

Créer un point de terminaison entrant

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le panneau de navigation, choisissez Inbound endpoints (Points de terminaison entrants).
3. Dans la barre de navigation, choisissez la région dans laquelle vous voulez créer un point de terminaison entrant.
4. Choisissez Create inbound endpoint (Créer point de terminaison entrant).
5. Entrez les valeurs applicables. Pour plus d'informations, veuillez consulter Valeurs à spécifier lors de la création ou de la modification de points de terminaison entrants.
6. Choisissez Créer.
7. Configurez les résolveurs DNS sur votre réseau pour réacheminer les requêtes DNS applicables vers les adresses IP de votre point de terminaison entrant. Pour plus d'informations, consultez la documentation de votre application DNS.

Valeurs à spécifier lors de la création ou de la modification de points de terminaison entrants

Lorsque vous créez ou modifiez un point de terminaison entrant, spécifiez les valeurs suivantes :

ID Outpost

Si vous créez le point de terminaison d'un résolveur sur un AWS Outposts VPC, il s'agit AWS Outposts de l'ID.

Nom du point de terminaison

Un nom convivial vous permettant de retrouver facilement le point de terminaison entrant sur le tableau de bord.

Catégorie de terminal

Choisissez par défaut ou Délégation. Lorsque la catégorie est Par défaut, le résolveur de votre réseau transmet les demandes DNS à l'adresse IP du point de terminaison entrant. Lorsque la catégorie est Délégation, l'autorité d'un domaine est déléguée au résolveur Route 53.

VPC dans la région region-name

Toutes les requêtes DNS entrantes à partir de votre réseau transitent via ce VPC lors de leur transfert vers Resolver.

Groupe de sécurité de ce point de terminaison

L'ID d'un ou de plusieurs groupes de sécurité que vous souhaitez utiliser pour contrôler l'accès à ce VPC. Le groupe de sécurité que vous spécifiez doit inclure une ou plusieurs règles entrantes. Les règles entrantes doivent autoriser l'accès TCP et UDP sur le port 53. Si vous utilisez le protocole DoH, vous devrez également autoriser le port 443 dans le groupe de sécurité. Vous ne pouvez pas modifier cette valeur après avoir créé le point de terminaison.

Certaines règles de groupe de sécurité entraînent le suivi de votre connexion et le nombre maximum de requêtes par seconde et par adresse IP pour un point de terminaison entrant peut être inférieur à 1 500. Pour éviter le suivi des connexions causé par un groupe de sécurité, consultez la section Connexions non suivies.

> **Note**
>
> Pour ajouter plusieurs groupes de sécurité, utilisez la AWS CLI commande`create-resolver-endpoint`. Pour de plus amples informations, consultez create-resolver-endpoint.

Pour plus d'informations, consultez Groupes de sécurité pour votre VPC dans le Guide de l'utilisateur Amazon VPC.

Type de point de terminaison

Le type de point de terminaison peut être soit IPv4 IPv6 des adresses IP à double pile. Pour un point de terminaison à double pile, le point de terminaison aura à la fois IPv4 une IPv6 adresse à laquelle votre résolveur DNS sur votre réseau peut transférer les requêtes DNS.

> **Note**
>
> Pour des raisons de sécurité, nous refusons l'accès direct au IPv6 trafic depuis l'Internet public pour toutes les adresses IPv6 IP et à double pile.

Adresses IP

Les adresses IP vers lesquelles vous souhaitez que les résolveurs DNS de votre réseau réacheminent les requêtes DNS. Nous vous demandons de spécifier au moins deux adresses IP pour la redondance. Si vous avez créé un point de terminaison entrant de délégation, utilisez ces adresses IP comme référence pour les enregistrements NS du sous-domaine pour lequel vous souhaitez déléguer l'autorité à Route 53 Resolver. Remarques :

Plusieurs zones de disponibilité

Nous vous recommandons de spécifier des adresses IP dans au moins deux zones de disponibilité. Si vous le souhaitez, vous pouvez spécifier des adresses IP supplémentaires dans ces zones de disponibilité ou dans d'autres.

Adresses IP et interfaces réseau Elastic Amazon VPC

Pour chaque combinaison de zone de disponibilité, sous-réseau, et adresse IP que vous spécifiez, Resolver crée une interface réseau Elastic Amazon VPC. Pour le nombre maximum actuel de requêtes DNS par seconde et par adresse IP dans un point de terminaison, consultez Quotas sur Route 53 Resolver. Pour plus d'informations sur la tarification pour chaque interface réseau Elastic, veuillez consulter la section « Amazon Route 53 » sur la page de tarification d'Amazon Route 53.

> **Note**
>
> Le point de terminaison Resolver possède une adresse IP privée. Ces adresses IP ne changeront pas au cours de la durée de vie d'un point de terminaison.

Pour chaque adresse IP, spécifiez les valeurs suivantes. Chaque adresse IP doit se trouver dans une zone de disponibilité du VPC que vous avez indiquée dans VPC dans la région region-name.

Zone de disponibilité

La zone de disponibilité par laquelle vous voulez que les requêtes DNS transitent lors de leur transfert vers votre VPC. La zone de disponibilité que vous spécifiez doit être configurée avec un sous-réseau.

Sous-réseau

Le sous-réseau qui contient les adresses IP que vous souhaitez attribuer à votre point de terminaison Resolver. ENIs Il s'agit des adresses auxquelles vous allez envoyer des requêtes DNS. Le sous-réseau doit avoir une adresse IP disponible.

L'adresse IP du sous-réseau doit correspondre au type de point de terminaison.

Adresse IP

Adresse IP unique vers laquelle les requêtes DNS doivent être transférées.

Choisissez si vous souhaitez que Resolver choisisse une adresse IP pour vous parmi les adresses IP disponibles dans le sous-réseau indiqué, ou si vous voulez indiquer l'adresse IP vous-même.

Si vous choisissez de spécifier vous-même l'adresse IP, entrez une IPv6 adresse IPv4 ou, ou les deux.

Protocoles

Le protocole de point de terminaison détermine la manière dont les données sont transmises à un point de terminaison entrant. Choisissez un ou plusieurs protocoles en fonction du niveau de sécurité requis.

- Do53 : (Par défaut) Les données sont relayées à l'aide du Route 53 Resolver sans chiffrement supplémentaire. Bien que les données ne puissent pas être lues par des tiers, elles peuvent être consultées au sein des AWS réseaux. Il s'agit du seul protocole actuellement disponible pour la catégorie des points de terminaison entrants de délégation.
- DoH : Les données sont transmises via une session HTTPS chiffrée. Le DoH ajoute un niveau de sécurité supplémentaire selon lequel les données ne peuvent pas être déchiffrées par des utilisateurs non autorisés et ne peuvent être lues par personne d'autre que le destinataire prévu.

- DOH-FIPS : Les données sont transmises via une session HTTPS chiffrée conforme à la norme de chiffrement FIPS 140-2. Pris en charge uniquement pour les points de terminaison entrants. Pour plus d'informations, veuillez consulter FIPS PUB 140-2.

> **Note**
>
> Pour les points de terminaison entrants DOH/DOH-FIPS, il existe un problème connu lié à la publication d'une adresse IP source incorrecte dans le journal des requêtes Route 53 Resolver.

Pour un point de terminaison entrant, vous pouvez appliquer les protocoles comme suit :

- Do53 et DoH en combinaison.
- Do53 et DoH-FIPS en combinaison.
- Do53 uniquement.
- DoH uniquement.
- DoH-FIPS uniquement.
- Aucun, qui est traité comme Do53.

> **Important**
>
> Vous ne pouvez pas modifier directement le protocole d'un point de terminaison entrant uniquement de Do53 uniquement à DoH ou DOH-FIPS. Cela permet d'éviter une interruption soudaine du trafic entrant qui repose sur Do53. Pour changer le protocole de Do53 à DoH ou DOH-FIPS, vous devez d'abord activer Do53 et DoH ou Do53 et DOH-FIPS, pour vous assurer que tout le trafic entrant a été transféré à l'aide du protocole DoH ou DOH-FIPS, puis supprimer le Do53.

Balises

Spécifiez une ou plusieurs clés et les valeurs correspondantes. Par exemple, vous pouvez indiquer Cost center (Centre de coûts) pour Key (Clé) et 456 pour Value (Valeur).

Gestion des points de terminaison entrants

Pour gérer les points de terminaison entrants, exécutez la procédure applicable.

Rubriques

- Affichage et modification des points de terminaison entrants
- Affichage du statut des points de terminaison entrants
- Suppression des points de terminaison entrants

Affichage et modification des points de terminaison entrants

Pour afficher et modifier les paramètres d'un point de terminaison entrant, exécutez la procédure suivante.

Afficher ou modifier les paramètres d'un point de terminaison entrant

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le panneau de navigation, choisissez Inbound endpoints (Points de terminaison entrants).
3. Dans la barre de navigation, choisissez la région dans laquelle vous avez créé le point de terminaison entrant.
4. Choisissez l'option correspondant au point de terminaison que vous souhaitez consulter ou modifier.
5. Choisissez View details (Consulter les détails) ou Edit (Modifier).

   Pour plus d'informations sur les valeurs des points de terminaison entrants, consultez Valeurs à spécifier lors de la création ou de la modification de points de terminaison entrants.
6. Si vous avez choisi Edit (Modifier), entrez les valeurs applicables puis sélectionnez Save (Enregistrer).

Affichage du statut des points de terminaison entrants

Pour afficher le statut d'un point de terminaison entrant, procédez comme suit.

Pour afficher le statut d'un point de terminaison entrant

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le panneau de navigation, choisissez Inbound endpoints (Points de terminaison entrants).

3. Dans la barre de navigation, choisissez la région dans laquelle vous avez créé le point de terminaison entrant. La colonne Status (Statut) contient l'une des valeurs suivantes :

   Création

   Resolver crée et configure une ou plusieurs interfaces réseau Amazon VPC pour ce point de terminaison.

   Fonctionnement

   Les interfaces réseau Amazon VPC pour ce point de terminaison sont correctement configurées et en mesure de transmettre les requêtes DNS entrantes ou sortantes entre votre réseau et Resolver.

   Mise à jour

   Le résolveur associe ou dissocie une ou plusieurs interfaces réseau à l'aide de ce point de terminaison.

   Récupération automatique

   Resolver tente de récupérer une ou plusieurs des interfaces réseau qui sont associées à ce point de terminaison. Pendant le processus de récupération, le point de terminaison fonctionne avec une capacité limitée, en raison de la limite du nombre de requêtes DNS par adresse IP (par interface réseau). Pour connaître la limite actuelle, veuillez consulter Quotas sur Route 53 Resolver.

   Action requise

   Ce point de terminaison est non sain, et Resolver ne peut pas le récupérer automatiquement. Pour résoudre le problème, nous vous recommandons de vérifier chaque adresse IP que vous avez associé au point de terminaison. Pour chaque adresse IP qui n'est pas disponible, ajouter une autre adresse IP, puis supprimer l'adresse IP qui n'est pas disponible. (Un point de terminaison doivent toujours inclure au moins deux adresses IP.) Un état Action needed (Action nécessaire) peut avoir plusieurs causes. Voici les deux plus courantes :

   - Une ou plusieurs des interfaces réseau qui sont associées au point de terminaison ont été supprimées en utilisant Amazon VPC.
   - L'interface réseau n'a pas pu être créée pour une certaine raison que Resolver ne peut pas contrôler.

Suppression

Le résolveur supprime ce point de terminaison et les interfaces réseau associées.

Suppression des points de terminaison entrants

Pour supprimer un point de terminaison entrant, utilisez la procédure suivante.

> **Important**
>
> Si vous supprimez un point de terminaison entrant, les requêtes DNS de votre réseau ne seront plus réacheminées vers Resolver dans le VPC que vous avez indiqué dans le point de terminaison.

Supprimer un point de terminaison entrant

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le panneau de navigation, choisissez Inbound endpoints (Points de terminaison entrants).
3. Dans la barre de navigation, choisissez la région dans laquelle vous avez créé le point de terminaison entrant.
4. Choisissez l'option du point de terminaison que vous souhaitez supprimer.
5. Sélectionnez Delete (Supprimer).
6. Pour confirmer que vous voulez supprimer le point de terminaison, saisissez le nom du point de terminaison et sélectionnez Submit (Envoyer).

Réacheminement des requêtes DNS sortantes vers votre réseau

Pour transférer les requêtes DNS provenant d' EC2 instances Amazon en une ou plusieurs VPCs vers votre réseau, vous devez créer un point de terminaison sortant et une ou plusieurs règles :

Point de terminaison sortant

Pour transférer les requêtes DNS de votre réseau VPCs vers votre réseau, vous devez créer un point de terminaison sortant. Un point de terminaison sortant spécifie les adresses IP d'où proviennent les requêtes. Ces adresses IP, que vous choisissez parmi la plage d'adresses

IP disponibles pour votre VPC, ne sont pas des adresses IP publiques. Cela signifie que, pour chaque point de terminaison sortant, vous devez connecter votre VPC à votre réseau à l'aide d'une connexion AWS Direct Connect , d'une connexion VPN ou d'une passerelle de traduction d'adresses réseau (NAT). Notez que vous pouvez utiliser le même point de terminaison sortant pour plusieurs points de terminaison VPCs dans la même région, ou vous pouvez créer plusieurs points de terminaison sortants. Si vous souhaitez utiliser votre point de terminaison sortant DNS64, vous pouvez l'activer à DNS64 l'aide d'Amazon Virtual Private Cloud. Pour plus d'informations, consultez DNS64 et consultez NAT64 le guide de l'utilisateur Amazon VPC.

L'adresse IP cible de la règle Route 53 Resolver est choisie au hasard par Resolver et il n'y a aucune préférence quant au choix d'une adresse IP cible particulière par rapport à une autre. Si une adresse IP cible ne répond pas à la demande DNS transmise, le résolveur réessaiera d'utiliser une adresse IP aléatoire parmi la cible. IPs

Assurez-vous que toutes les adresses IP cibles sont accessibles depuis les points de terminaison du résolveur. Si Resolver n'est pas en mesure de transférer les requêtes DNS sortantes vers l'une des adresses IP cibles, cela peut entraîner des délais de résolution DNS prolongés.

Règles

Pour spécifier les noms de domaine des requêtes que vous voulez réacheminer vers les résolveurs DNS de votre réseau, vous devez créer une ou plusieurs règles. Chaque règle de transfert spécifie un nom de domaine. Vous associez ensuite les règles VPCs pour lesquelles vous souhaitez transférer les requêtes vers votre réseau.

Les règles de délégation sortante suivent des principes de délégation spécifiques qui diffèrent des règles de transfert standard. Lorsque vous créez une règle de délégation, Route 53 Resolver évalue les enregistrements de délégation contenus dans la règle par rapport aux enregistrements NS dans les réponses DNS afin de déterminer si une délégation doit avoir lieu. Le résolveur Route 53 déléguera l'autorité à vos résolveurs locaux uniquement lorsqu'il existe une correspondance entre la configuration des règles de délégation et les enregistrements NS réels renvoyés dans la réponse DNS. Contrairement aux règles de transfert qui redirigent les requêtes en fonction de la correspondance des noms de domaine, les règles de délégation respectent la chaîne de délégation DNS et ne s'activent que lorsque les serveurs de noms faisant autorité dans la réponse correspondent à la configuration de délégation.

Pour plus d’informations, consultez les rubriques suivantes :

- Private hosted zones that have overlapping namespaces
- Private hosted zones and Route 53 Resolver rules

Configuration du réacheminement sortant

Pour configurer Resolver afin de réacheminer les requêtes DNS créées dans votre VPC vers votre réseau, exécutez les procédures suivantes.

> **Important**
>
> Après avoir créé un point de terminaison sortant, vous devez créer une ou plusieurs règles et les associer à une ou plusieurs VPCs règles. Les règles spécifient les noms de domaine des requêtes DNS que vous souhaitez réacheminer vers votre réseau.

Créer un point de terminaison sortant

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le panneau de navigation, choisissez Outbound endpoints (Points de terminaison sortants).
3. Dans la barre de navigation, choisissez la région dans laquelle vous voulez créer un point de terminaison sortant.
4. Choisissez Create outbound endpoint (Créer point de terminaison sortant).
5. Entrez les valeurs applicables. Pour plus d'informations, veuillez consulter Valeurs à spécifier lors de la création ou de la modification de points de terminaison sortants.
6. Choisissez Créer.

   > **Note**
   >
   > Créer un point de terminaison sortant prend une minute ou deux. Vous ne pouvez pas créer d'autre point de terminaison sortant avant d'avoir créé le premier.

7. Créez une ou plusieurs règles pour spécifier les noms de domaine des requêtes DNS que vous voulez réacheminer vers votre réseau. Pour en savoir plus, consultez la procédure suivante.

Pour créer une ou plusieurs règles de réacheminement, exécutez la procédure suivante.

Pour créer des règles de transfert et les associer à une ou plusieurs VPCs

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation, choisissez Règles.
3. Dans la barre de navigation, choisissez la région dans laquelle vous voulez créer la règle.
4. Choisissez Créer une règle.
5. Entrez les valeurs applicables. Pour plus d'informations, veuillez consulter Valeurs à spécifier lors de la création ou de la modification de règles.
6. Choisissez Enregistrer.
7. Pour ajouter une autre règle, répétez les étapes 4 à 6.

Valeurs à spécifier lors de la création ou de la modification de points de terminaison sortants

Lorsque vous créez ou modifiez un point de terminaison sortant, spécifiez les valeurs suivantes :

ID Outpost

Si vous créez le point de terminaison d'un résolveur sur un AWS Outposts VPC, il s'agit AWS Outposts de l'ID.

Nom du point de terminaison

Un nom convivial vous permettant de retrouver facilement le point de terminaison sortant sur le tableau de bord.

VPC dans la région region-name

Toutes les requêtes DNS sortantes transiteront via ce VPC lors de leur transfert vers votre réseau.

Groupe de sécurité de ce point de terminaison

L'ID d'un ou de plusieurs groupes de sécurité que vous souhaitez utiliser pour contrôler l'accès à ce VPC. Le groupe de sécurité que vous spécifiez doit inclure une ou plusieurs règles sortantes. Les règles sortantes doivent autoriser l'accès TCP et UDP sur le port que vous utilisez pour les requêtes DNS sur votre réseau. Vous ne pouvez pas modifier cette valeur après avoir créé un point de terminaison.

Certaines règles de groupe de sécurité entraînent le suivi de votre connexion et peuvent avoir un impact sur le nombre maximal de requêtes par seconde entre le point de terminaison sortant et votre serveur de noms cible. Pour éviter le suivi des connexions causé par un groupe de sécurité, consultez la section Connexions non suivies.

Pour plus d'informations, consultez Groupes de sécurité pour votre VPC dans le Guide de l'utilisateur Amazon VPC.

Type de point de terminaison

Le type de point de terminaison peut être soit IPv4 IPv6 des adresses IP à double pile. Pour un point de terminaison à double pile, le point de terminaison aura à la fois IPv4 une IPv6 adresse à laquelle votre résolveur DNS sur votre réseau peut transférer les requêtes DNS.

> **Note**
>
> Pour des raisons de sécurité, nous refusons l'accès direct au IPv6 trafic Internet public pour toutes les adresses IPv6 IP et à double pile.

Adresses IP

Les adresses IP de votre VPC vers lesquelles vous voulez que Resolver réachemine les requêtes DNS lors de leur transfert vers les résolveurs de votre réseau. Il ne s'agit pas des adresses IP des résolveurs DNS de votre réseau ; vous spécifiez les adresses IP des résolveurs lorsque vous créez les règles que vous associez à une ou plusieurs d'entre elles. VPCs Nous vous demandons de spécifier au moins deux adresses IP pour la redondance.

> **Note**
>
> Le point de terminaison Resolver possède une adresse IP privée. Ces adresses IP ne changeront pas au cours de la durée de vie d'un point de terminaison.

Remarques :

Plusieurs zones de disponibilité

Nous vous recommandons de spécifier des adresses IP dans au moins deux zones de disponibilité. Si vous le souhaitez, vous pouvez spécifier des adresses IP supplémentaires dans ces zones de disponibilité ou dans d'autres.

Adresses IP et interfaces réseau Elastic Amazon VPC

Pour chaque combinaison de zone de disponibilité, sous-réseau, et adresse IP que vous spécifiez, Resolver crée une interface réseau Elastic Amazon VPC. Pour le nombre maximum actuel de requêtes DNS par seconde et par adresse IP dans un point de terminaison, consultez Quotas sur Route 53 Resolver. Pour plus d'informations sur la tarification pour chaque interface réseau Elastic, veuillez consulter la section « Amazon Route 53 » sur la page de tarification d'Amazon Route 53.

Ordre des adresses IP

Vous pouvez spécifier des adresses IP dans n'importe quel ordre. Lors du réacheminement de requêtes DNS, Resolver ne choisit pas les adresses IP en fonction de l'ordre dans lequel elles sont répertoriées.

Pour chaque adresse IP, spécifiez les valeurs suivantes. Chaque adresse IP doit se trouver dans une zone de disponibilité du VPC que vous avez indiquée dans VPC dans la région region-name.

Zone de disponibilité

La zone de disponibilité par laquelle vous voulez que les requêtes DNS transitent lors de leur transfert vers votre réseau. La zone de disponibilité que vous spécifiez doit être configurée avec un sous-réseau.

Sous-réseau

Le sous-réseau qui contient l'adresse IP depuis laquelle vous voulez que les requêtes DNS soient lancées lors de leur transfert vers votre réseau. Le sous-réseau doit avoir une adresse IP disponible.

L'adresse IP du sous-réseau doit correspondre au type de point de terminaison.

Adresse IP

Adresse IP à parti de laquelle vous voulez que les requêtes DNS soient lancées lors de leur transfert vers votre réseau.

Choisissez si vous souhaitez que Resolver choisisse une adresse IP pour vous parmi les adresses IP disponibles dans le sous-réseau indiqué, ou si vous voulez indiquer l'adresse IP vous-même.

Si vous choisissez de spécifier vous-même l'adresse IP, entrez une IPv6 adresse IPv4 ou, ou les deux.

Protocoles

Le protocole de point de terminaison détermine la manière dont les données sont transmises à un point de terminaison sortant. Choisissez un ou plusieurs protocoles en fonction du niveau de sécurité requis.

- Do53 : (Par défaut) Les données sont relayées à l'aide du Route 53 Resolver sans chiffrement supplémentaire. Bien que les données ne puissent pas être lues par des parties externes, elles peuvent être consultées au sein des réseaux AWS .
- DoH : Les données sont transmises via une session HTTPS chiffrée. Le DoH ajoute un niveau de sécurité supplémentaire selon lequel les données ne peuvent pas être déchiffrées par des utilisateurs non autorisés et ne peuvent être lues par personne d'autre que le destinataire prévu.

Pour un point de terminaison sortant, vous pouvez appliquer les protocoles comme suit :

- Do53 et DoH en combinaison.
- Do53 uniquement.
- DoH uniquement.
- Aucun, qui est traité comme Do53.

Balises

Spécifiez une ou plusieurs clés et les valeurs correspondantes. Par exemple, vous pouvez indiquer Cost center (Centre de coûts) pour Key (Clé) et 456 pour Value (Valeur).

Valeurs à spécifier lors de la création ou de la modification de règles

Lorsque vous créez ou modifiez une règle de réacheminement, spécifiez les valeurs suivantes :

Nom de la règle

Un nom convivial vous permettant de retrouver facilement la règle sur le tableau de bord.

Type de règle

Choisissez la valeur applicable :

- Forward (Réacheminer) - Lorsque vous voulez réacheminer les requêtes DNS pour le nom de domaine indiqué vers les résolveurs de votre réseau, choisissez cette option.
- Déléguer : choisissez cette option lorsque vous souhaitez déléguer l'autorité d'un sous-domaine, hébergé dans une zone hébergée privée, à votre résolveur sur site (ou à un résolveur sur un autre VPC).

- Système - Choisissez cette option lorsque vous voulez que Resolver remplace de manière sélective le comportement qui est défini dans une règle de réacheminement. Lorsque vous créez une règle système, Resolver résout les requêtes DNS pour les sous-domaines indiqués, qui seraient sinon résolues par les résolveurs DNS de votre réseau.

Par défaut, les règles de réacheminement s'appliquent à un nom de domaine et à tous ses sous-domaines. Si vous souhaitez réacheminer les requêtes d'un domaine vers un résolveur de votre réseau, mais pas celles de certains sous-domaines, créez une règle système pour les sous-domaines. Par exemple, si vous créez une règle de réacheminement pour exemple.com, mais que vous ne voulez pas réacheminer les requêtes pour acme.exemple.com, créez une règle système et indiquez acme.exemple.com pour le nom de domaine.

Enregistrement de délégation — pour la règle de délégation uniquement

— Les requêtes DNS qui correspondent à ce domaine sont transmises aux résolveurs de votre réseau.

> **Note**
>
> Comme condition préalable à une règle de délégation, vous devez créer des enregistrements NS dans la zone hébergée privée, lorsque vous utilisez une zone hébergée privée pour une délégation sortante. L'enregistrement est le suivant : NS - Serveurs de noms à déléguer via le point de terminaison sortant du résolveur avec règle déléguée. Pour de plus amples informations, veuillez consulter Type d'enregistrement NS.

VPCs qui utilisent cette règle

Les VPCs qui utilisent cette règle pour transférer les requêtes DNS pour le ou les noms de domaine spécifiés. Vous pouvez appliquer une règle à autant de personnes VPCs que vous le souhaitez.

Nom de domaine : pour la règle directe uniquement

Les requêtes DNS pour ce nom de domaine sont réacheminées vers les adresses IP que vous spécifiez dans le champ Target IP addresses (Adresses IP cible). Pour plus d'informations, veuillez consulter Comment Resolver détermine si le nom de domaine d'une requête correspond aux règles.

Point de terminaison sortant

Resolver réachemine les requêtes DNS à travers le point de terminaison sortant indiqué ici vers les adresses IP indiquées dans Target IP addresses (Adresses IP cible).

Adresses IP cible

Lorsqu'une requête DNS correspond au nom que vous spécifiez dans le champ Domain name (Nom de domaine), le point de terminaison sortant réachemine la requête vers les adresses IP que vous spécifiez ici. Ce sont généralement les adresses IP des résolveurs DNS sur votre réseau.

L'option Target IP addresses (Adresses IP cible) n'est disponible que lorsque la valeur de Rule type (Type de règle) est Forward (Réacheminer).

Spécifiez IPv4 IPv6 les adresses, les protocoles que ServerNameIndication vous souhaitez utiliser pour le point de terminaison. ServerNameIndication s'applique uniquement lorsque le protocole sélectionné est DoH.

La résolution de l'adresse IP cible du FQDN d'un résolveur DoH de votre réseau via le point de terminaison sortant n'est pas prise en charge. Les points de terminaison sortants ont besoin de l'adresse IP cible du résolveur DoH de votre réseau pour transférer les requêtes DoH. Si le résolveur DoH de votre réseau a besoin du FQDN dans le TLS SNI et dans l'en-tête HTTP Host, il doit être fourni. ServerNameIndication

ServerNameIndication

L'indication du nom du serveur DoH auquel vous souhaitez transférer les requêtes. Ceci n'est utilisé que si le protocole est DoH.

Balises

Spécifiez une ou plusieurs clés et les valeurs correspondantes. Par exemple, vous pouvez indiquer Cost center (Centre de coûts) pour Key (Clé) et 456 pour Value (Valeur).

Ce sont les tags qui AWS Billing and Cost Management permettent d'organiser votre AWS facture. Pour plus d'informations sur l'utilisation de balises pour l'allocation de coûts, consultez Utilisation des balises d'allocation de coûts dans le Guide de l'utilisateur AWS Billing .

Gestion des points de terminaison sortants

Pour gérer les points de terminaison sortants, exécutez la procédure applicable.

Rubriques

- Affichage et modification des points de terminaison sortants
- Affichage du statut des points de terminaison sortants
- Suppression des points de terminaison sortants

Affichage et modification des points de terminaison sortants

Pour afficher et modifier les paramètres d'un point de terminaison sortant, exécutez la procédure suivante.

Afficher ou modifier les paramètres d'un point de terminaison sortant

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le panneau de navigation, choisissez Outbound endpoints (Points de terminaison sortants).
3. Dans la barre de navigation, choisissez la région dans laquelle vous avez créé le point de terminaison sortant.
4. Choisissez l'option correspondant au point de terminaison que vous souhaitez consulter ou modifier.
5. Choisissez View details (Consulter les détails) ou Edit (Modifier).

   Pour plus d'informations sur les valeurs des points de terminaison sortants, veuillez consulter Valeurs à spécifier lors de la création ou de la modification de points de terminaison sortants.
6. Si vous avez choisi Edit (Modifier), entrez les valeurs applicables puis sélectionnez Save (Enregistrer).

Affichage du statut des points de terminaison sortants

Pour afficher le statut d'un point de terminaison sortant, procédez comme suit.

Pour afficher le statut d'un point de terminaison sortant

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le panneau de navigation, choisissez Outbound endpoints (Points de terminaison sortants).

3. Dans la barre de navigation, choisissez la région dans laquelle vous avez créé le point de terminaison sortant. La colonne Status (Statut) contient l'une des valeurs suivantes :

   Création

   Resolver crée et configure une ou plusieurs interfaces réseau Amazon VPC pour ce point de terminaison.

   Fonctionnement

   Les interfaces réseau Amazon VPC pour ce point de terminaison sont correctement configurées et en mesure de transmettre les requêtes DNS entrantes ou sortantes entre votre réseau et Resolver.

   Mise à jour

   Le résolveur associe ou dissocie une ou plusieurs interfaces réseau à l'aide de ce point de terminaison.

   Récupération automatique

   Resolver tente de récupérer une ou plusieurs des interfaces réseau qui sont associées à ce point de terminaison. Pendant le processus de récupération, le point de terminaison fonctionne avec une capacité limitée, en raison de la limite du nombre de requêtes DNS par adresse IP (par interface réseau). Pour connaître la limite actuelle, veuillez consulter Quotas sur Route 53 Resolver.

   Action requise

   Ce point de terminaison est non sain, et Resolver ne peut pas le récupérer automatiquement. Pour résoudre le problème, nous vous recommandons de vérifier chaque adresse IP que vous avez associé au point de terminaison. Pour chaque adresse IP qui n'est pas disponible, ajouter une autre adresse IP, puis supprimer l'adresse IP qui n'est pas disponible. (Un point de terminaison doivent toujours inclure au moins deux adresses IP.) Un état Action needed (Action nécessaire) peut avoir plusieurs causes. Voici les deux plus courantes :

   - Une ou plusieurs des interfaces réseau qui sont associées au point de terminaison ont été supprimées en utilisant Amazon VPC.
   - L'interface réseau n'a pas pu être créée pour une certaine raison que Resolver ne peut pas contrôler.

Suppression

Le résolveur supprime ce point de terminaison et les interfaces réseau associées.

Suppression des points de terminaison sortants

Avant de pouvoir supprimer un point de terminaison, vous devez d'abord supprimer toutes les règles associées à un VPC.

Pour supprimer un point de terminaison sortant, utilisez la procédure suivante.

> **Important**
>
> Si vous supprimez un point de terminaison sortant, Resolver cessera de réacheminer les requêtes DNS à partir de votre VPC vers votre réseau pour les règles qui spécifient le point de terminaison sortant supprimé.

Supprimer un point de terminaison sortant

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le panneau de navigation, choisissez Outbound endpoints (Points de terminaison sortants).
3. Dans la barre de navigation, choisissez la région dans laquelle vous avez créé le point de terminaison sortant.
4. Choisissez l'option du point de terminaison que vous souhaitez supprimer.
5. Sélectionnez Delete (Supprimer).
6. Pour confirmer que vous voulez supprimer le point de terminaison, saisissez le nom du point de terminaison puis sélectionnez Submit (Envoyer).

Gestion des règles de réacheminement

Si vous souhaitez que Resolver réachemine les requêtes pour les noms de domaine indiqués vers votre réseau, créez une règle de réacheminement pour chaque nom de domaine et spécifiez le nom du domaine pour lequel vous souhaitez réacheminer les requêtes.

Rubriques

- Affichage et modification des règles de réacheminement
- Créer des règles de réacheminement
- Ajout de règles pour la recherche inversée
- Associer des règles de réacheminement à un VPC
- Dissocier des règles de réacheminement d'un VPC
- Partage des règles du résolveur avec d'autres AWS comptes et utilisation de règles partagées
- Supprimer des règles de réacheminement
- Règles de transfert pour les requêtes DNS inverses dans Resolver

Affichage et modification des règles de réacheminement

Pour afficher et modifier les paramètres d'une règle de réacheminement, exécutez la procédure suivante.

Afficher et modifier les paramètres d'une règle de réacheminement

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le panneau de navigation, choisissez Rules (Règles).
3. Dans la barre de navigation, choisissez la région dans laquelle vous avez créé la règle.
4. Choisissez l'option correspondant à la règle que vous souhaitez consulter ou modifier.
5. Choisissez View details (Consulter les détails) ou Edit (Modifier).

   Pour plus d'informations sur les valeurs des règles de réacheminement, consultez Valeurs à spécifier lors de la création ou de la modification de règles.
6. Si vous avez choisi Edit (Modifier), entrez les valeurs applicables puis sélectionnez Save (Enregistrer).

Créer des règles de réacheminement

Pour créer une ou plusieurs règles de réacheminement, exécutez la procédure suivante.

Pour créer des règles de transfert et les associer à une ou plusieurs VPCs

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.

2. Dans le volet de navigation, choisissez Règles.
3. Dans la barre de navigation, choisissez la région dans laquelle vous voulez créer la règle.
4. Choisissez Créer une règle.
5. Entrez les valeurs applicables. Pour plus d'informations, veuillez consulter Valeurs à spécifier lors de la création ou de la modification de règles.
6. Choisissez Enregistrer.
7. Pour ajouter une autre règle, répétez les étapes 4 à 6.

Ajout de règles pour la recherche inversée

Si vous devez contrôler les recherches inversées dans votre VPC, vous pouvez ajouter des règles à votre point de terminaison de résolveur sortant.

Pour créer la règle de recherche inversée

1. Suivez les étapes de la procédure précédente, jusqu'à l'étape 5.
2. Lorsque vous spécifiez votre règle, entrez lePTRpour l'adresse IP ou les adresses pour lesquelles vous souhaitez une règle de transfert de recherche inversée.

   Par exemple, pour réacheminer des recherches pour des adresses dans la plage 10.0.0.0/23, entrez deux règles :

   - 0.0.10.in-addr.arpa
   - 1.0.10.in-addr.arpa

   Toute adresse IP de ces sous-réseaux sera référencée en tant que sous-domaine de ces registres PTR. Par exemple, 10.0.1.161 aura une adresse de recherche inverse qui sera 161.1.0.10.in-addr.arpa, qui est un sous-domaine de 1.0.10.in-addra.arpa.
3. Spécifiez le serveur vers lequel transférer ces recherches.
4. Ajoutez ces règles à votre point de terminaison de résolveur sortant.

Notez que l'activation de `enableDNSHostNames` pour votre VPC ajoute automatiquement des registres PTR. Consultez Qu'est-ce que c'est Amazon Route 53 Resolver ?. La procédure précédente n'est requise que si vous souhaitez indiquer explicitement un résolveur pour des plages IP données, par exemple lors du transfert de requêtes vers un serveur Active Directory.

Associer des règles de réacheminement à un VPC

Après avoir créé une règle de transfert, vous devez l'associer à une ou plusieurs d'entre elles VPCs. Les règles ne fonctionneront qu'une fois associées à un VPC. Lorsque vous associez une règle à un VPC, Resolver commence à réacheminer les requêtes DNS pour le nom de domaine indiqué dans la règle vers les résolveurs DNS également spécifiés dans la règle. Les requêtes transitent par le point de terminaison sortant que vous avez spécifié lorsque vous avez créé la règle.

Pour associer une règle de transfert à une ou plusieurs VPCs

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le panneau de navigation, choisissez Rules (Règles).
3. Dans la barre de navigation, choisissez la région dans laquelle vous avez créé la règle.
4. Choisissez le nom de la règle que vous souhaitez associer à une ou plusieurs règles VPCs.
5. Choisissez Associate VPC (Associer un VPC).
6. Sous VPCs cette règle d'utilisation, choisissez VPCs celle à laquelle vous souhaitez associer la règle.
7. Choisissez Ajouter.

Dissocier des règles de réacheminement d'un VPC

Dissociez une règle de réacheminement d'un VPC dans les cas suivants :

- Pour les requêtes DNS provenant de ce VPC, vous voulez que Resolver cesse de réacheminer vers votre réseau les requêtes pour le nom de domaine indiqué dans la règle.
- Vous souhaitez supprimer la règle de réacheminement. Si une règle est actuellement associée à une ou plusieurs d'entre elles VPCs, vous devez la dissocier de tous VPCs avant de pouvoir la supprimer.

Si vous souhaitez dissocier une règle de transfert d'une ou de plusieurs règles VPCs, effectuez la procédure suivante.

Dissocier une règle de réacheminement d'un VPC

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.

2. Dans le panneau de navigation, choisissez Rules (Règles).
3. Dans la barre de navigation, choisissez la région dans laquelle vous avez créé la règle.
4. Choisissez le nom de la règle que vous souhaitez dissocier d'une ou de plusieurs règles. VPCs
5. Choisissez l'option pour le CPV duquel vous voulez dissocier la règle.
6. Choisissez Dissocier.
7. Entrez disassociate pour confirmer.
8. Sélectionnez Envoyer.

Partage des règles du résolveur avec d'autres AWS comptes et utilisation de règles partagées

Vous pouvez partager les règles du résolveur que vous avez créées à l'aide d'un AWS compte avec d'autres AWS comptes. Pour partager les règles, la console Route 53 Resolver s'intègre à AWS Resource Access Manager. Pour plus d'informations sur Resource Access Manager, consultez le Guide de l'utilisateur Resource Access Manager.

Remarques :

Associer des règles partagées à VPCs

Si un autre AWS compte partage une ou plusieurs règles avec le vôtre, vous pouvez associer les règles à votre compte de VPCs la même manière que vous associez les règles que vous avez créées à votre compte VPCs. Pour de plus amples informations, veuillez consulter Associer des règles de réacheminement à un VPC.

Supprimer ou annuler le partage d'une règle

Si vous partagez une règle avec d'autres comptes, puis que vous la supprimez ou que vous arrêtez de la partager, et si la règle était associée à un ou plusieurs comptes VPCs, Route 53 Resolver commence à traiter les requêtes DNS pour ces comptes en VPCs fonction des règles restantes. Le comportement est identique que si vous dissociez la règle depuis le VPC.

Si une règle est partagée avec une unité d'organisation (UO) et qu'un compte de l'UO est déplacé vers une autre UO, toutes les associations avec la règle partagée avec un VPC du compte seront supprimées. Toutefois, si la règle du résolveur était déjà partagée avec l'unité organisationnelle de destination, l'association VPC restera intacte et ne sera pas dissociée.

Nombre maximal de règles et d'associations

Lorsqu'un compte crée une règle et la partage avec un ou plusieurs autres comptes, le nombre maximum de règles par AWS région s'applique au compte qui a créé la règle.

Lorsqu'un compte avec lequel une règle est partagée associe la règle à une ou plusieurs règles VPCs, le nombre maximum d'associations entre les règles et VPCs par région s'applique au compte avec lequel la règle est partagée.

Pour consulter les quotas Resolver actuels, consultez Quotas sur Route 53 Resolver.

Autorisations

Pour partager une règle avec un autre AWS compte, vous devez être autorisé à utiliser l'PutResolverRulePolicyaction.

Restrictions relatives au AWS compte avec lequel une règle est partagée

Le compte avec lequel une règle est partagée ne peut pas modifier ni supprimer la règle.

Identification

Seul le compte qui a créé une règle peut ajouter, supprimer ou consulter les balises de la règle.

Pour consulter le statut de partage actuel d'une règle (y compris le compte qui a partagé la règle ou le compte avec lequel une règle est partagée) et partager des règles avec un autre compte, exécutez la procédure suivante.

Pour consulter l'état du partage et partager les règles avec un autre AWS compte

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le panneau de navigation, choisissez Rules (Règles).
3. Dans la barre de navigation, choisissez la région dans laquelle vous avez créé la règle.

   La colonne Sharing status (Statut de partage) affiche le statut de partage actuel des règles qui ont été créées par le compte actuel ou qui sont partagées avec le compte actuel :

   - Non partagé : le AWS compte actuel a créé la règle, et celle-ci n'est partagée avec aucun autre compte.
   - Shared by me (Partagé par moi) : le compte actuel a créé la règle et l'a partagée avec un ou plusieurs comptes.

- Shared with me (Partagé avec moi) : un autre compte a créé la règle et l'a partagée avec le compte actuel.

4. Choisissez le nom de la règle dont vous souhaitez afficher les informations de partage ou que vous souhaitez partager avec un autre compte.

   Sur la *`rule name`* page Règle :, la valeur sous Propriétaire indique l'ID du compte qui a créé la règle. Il s'agit du compte actuel, à moins que la valeur Sharing status (Statut de partage) soit Shared with me (Partagée avec moi). Dans ce cas, l'option Owner (Propriétaire) désigne le compte qui a créé la règle et l'a partagée avec le compte actuel.

5. Sélectionnez Share (Partager) pour afficher des informations supplémentaires ou pour partager la règle avec un autre compte. Une page de la console Resource Access Manager s'affiche, en fonction de la valeur de Sharing status (Statut de partage) :

   - Not shared (Non partagé) : la page Create resource share (Créer partage de ressource) s'affiche. Pour plus d'informations sur la façon de partager la règle avec un autre compte, une unité d'organisation ou une organisation, passez directement à l'étape 6.
   - Shared by me (Partagé par moi) : la page Shared resources (Ressources partagées) affiche les règles et autres ressources qui sont détenues par le compte actuel et partagées avec d'autres comptes.
   - Shared with me (Partagé avec moi) : la page Shared resources (Ressources partagées) affiche les règles et autres ressources qui sont détenues par d'autres comptes et partagées avec le compte actuel.

6. Pour partager une règle avec un autre AWS compte, unité d'organisation ou organisation, spécifiez les valeurs suivantes.

   > **Note**
   >
   > Vous ne pouvez pas mettre à jour les paramètres de partage. Si vous voulez modifier l'un des paramètres suivants, vous devez repartager une règle avec les nouveaux paramètres, puis supprimer les anciens paramètres de partage.

   Description

   Saisissez une courte description qui vous aide à mémoriser les raisons pour lesquelles vous avez partagé la règle.

Ressources

Cochez la case correspondant à la règle à partager.

Principaux

Entrez le numéro de AWS compte, le nom de l'unité d'organisation ou le nom de l'organisation.

Balises

Spécifiez une ou plusieurs clés et les valeurs correspondantes. Par exemple, vous pouvez indiquer Cost center (Centre de coûts) pour Key (Clé) et 456 pour Value (Valeur).

Ce sont les étiquettes qui AWS Billing and Cost Management permettent d'organiser votre AWS facture ; vous pouvez également les utiliser à d'autres fins. Pour plus d'informations sur l'utilisation de balises pour l'allocation de coûts, consultez Utilisation des balises d'allocation de coûts dans le Guide de l'utilisateur AWS Billing .

Supprimer des règles de réacheminement

Pour supprimer une règle de réacheminement, exécutez la procédure suivante.

Remarques :

- Si la règle de transfert est associée à une règle VPCs, vous devez dissocier la règle de la règle VPCs avant de pouvoir la supprimer. Pour de plus amples informations, veuillez consulter Dissocier des règles de réacheminement d'un VPC.
- Vous ne pouvez pas supprimer la règle par défaut du Internet Resolver (Résolveur Internet), qui a une valeur de Recursive (Récursif) pour le Type. Avec cette règle, Route 53 Resolver agit en tant que résolveur récursif pour tous les noms de domaine pour lesquels vous n'avez pas créé de règles personnalisées et pour lesquels Resolver n'a pas créé de règles autodéfinies. Pour plus d'informations sur la façon dont les règles sont classées, consultez Utilisation de règles pour contrôler les requêtes qui sont réacheminées vers votre réseau.

Supprimer une règle de réacheminement

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le panneau de navigation, choisissez Rules (Règles).

3. Dans la barre de navigation, choisissez la région dans laquelle vous avez créé la règle.
4. Choisissez l'option correspondant à la règle que vous souhaitez supprimer.
5. Sélectionnez Delete (Supprimer).
6. Pour confirmer que vous voulez supprimer la règle, saisissez le nom de la règle et sélectionnez Submit (Envoyer).

Règles de transfert pour les requêtes DNS inverses dans Resolver

Lorsque le `enableDnsHostnames` et `enableDnsSupport` sont réglés sur `true` pour un cloud privé virtuel (VPC) à partir d'Amazon VPC, Resolver crée automatiquement des règles de système autodéfinies pour les requêtes DNS inverses. Pour plus d'informations sur ces paramètres, veuillez consulter Attributs DNS dans votre VPC dans le Guide du développeur Amazon VPC.

Les règles de transfert pour les requêtes DNS inverses sont particulièrement utiles pour les services tels que SSH ou Active Directory, qui peuvent authentifier les utilisateurs en effectuant une recherche DNS inverse pour l'adresse IP à partir de laquelle un client tente de se connecter à une ressource. Pour plus d'informations sur les règles système autodéfinies, veuillez consulter Noms de domaine pour lesquels Resolver crée des règles système autodéfinies.

Vous pouvez désactiver ces règles et modifier toutes les requêtes DNS inverses afin qu'elles soient, par exemple, transférées vers vos serveurs de noms sur site pour résolution.

Une fois que vous avez désactivé les règles automatiques, créez des règles pour transférer les requêtes au besoin vers vos ressources sur site. Pour plus d'informations sur la gestion des règles de transfert, veuillez consulter Gestion des règles de réacheminement.

Pour désactiver les règles autodéfinies

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation, sous Resolver VPCs, choisissez, puis choisissez un VPC ID.
3. Sous Autodefined rules for reverse DNS resolution (Règles autodéfinies pour la résolution DNS inverse), désactivez la case à cocher. Si la case à cocher est déjà désélectionnée, vous pouvez la sélectionner pour activer la résolution DNS inverse autodéfinie.

Pour les informations connexes APIs, voir Configuration APIs du résolveur.

Tutoriel sur les règles de délégation Resolver

La règle de délégation permet au résolveur Route 53 d'atteindre les serveurs de noms hébergeant la zone déléguée via le point de terminaison sortant spécifié. Alors que la règle de transfert indique au résolveur Route 53 de transférer les requêtes DNS aux serveurs de noms correspondant au domaine spécifié via le point de terminaison sortant, la règle de délégation indique au résolveur Route 53 d'atteindre les serveurs de noms délégués via le point de terminaison sortant spécifié lorsque les enregistrements NS délégués sont renvoyés. Route 53 Resolver envoie une requête aux serveurs de noms délégués lorsque les enregistrements NS de la réponse DNS correspondent au nom de domaine spécifié dans l'enregistrement de délégation.

Étapes d'utilisation de la délégation sortante du point de terminaison Resolver

1. Créez un point de terminaison sortant Route 53 Resolver dans le VPC dont vous souhaitez que les requêtes DNS proviennent vers les résolveurs de votre réseau.

   Vous pouvez utiliser l'API ou la commande CLI suivante :

   - API `CreateResolverEndpoint`
   - `create-resolver-endpoint` CLI

2. Créez une ou plusieurs règles de délégation, qui spécifient les noms de domaine pour lesquels les requêtes doivent être déléguées à votre réseau via le point de terminaison sortant spécifié.

   Exemple de création de règles de délégation avec la CLI :

   ```
   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. Associez la règle de délégation à celle VPCs pour laquelle vous souhaitez que les requêtes soient déléguées.

   Vous pouvez utiliser l'API ou la commande CLI suivante :

- AssociateResolverRuleAPI.
- associate-resolver-rulesCommande CLI.

Types de délégation pris en charge par le point de terminaison sortant de Resolver

Route 53 Resolver prend en charge deux types de délégation sortante :

- Délégation sortante de la zone hébergée privée Route 53 vers Route 53 Resolver :

  Délégue un sous-domaine d'une zone hébergée privée vers un serveur DNS local ou vers une zone hébergée publique sur Internet à l'aide de la délégation sortante. Cette délégation sortante vous permet de répartir la gestion de vos enregistrements DNS entre la zone hébergée privée et la zone déléguée. La délégation peut être effectuée avec ou sans enregistrement adhésif dans une zone hébergée privée en fonction de votre configuration DNS. Pour plus d'informations, consultez. Zone hébergée privée vers le trafic sortant
- Route 53 Resolver de la délégation sortante vers la délégation sortante :

  Délégue un sous-domaine de votre serveur DNS local à un autre serveur local situé au même endroit ou à un emplacement différent en utilisant la délégation sortante à sortante. Cela est similaire à la délégation d'une zone hébergée privée vers un point de terminaison sortant, où vous pouvez déléguer à une zone hébergée sur votre serveur de noms local. Pour de plus amples informations, veuillez consulter De l'aller vers l'sortant.

Exemple de configuration de délégation sortante de la zone hébergée privée Route 53 vers Route 53 Resolver

Supposons une configuration DNS dans laquelle la zone hébergée parent est hébergée dans une zone hébergée privée Route 53 dans un Amazon VPC et où les sous-domaines sont délégués à des serveurs de noms hébergés en Europe, en Asie et en Amérique du Nord. Toutes les requêtes DNS sont transmises via le résolveur Route 53.

Suivez les exemples d'étapes pour configurer votre zone hébergée privée et votre résolveur Route 53.

Configurer une zone hébergée privée pour la délégation sortante

1. Pour la configuration de la zone hébergée privée :

   Zone hébergée par le parent : `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. Pour le serveur de noms local de la région Europe sur site :

   - Zone hébergée : `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. Pour le serveur de noms local de la région Asie sur site :

   Zone hébergée :`apac.hr.example.com`, `10.0.0.40`

   Le serveur de noms apac peut déléguer le sous-domaine à d'autres serveurs de noms.

```
$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
```

Zone hébergée :`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. Pour le serveur de noms local de la région Amérique du Nord :

   Zone hébergée : `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
```

Configuration du résolveur Route 53

- Pour le résolveur Route 53, vous devez configurer une règle directe et deux règles de délégation :

  Règle directe

  1. Pour transférer l'enregistrement de out-of-zone délégation, le résolveur Route 53 connaisse l'adresse IP du NS délégué pour transmettre la demande initiale.

     nom de domaine : target-ips : `hr.example.net` `10.0.0.50`

  Règles de délégation

  1. Règle de délégation pour la délégation en zone :

     enregistrement de délégation : `hr.example.com`
  2. Règle de délégation pour la délégation hors zone :

enregistrement de délégation : `hr.example.net`

Exemple de configuration de délégation sortante vers sortie

Au lieu d'avoir la zone hébergée parent dans un Amazon VPC, supposons une configuration DNS dans laquelle la zone hébergée parent se trouve dans l'emplacement central sur site et les sous-domaines sont délégués à des serveurs de noms hébergés en Europe, en Asie et en Amérique du Nord. Toutes les requêtes DNS sont transmises via le résolveur Route 53.

Suivez les étapes décrites dans les exemples pour configurer votre DNS local et le résolveur Route 53.

Configuration du DNS sur site

1. Pour le serveur de noms local situé dans la région centrale sur site :

   - Zone hébergée par le parent : `hr.example.com`

     Zone hébergée`hr.example.com`, adresse IP NS : `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. Pour le serveur de noms local de la région Europe sur site (la configuration des serveurs de noms d'Europe, d'Asie et d'Amérique du Nord est la même que pour la zone hébergée privée vers la délégation sortante) :

   - Zone hébergée : `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. Pour le serveur de noms local de la région Asie sur site :

   Zone hébergée :`apac.hr.example.com`, `10.0.0.40`

   Le serveur de noms apac peut déléguer le sous-domaine à d'autres serveurs de noms.

```
$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
```

   Zone hébergée :`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. Pour le serveur de noms local de la région Amérique du Nord :

   Zone hébergée : `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
```

Configuration du résolveur Route 53

- Pour le Route 53 Resolver, vous devez configurer des règles de transfert et des règles de délégation :

  Règles de transfert

  1. Pour transférer la demande initiale afin que les requêtes soient transmises à la zone hébergée parent située `hr.example.com` au centre :

     nom de domaine : target-ips : `hr.example.com` `10.0.0.20`
  2. Pour transférer l'enregistrement de out-of-zone délégation, le résolveur Route 53 connaisse l'adresse IP du serveur de noms délégué pour transférer la demande initiale :

     nom de domaine : target-ips : `hr.example.net` `10.0.0.50`

  Règles de délégation

  1. Règle de délégation pour la délégation en zone :

     dossier de délégation : `hr.example.com`
  2. Règle de délégation pour la délégation hors zone :

     enregistrement de délégation : `hr.example.net`

Activation de la validation DNSSEC dans Amazon Route 53

Lorsque vous activez la validation DNSSEC pour un cloud privé virtuel (VPC) dans Amazon Route 53, les signatures DNSSEC sont vérifiées cryptographiquement pour s'assurer que la réponse n'a pas été altérée. Vous activez la validation DNSSEC sur la page détaillée de votre VPC.

La validation DNSSEC est appliquée par le résolveur de Route 53 aux noms signés publics lorsqu'il effectue une résolution DNS récursive.

Toutefois, si le résolveur de Route 53 est transféré vers un autre résolveur DNS, ce résolveur effectue une résolution DNS récursive et doit donc également appliquer la validation DNSSEC.

> **Important**
>
> L'activation de la validation DNSSEC peut affecter la résolution DNS pour les registres DNS publics de ressources AWS dans un VPC, ce qui pourrait entraîner une panne. Sachez que l'activation ou la désactivation de la validation DNSSEC peut prendre plusieurs minutes.

> **Note**
>
> À l'heure actuelle, le Amazon Route 53 Resolver bit d'en-tête EDNS de votre VPC (alias AmazonProvided DNS) ignore le bit d'en-tête EDNS DO (DNSSEC OK) et le bit CD (Checking Disabled) de la requête DNS. Si vous avez configuré DNSSEC, cela signifie que, bien que Route 53 Resolver effectue la validation DNSSEC, il ne renvoie pas les enregistrements DNSSEC et n'active pas le bit AD dans la réponse. Par conséquent, l'exécution de votre propre validation DNSSEC n'est pas actuellement prise en charge par Route 53 Resolver. Si vous devez le faire, vous devrez effectuer votre propre résolution DNS récursive.

Pour activer la validation DNSSEC pour un VPC

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation, sous Resolver, choisissez VPCs.
3. Sous validation DNSSEC, cochez la case. Si la case est déjà cochée, vous pouvez la désactiver pour désactiver la validation DNSSEC.

   Sachez que l'activation ou la désactivation de la validation DNSSEC peut prendre plusieurs minutes.

Acheminement du trafic Internet vers vos AWS ressources

Vous pouvez utiliser Amazon Route 53 pour acheminer le trafic vers diverses AWS ressources.

- Acheminer le trafic vers une API Amazon API Gateway à l'aide de votre nom de domaine
- Acheminement du trafic vers une CloudFront distribution Amazon à l'aide de votre nom de domaine
- Acheminement du trafic vers une EC2 instance Amazon
- Acheminement du trafic vers un AWS App Runner service
- Acheminement du trafic vers un AWS Global Accelerator
- Acheminement du trafic vers un AWS Elastic Beanstalk environnement
- Routage du trafic vers un équilibreur de charge ELB
- Routage du trafic vers un site Web hébergé dans un compartiment Amazon S3
- Acheminer le trafic vers un point de terminaison d'interface Amazon Virtual Private Cloud à l'aide de votre nom de domaine
- Acheminement du trafic vers Amazon WorkMail
- Acheminement du trafic vers le point de terminaison du domaine Amazon OpenSearch Service
- Acheminement du trafic vers le point de terminaison du domaine du service Amazon VPC Lattice
- Acheminement du trafic vers d'autres AWS ressources
- Création d'Amazon Route 53 et de Amazon Route 53 Resolver ressources avec AWS CloudFormation

Acheminer le trafic vers une API Amazon API Gateway à l'aide de votre nom de domaine

Vous pouvez utiliser Amazon API Gateway pour créer, publier, gérer, surveiller et sécuriser APIs. Vous pouvez créer APIs ces AWS services d'accès ou d'autres services Web en plus des données stockées dans le AWS Cloud.

La méthode que vous utilisez pour acheminer le trafic du domaine vers une API API Gateway est la même, que vous ayez créé un point de terminaison API Gateway régional ou un point de terminaison API Gateway optimisé pour les périphériques. Si vous créez un point de terminaison API Gateway privé, le processus est légèrement différent.

- Point de terminaison d'API régional : vous créez un enregistrement d'alias Route 53 qui achemine le trafic vers le point de terminaison d'API régional.
- Point de terminaison d'API optimisé pour les périphériques : vous créez un enregistrement d'alias Route 53 qui achemine le trafic vers l'API optimisée pour les périphériques. Cela entraîne le routage du trafic vers la CloudFront distribution associée à l'API optimisée pour les périphériques.
- Point de terminaison d'API privé : vous créez un enregistrement d'alias Route 53 qui achemine le trafic vers votre point de terminaison d'API privé à l'aide d'un point de terminaison VPC d'interface pour API Gateway dans une zone hébergée privée.

Un enregistrement d'alias est une extension Route 53 de DNS similaire à un enregistrement CNAME. Pour plus d'informations sur la comparaison entre des enregistrements d'alias et des enregistrements CNAME, veuillez consulter Choix entre des enregistrements avec ou sans alias.

> **Note**
>
> Route 53 ne facture pas les requêtes d'alias adressées à API Gateway APIs ou à d'autres AWS ressources.

Rubriques

- Prérequis
- Configuration de Route 53 pour acheminer le trafic vers un point de terminaison API Gateway

Prérequis

Pour commencer, vous. devez disposer des éléments suivants :

- Une API API Gateway qui possède un nom de domaine personnalisé, comme api.example.com, qui correspond au nom de l'enregistrement Route 53 que vous souhaitez créer.

  Pour plus d’informations, consultez les rubriques suivantes :

  - Configuration de noms de domaine personnalisés pour HTTP APIs dans le manuel Amazon API Gateway Developer Guide.
  - Configuration de noms de domaine personnalisés pour REST APIs dans le manuel Amazon API Gateway Developer Guide.

- Configuration de noms de domaine personnalisés WebSocket APIs dans le manuel Amazon API Gateway Developer Guide.
- Noms de domaine personnalisés pour le domaine privé APIs dans API Gateway dans le manuel Amazon API Gateway Developer Guide.

- Un nom de domaine enregistré. Vous pouvez utiliser Amazon Route 53 en tant que bureau d'enregistrement de domaine, ou vous pouvez utiliser un autre bureau d'enregistrement.
- Route 53 en tant que service DNS pour le domaine. Si vous enregistrez votre nom de domaine à l'aide de Route 53, nous configurons automatiquement Route 53 en tant que service DNS pour le domaine.

  Pour en savoir plus sur l'utilisation de Route 53 comme fournisseur de service DNS pour votre domaine, consultez Configuration d'Amazon Route 53 en tant que service DNS d'un domaine existant.

Configuration de Route 53 pour acheminer le trafic vers un point de terminaison API Gateway

Pour configurer Route 53 pour acheminer le trafic vers un point de terminaison API Gateway, exécutez la procédure suivante.

Custom domain names for public APIs

La procédure suivante décrit comment acheminer le trafic vers un point de terminaison API Gateway pour un nom de domaine personnalisé destiné au public APIs.

Pour acheminer le trafic vers un point de terminaison API Gateway

1. Si vous avez créé la zone hébergée Route 53 et le point de terminaison à l'aide du même compte, passez à l'étape 2.

   Si vous avez créé la zone hébergée et le point de terminaison à l'aide de différents comptes, obtenez le nom de domaine cible pour le nom de domaine personnalisé que vous souhaitez utiliser :

   a. Connectez-vous à la console API Gateway AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/apigateway/.

b. Dans le panneau de navigation, sélectionnez Custom domain names (Noms de domaine personnalisés).

c. Sélectionnez le nom de domaine personnalisé que vous souhaitez utiliser et obtenez la valeur du nom de domaine de l'API Gateway.

2. Ouvrez la console Route 53 à l'adresse https://console.aws.amazon.com/route53/.
3. Dans le panneau de navigation, choisissez Zones hébergées.
4. Choisissez le nom de la zone hébergée qui a le nom de domaine que vous souhaitez utiliser pour acheminer le trafic vers votre API.
5. Choisissez Créer un registre.
6. Indiquez l'une des valeurs suivantes :

> **Important**
>
> Nous vous recommandons d'activer Alias. Pour les noms de domaine qui n'utilisent pas d'enregistrement Route 53 Alias, vous pouvez rencontrer des problèmes si vous utilisez un VPC avec un DNS privé activé pour appeler une API privée. Le DNS privé remplace le comportement de résolution DNS par défaut au sein du VPC, ce qui peut entraîner des conflits avec les enregistrements DNS externes.

Stratégie de routage

Choisissez la stratégie de routage applicable. Pour de plus amples informations, veuillez consulter Sélection d'une stratégie de routage.

Nom de l'enregistrement

Entrez le nom de domaine que vous souhaitez utiliser pour acheminer le trafic vers votre API.

L'API vers laquelle vous souhaitez acheminer le trafic doit inclure un nom de domaine personnalisé, comme api.example.com, qui correspond au nom de l'enregistrement Route 53.

Alias

Si vous utilisez la méthode de création d'enregistrement Quick create (Création rapide), activez Alias.

Valeur/acheminer le trafic vers

Choisissez Alias to API Gateway API (Alias vers API API Gateway), puis choisissez la région d'origine du point de terminaison.

La façon dont vous spécifiez la valeur pour Endpoint varie selon que vous avez créé la zone hébergée et l'API en utilisant le même AWS compte ou des comptes différents :

- Même compte — La liste des noms de domaine cibles inclut uniquement ceux APIs dont le nom de domaine personnalisé correspond à la valeur que vous avez spécifiée pour le nom de l'enregistrement. Choisissez la valeur applicable.
- Différents comptes : entrez la valeur que vous avez obtenue à l'étape 1 de cette procédure.

Type de registre

Choisissez A — IPv4 adresse.

Évaluer l'état de la cible

Pour contrôler le basculement DNS, configurez des surveillances de l'état personnalisés. Par exemple, consultez Configurer des surveillances de l'état personnalisés pour le basculement DNS dans le guide de l'utilisateur d'API Gateway.

7. Choisissez Créer des enregistrements.

   Les changements se propagent généralement sur tous les serveurs Route 53 en 60 secondes. Lorsque la propagation est terminée, vous pourrez acheminer le trafic vers votre API en utilisant le nom de l'enregistrement d'alias que vous avez créé au cours de cette procédure.

Custom domain names for private APIs

La procédure suivante décrit comment acheminer le trafic vers un point de terminaison API Gateway pour un nom de domaine personnalisé pour un domaine privé APIs.

Pour acheminer le trafic vers un point de terminaison API Gateway

1. Ouvrez la console Route 53 à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le panneau de navigation, choisissez Zones hébergées.

3. Choisissez le nom de la zone hébergée privée qui possède le nom de domaine que vous souhaitez utiliser pour acheminer le trafic vers votre API.
4. Choisissez Créer un registre.
5. Indiquez l'une des valeurs suivantes :

   Stratégie de routage

   Choisissez la stratégie de routage applicable. Pour de plus amples informations, veuillez consulter Sélection d'une stratégie de routage.

   Nom de l'enregistrement

   Entrez le nom de domaine que vous souhaitez utiliser pour acheminer le trafic vers votre API.

   L'API vers laquelle vous souhaitez acheminer le trafic doit inclure un nom de domaine personnalisé, comme api.example.com, qui correspond au nom de l'enregistrement Route 53.

   Alias

   Activez Alias.

   Valeur/acheminer le trafic vers

   Choisissez Alias to VPC Endpoint. Choisissez la région d'où provient le point de terminaison, puis sélectionnez votre point de terminaison VPC.

   Type de registre

   Si vous l'utilisez IPv6 pour votre point de terminaison VPC, créez un type d'enregistrement AAAA. Si vous utilisez une double pile pour votre point de terminaison de VPC, créez un enregistrement de type AAAA et un type d'enregistrement A.

   Évaluer l'état de la cible

   Pour contrôler le basculement DNS, configurez des surveillances de l'état personnalisés. Par exemple, consultez Configurer des surveillances de l'état personnalisés pour le basculement DNS dans le guide de l'utilisateur d'API Gateway.
6. Choisissez Créer des enregistrements.

   Les changements se propagent généralement sur tous les serveurs Route 53 en 60 secondes. Lorsque la propagation est terminée, vous pourrez acheminer le trafic vers

votre API en utilisant le nom de l'enregistrement d'alias que vous avez créé au cours de cette procédure.

Acheminement du trafic vers une CloudFront distribution Amazon à l'aide de votre nom de domaine

Vous pouvez utiliser Amazon CloudFront, le réseau de diffusion de AWS contenu (CDN), pour accélérer la diffusion de votre contenu Web. CloudFront peut diffuser l'intégralité de votre site Web, y compris le contenu dynamique, statique, en streaming et interactif, en utilisant un réseau mondial de sites périphériques. Les utilisateurs qui demandent votre contenu sont acheminés automatiquement vers l'emplacement périphérique qui leur offre la latence la plus faible.

> **Note**
>
> Vous pouvez acheminer le trafic vers une CloudFront distribution uniquement pour les zones hébergées publiques.

CloudFront Pour distribuer le contenu de votre site Web, créez une distribution et définissez ses paramètres. Par exemple, spécifiez le compartiment Amazon S3 ou le serveur HTTP CloudFront à partir duquel vous souhaitez obtenir votre contenu, si vous souhaitez que seuls les utilisateurs sélectionnés aient accès à votre contenu et si vous souhaitez que les utilisateurs utilisent le protocole HTTPS.

Lorsque vous créez une distribution, CloudFront attribuez un nom de domaine à la distribution, tel qued111111abcdef8.cloudfront.net. Vous pouvez utiliser ce nom de domaine URLs pour votre contenu, par exemple :

```
http://d111111abcdef8.cloudfront.net/logo.jpg
```

Vous pouvez également utiliser votre propre nom de domaine dans URLs, par exemple :

```
http://example.com/logo.jpg
```

Suivez les étapes décrites dans le guide du CloudFront développeur Amazon pour utiliser votre propre nom de domaine dans vos fichiers URLs dans une CloudFront distribution, au lieu du nom de domaine attribué à CloudFront votre distribution. Pour plus d'informations sur l'utilisation de votre

propre nom de domaine dans une CloudFront distribution, voir Utilisation de la personnalisation URLs en ajoutant des noms de domaine alternatifs (CNAMEs).

Lorsque vous utilisez un nom de domaine Route 53 avec une CloudFront distribution, utilisez Amazon Route 53 pour créer un enregistrement d'alias pointant vers votre CloudFront distribution. Un enregistrement d'alias est une extension de Route 53 au DNS. Il est similaire à un enregistrement CNAME, mais vous pouvez créer un enregistrement d'alias pour le domaine racine, par exemple, example.com, ainsi que pour les sous-domaines, par exemple www.example.com. (Vous pouvez créer des enregistrements CNAME uniquement pour les sous-domaines.) Lorsque Route 53 reçoit une requête DNS qui correspond au nom et au type d'un enregistrement d'alias, Route 53 répond avec le nom de domaine associé à votre distribution.

> **Note**
>
> Route 53 ne facture pas les requêtes d'alias adressées aux CloudFront distributions ou à d'autres AWS ressources.

Prérequis

Pour commencer, vous devez disposer des éléments suivants :

1. Un nom de domaine enregistré. Vous pouvez utiliser Amazon Route 53 en tant que bureau d'enregistrement de domaine, ou vous pouvez utiliser un autre bureau d'enregistrement.
2. Route 53 en tant que service DNS pour le domaine. Si vous enregistrez votre nom de domaine à l'aide de Route 53, nous configurons automatiquement Route 53 en tant que service DNS pour le domaine.

   Pour en savoir plus sur l'utilisation de Route 53 comme fournisseur de service DNS pour votre domaine, consultez Configuration d'Amazon Route 53 en tant que service DNS d'un domaine existant.
3. Demandez un certificat public afin que les CloudFront distributions Amazon nécessitent le protocole HTTPS. Pour plus d'informations, consultez Étape 2 : demander un certificat public et Validation DNS dans AWS Certificate Managerdans le Guide de l'utilisateur AWS Certificate Manager .
4. Un CloudFront distributeur ou un locataire CloudFront de distribution. La distribution doit inclure un autre nom de domaine correspondant au nom de domaine que vous souhaitez utiliser pour

votre distribution URLs au lieu du nom de domaine CloudFront attribué à votre distribution. Pour un tenant de CloudFront distribution, il doit contenir le nom de domaine que vous souhaitez utiliser pour votre URLs.

Par exemple, si vous souhaitez que votre contenu contienne le nom de domaine exemple.com, le champ Nom de domaine alternatif de la distribution doit inclure exemple.com. URLs

Pour plus d'informations, consultez la documentation suivante dans le manuel Amazon CloudFront Developer Guide :

- Liste des tâches de création d'une distribution
- Création ou mise à jour d'une distribution à l'aide de la console CloudFront

Configuration d'Amazon Route 53 pour acheminer le trafic vers une CloudFront distribution

Pour configurer Amazon Route 53 afin d'acheminer le trafic vers une CloudFront distribution, procédez comme suit. Pour plus d'informations sur l'utilisation de votre propre nom de domaine dans une CloudFront distribution, consultez la section Utilisation personnalisée URLs en ajoutant des noms de domaine alternatifs (CNAMEs) dans le manuel Amazon CloudFront Developer Guide.

> **Note**
>
> Les changements se propagent généralement sur tous les serveurs Route 53 en 60 secondes. Lorsque les modifications se propageront, vous pourrez acheminer le trafic vers votre CloudFront distribution en utilisant le nom de l'enregistrement d'alias que vous créez dans cette procédure.

Pour acheminer le trafic vers une distribution CloudFront

1. Obtenez le nom de domaine CloudFront attribué à votre distribution et déterminez s'il IPv6 est activé :

   a. Connectez-vous à la CloudFront console AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.

   b. Dans la colonne ID, sélectionnez le nom lié de la distribution vers laquelle vous souhaitez acheminer le trafic (et non la case à cocher).

c. Dans l'onglet General (Général), obtenez la valeur du champ Distribution Domain name (Nom de domaine de distribution).

d. Dans l'onglet Général, dans la section Paramètres, choisissez Modifier et faites défiler la page pour vérifier si le IPv6champ IPv6 est activé pour la distribution. Si cette option IPv6 est activée, vous devez créer deux enregistrements d'alias pour la distribution, l'un pour acheminer le IPv4 trafic vers la distribution et l'autre pour acheminer le IPv6 trafic. Choisissez Cancel (Annuler).

   Pour plus d'informations, consultez la section Activer IPv6 dans la rubrique Valeurs que vous spécifiez lorsque vous créez ou mettez à jour une distribution dans le manuel Amazon CloudFront Developer Guide.

2. Pour un locataire du CloudFront service de distribution,

   a. Choisissez SaaS dans le menu de navigation de gauche, puis Distribution tenants, puis choisissez le locataire de distribution avec le nom de domaine vers lequel vous souhaitez acheminer le trafic

   b. dans la section Informations générales, copiez la valeur du point de terminaison.

3. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.

4. Dans le panneau de navigation, choisissez Zones hébergées.

5. Choisissez le nom associé de la zone hébergée pour le domaine que vous souhaitez utiliser pour acheminer le trafic vers votre CloudFront distribution.

6. Choisissez Créer un registre.

   Vous pouvez utiliser l'assistant pour créer les enregistrements ou choisir Switch to quick create (Passer à la création rapide).

7. Indiquez l’une des valeurs suivantes :

   Stratégie de routage

   Choisissez la stratégie de routage applicable. Pour de plus amples informations, veuillez consulter Sélection d'une stratégie de routage.

   Nom de l'enregistrement

   Entrez le nom de domaine que vous souhaitez utiliser pour acheminer le trafic vers votre CloudFront distribution. La valeur par défaut est le nom de la zone hébergée.

Par exemple, si le nom de la zone hébergée est example.com et si vous souhaitez utiliser acme.example.com pour acheminer le trafic vers votre distribution, entrez acme.

Alias

Si vous utilisez la méthode de création d'enregistrement Quick create (Création rapide), activez Alias.

> **Important**
>
> Vous devez créer un enregistrement Alias pour que la CloudFront distribution fonctionne.

Valeur/acheminer le trafic vers

Choisissez Alias pour CloudFront les distributions. La région us-east-1 est sélectionnée par défaut. Choisissez le nom de domaine CloudFront attribué à la distribution lorsque vous l'avez créée. Il s'agit de la valeur obtenue à l'étape 1.

Pour un locataire CloudFront de distribution, choisissez le point de terminaison à l'étape 2.

Type de registre

Choisissez A — IPv4 adresse.

Si la distribution IPv6 est activée et que vous créez un deuxième enregistrement, choisissez AAAA — IPv6 adresse.

Évaluer l'état de la cible

Acceptez la valeur par défaut de No (Non).

8. Choisissez Créer des enregistrements.
9. Si cette option IPv6 est activée pour la distribution, répétez les étapes 5 à 7. Spécifiez les mêmes paramètres, sauf pour le champ Type d'enregistrement, comme indiqué à l'étape 6.

Acheminement du trafic vers une EC2 instance Amazon

Amazon EC2 fournit une capacité de calcul évolutive dans le AWS cloud. Vous pouvez lancer un environnement informatique EC2 virtuel (une instance) à l'aide d'un modèle préconfiguré (Amazon

Machine Image ou AMI). Lorsque vous lancez une EC2 instance, le système d'exploitation (Linux ou Microsoft Windows) et les logiciels supplémentaires inclus dans l'AMI, tels que le serveur Web ou le logiciel de base de données, sont EC2 automatiquement installés.

Vous pouvez acheminer le trafic de votre domaine, tel que example.com, vers votre serveur à l'aide d'Amazon Route 53, si vous hébergez un site Web ou si vous exécutez une application Web sur une EC2 instance.

Prérequis

Pour commencer, vous devez disposer des éléments suivants :

- Une EC2 instance Amazon. Pour plus d'informations sur le lancement d'une EC2 instance, consultez la documentation suivante :
  - Linux — Consultez Getting started with Amazon EC2 Linux instances dans le guide de EC2 l'utilisateur Amazon
  - Microsoft Windows — Consultez Getting started with Amazon EC2 Windows instances dans le guide de EC2 l'utilisateur Amazon

  > **Important**
  >
  > Nous vous recommandons également de créer une adresse IP élastique et de l'associer à votre EC2 instance. Une adresse IP élastique garantit que l'adresse IP de votre EC2 instance Amazon ne changera jamais. Pour plus d'informations, consultez Tarification des adresses IP élastiques.

- Un nom de domaine enregistré. Vous pouvez utiliser Amazon Route 53 en tant que bureau d'enregistrement de domaine, ou vous pouvez utiliser un autre bureau d'enregistrement.
- Route 53 en tant que service DNS pour le domaine. Si vous enregistrez votre nom de domaine à l'aide de Route 53, nous configurons automatiquement Route 53 en tant que service DNS pour le domaine.

  Pour en savoir plus sur l'utilisation de Route 53 comme fournisseur de service DNS pour votre domaine, consultez Configuration d'Amazon Route 53 en tant que service DNS d'un domaine existant.

Configuration d'Amazon Route 53 pour acheminer le trafic vers une EC2 instance Amazon

Pour configurer Amazon Route 53 afin d'acheminer le trafic vers une EC2 instance, effectuez la procédure suivante.

Pour acheminer le trafic vers une EC2 instance Amazon

1. Obtenez l'adresse IP de l' EC2 instance Amazon :
   a. Connectez-vous à la EC2 console Amazon AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/ec2/.
   b. Dans la liste des régions située dans le coin supérieur droit de la console, choisissez la région dans laquelle vous avez lancé l'instance.
   c. Dans le panneau de navigation, choisissez Instances.
   d. Dans le tableau, choisissez l'instance vers laquelle vous souhaitez acheminer le trafic.
   e. Dans le volet inférieur, sous l'onglet Description, obtenez la valeur d'Elastic IPs.

      Si vous n'avez pas associé d'adresse IP élastique à l'instance, obtenez la valeur de l'adresse IP IPv4 publique.
2. Ouvrez la console Route 53 à l'adresse https://console.aws.amazon.com/route53/.
3. Dans le panneau de navigation, choisissez Zones hébergées.
4. Choisissez le nom de la zone hébergée qui correspond au nom du domaine pour lequel vous souhaitez acheminer le trafic.
5. Choisissez Créer un registre.
6. Indiquez l’une des valeurs suivantes :

   Stratégie de routage

   Choisissez la stratégie de routage applicable. Pour de plus amples informations, veuillez consulter Sélection d'une stratégie de routage.

   Nom de l'enregistrement

   Entrez le nom de domaine que vous souhaitez utiliser pour acheminer le trafic vers votre EC2 instance. La valeur par défaut est le nom de la zone hébergée.

Par exemple, si le nom de la zone hébergée est example.com et que vous souhaitez utiliser acme.example.com pour acheminer le trafic vers votre EC2 instance, entrez acme.

Valeur/acheminer le trafic vers

Choisissez IP address or another value depending on the record type (Adresse IP ou autre valeur selon le type d'enregistrement). Entrez l'adresse IP que vous avez obtenue à l'étape 1.

Type de registre

Choisissez A — IPv4 adresse.

TTL (secondes)

Acceptez la valeur par défaut 300.

7. Choisissez Créer des enregistrements.

   Les changements se propagent généralement sur tous les serveurs Route 53 en 60 secondes. Une fois la propagation terminée, vous pourrez acheminer le trafic vers votre EC2 instance en utilisant le nom de l'enregistrement que vous avez créé dans cette procédure.

> **Important**
>
> Si vous libérez l'adresse IP Elastic, assurez-vous de supprimer également l'enregistrement DNS pointant vers celle-ci. Sinon, vous aurez un enregistrement DNS suspendu qui pourra être pris par un utilisateur non autorisé.

Acheminement du trafic vers un AWS App Runner service

AWS App Runner est un service entièrement géré qui permet aux développeurs de déployer facilement des applications Web conteneurisées APIs à grande échelle, sans aucune expérience préalable en matière d'infrastructure. Commencez par votre code source ou une image de conteneur. App Runner crée et déploie automatiquement l'application Web, équilibre la charge du trafic grâce au chiffrement, s'adapte à vos besoins en matière de trafic et permet à vos services de communiquer facilement avec d'autres AWS services et applications exécutés dans un Amazon VPC privé. Avec App Runner, plutôt que de penser aux serveurs ou à la mise à l'échelle, vous avez plus de temps pour vous concentrer sur vos applications. Pour plus d'informations, veuillez consulter la rubrique Présentation de AWS App Runner dans le Guide du développeur AWS App Runner .

> **Important**
>
> Amazon Route 53 prend actuellement en charge les enregistrements d'alias pour les AWS App Runner services créés après le 1er août 2022.

Pour acheminer le trafic de domaine vers un service App Runner, utilisez Amazon Route 53 pour créer un enregistrement d'alias qui pointe vers votre service App Runner. Un enregistrement d'alias est une extension de Route 53 au DNS. Il est similaire à un enregistrement CNAME, mais vous pouvez créer un enregistrement d'alias pour le domaine racine, par exemple, example.com, ainsi que pour les sous-domaines, par exemple www.example.com (http://www.example.com/). Vous pouvez créer des enregistrements CNAME uniquement pour les sous-domaines.

> **Note**
>
> Route 53 ne facture pas les requêtes d'alias pour le service App Runner ou autres ressources AWS .

Prérequis

Pour commencer, vous. devez disposer des éléments suivants :

- Un service App Runner. Pour plus d'informations sur la création d'un service App Runner, consultez Débuter avec App Runner.
- Un nom de domaine enregistré. Vous pouvez utiliser Amazon Route 53 en tant que bureau d'enregistrement de domaine, ou vous pouvez utiliser un autre bureau d'enregistrement.
- Route 53 en tant que service DNS pour le domaine. Si vous enregistrez votre nom de domaine à l'aide de Route 53, nous configurons automatiquement Route 53 en tant que service DNS pour le domaine.

  Pour en savoir plus sur l'utilisation de Route 53 comme fournisseur de service DNS pour votre domaine, consultez Configuration d'Amazon Route 53 en tant que service DNS d'un domaine existant.
- Associez le domaine personnalisé à votre service App Runner. Pour plus d'informations, consultez Gestion des noms de domaine personnalisés pour App Runner.

- Configurez l'enregistrement de validation du certificat renvoyé par App Runner à votre zone hébergée Route 53 pour démarrer le processus de validation du domaine. Pour plus d'informations, consultez Validation DNS dans AWS Certificate Manager dans le Guide de l'utilisateur AWS Certificate Manager .

Configuration d'Amazon Route 53 pour acheminer le trafic vers un service App Runner

Pour configurer Amazon Route 53 pour acheminer le trafic vers une un service App Runner, exécutez la procédure suivante.

Pour acheminer le trafic vers un service App Runner

1. Ouvrez la console Route 53 à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le panneau de navigation, choisissez Zones hébergées.
3. Choisissez le nom de la zone hébergée qui correspond au nom du domaine pour lequel vous souhaitez acheminer le trafic.
4. Choisissez Créer un registre.
5. Indiquez l'une des valeurs suivantes :

   Stratégie de routage

   Choisissez la stratégie de routage applicable. Pour de plus amples informations, veuillez consulter Sélection d'une stratégie de routage.

   Nom de l'enregistrement

   Saisissez le nom de domaine que vous souhaitez utiliser pour acheminer le trafic vers votre service App Runner. La valeur par défaut est le nom de la zone hébergée.

   Par exemple, si le nom de la zone hébergée est example.com et si vous souhaitez utiliser acme.example.com pour acheminer le trafic vers votre service, saisissez acme.

   Valeur/acheminer le trafic vers

   Choisissez Alias to App Runner Service (Alias du service App Runner), puis la Région AWS. Choisissez le nom de domaine de l'environnement vers lequel vous souhaitez acheminer le trafic.

Type de registre

Acceptez la valeur par défaut, A — IPv4 adresse.

Évaluer l'état de la cible

Acceptez la valeur par défaut de Yes (Oui).

6. Choisissez Créer des enregistrements.

   Les changements se propagent généralement sur tous les serveurs Route 53 en 60 secondes. Lorsque la propagation est terminée, vous pourrez acheminer le trafic vers votre service App Runner en utilisant le nom de l'enregistrement d'alias que vous avez créé au cours de cette procédure.

Acheminement du trafic vers un AWS Global Accelerator

AWS Global Accelerator est un service dans lequel vous créez des accélérateurs afin d'améliorer les performances de vos applications pour les utilisateurs locaux et internationaux. Le service réagit instantanément aux changements de santé ou de configuration pour garantir que le trafic Internet des clients est toujours dirigé vers des terminaux sains. Global Accelerator inclut une architecture tolérante aux pannes AWS Shield Standard, et intègre, pour une atténuation automatique en ligne des attaques DDo S. Pour plus d'informations, consultez la section Qu'est-ce que Global Accelerator dans le guide du AWS Global Accelerator développeur.

Par défaut, Global Accelerator vous fournit des adresses IP statiques que vous associez à votre accélérateur. Les adresses IP statiques sont diffusées en mode anycast depuis le réseau AWS périphérique. Les accélérateurs incluent un nom DNS par défaut, mais dans la plupart des scénarios, vous pouvez configurer le DNS pour qu'il utilise votre nom de domaine personnalisé (tel que www.exemple.com) avec votre accélérateur, au lieu d'utiliser les adresses IP statiques attribuées ou le nom DNS par défaut.

> **Note**
>
> Route 53 ne facture pas les requêtes d'alias adressées à Global Accelerator ou à d'autres AWS ressources.

Prérequis

Pour commencer, vous devez disposer des éléments suivants :

- Un accélérateur. Vous pouvez créer un accélérateur standard ou un accélérateur de routage personnalisé. Pour plus d'informations, voir Création d'un accélérateur standard et Création d'un accélérateur de routage personnalisé.
- Un nom de domaine enregistré. Vous pouvez utiliser Amazon Route 53 en tant que bureau d'enregistrement de domaine, ou vous pouvez utiliser un autre bureau d'enregistrement.
- Route 53 en tant que service DNS pour le domaine. Si vous enregistrez votre nom de domaine à l'aide de Route 53, nous configurons automatiquement Route 53 en tant que service DNS pour le domaine.

  Pour en savoir plus sur l'utilisation de Route 53 comme fournisseur de service DNS pour votre domaine, consultez Configuration d'Amazon Route 53 en tant que service DNS d'un domaine existant.

Configuration d'Amazon Route 53 pour acheminer le trafic vers un accélérateur

Pour configurer Amazon Route 53 afin d'acheminer le trafic vers un accélérateur, effectuez la procédure suivante.

Pour acheminer le trafic vers un accélérateur

1. Ouvrez la console Route 53 à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le panneau de navigation, choisissez Zones hébergées.
3. Choisissez le nom de la zone hébergée qui correspond au nom du domaine pour lequel vous souhaitez acheminer le trafic.
4. Choisissez Créer un registre.
5. Indiquez l’une des valeurs suivantes :

   Stratégie de routage

   Choisissez la stratégie de routage applicable. Pour de plus amples informations, veuillez consulter Sélection d'une stratégie de routage.

Nom de l'enregistrement

Entrez le nom de domaine que vous souhaitez utiliser pour acheminer le trafic vers votre accélérateur. La valeur par défaut est le nom de la zone hébergée.

Par exemple, si le nom de la zone hébergée est example.com et que vous souhaitez utiliser acme.example.com pour acheminer le trafic vers votre accélérateur global, entrez acme.

Valeur/acheminer le trafic vers

Choisissez Alias to Global Accelerator, puis choisissez le Région AWS. Choisissez le nom DNS de l'accélérateur.

Vous pouvez saisir le nom DNS d'un accélérateur que vous avez créé à l'aide de l'accélérateur actuel Compte AWS ou à l'aide d'un autre Compte AWS.

Type de registre

Acceptez la valeur par défaut, A — IPv4 adresse.

Évaluer l'état de la cible

Acceptez la valeur par défaut de Yes (Oui).

6. Choisissez Créer des enregistrements.

   Les changements se propagent généralement sur tous les serveurs Route 53 en 60 secondes. Une fois la propagation terminée, vous pourrez acheminer le trafic vers votre accélérateur en utilisant le nom de l'enregistrement d'alias que vous avez créé dans cette procédure.

Acheminement du trafic vers un AWS Elastic Beanstalk environnement

Si vous utilisez Amazon Route 53 AWS Elastic Beanstalk pour déployer et gérer des applications dans le AWS cloud, vous pouvez utiliser Amazon Route 53 pour acheminer le trafic DNS de votre domaine, tel que example.com, vers un environnement Elastic Beanstalk nouveau ou existant.

Pour acheminer le trafic DNS vers un environnement Elastic Beanstalk, consultez les procédures décrites dans les rubriques suivantes.

> **Note**
>
> Ces procédures supposent que vous utilisez déjà Route 53 en tant que service DNS pour votre domaine. Si vous utilisez un autre service DNS, consultez Configuration d'Amazon Route 53 en tant que service DNS d'un domaine existant pour en savoir plus sur l'utilisation de Route 53 comme fournisseur de service DNS pour votre domaine.

Rubriques

- Déploiement d'une application dans un environnement Elastic Beanstalk
- Obtention du nom de domaine pour votre environnement Elastic Beanstalk
- Création d'un enregistrement Amazon Route 53 qui achemine le trafic vers votre environnement Elastic Beanstalk

Déploiement d'une application dans un environnement Elastic Beanstalk

Si vous avez déjà un environnement Elastic Beanstalk vers lequel vous souhaitez acheminer le trafic, passez à la section Obtention du nom de domaine pour votre environnement Elastic Beanstalk.

Pour créer une application et la déployer dans un environnement Elastic Beanstalk

- Pour plus d'informations sur la création d'une application et son déploiement dans un environnement Elastic Beanstalk, consultez la section Mise en route avec Elastic Beanstalk dans le Guide du développeur AWS Elastic Beanstalk .

Obtention du nom de domaine pour votre environnement Elastic Beanstalk

Si vous connaissez déjà le nom de domaine de votre environnement Elastic Beanstalk, passez à la section Création d'un enregistrement Amazon Route 53 qui achemine le trafic vers votre environnement Elastic Beanstalk.

Pour obtenir le nom de domaine pour votre environnement Elastic Beanstalk

1. Connectez-vous à la console Elastic Beanstalk AWS Management Console et ouvrez-la à l'adresse. https://console.aws.amazon.com/elasticbeanstalk/

2. Dans la liste des applications, trouvez l'application vers laquelle vous souhaitez acheminer le trafic et notez la valeur de URL. Si vous n'apercevez pas la liste des applications, choisissez Applications, dans le panneau de navigation.

   Pour plus d'informations sur l'URL, veuillez consulter la section Nom de domaine de l'environnement Elastic Beanstalk dans le Guide du développeur Elastic Beanstalk.

Création d'un enregistrement Amazon Route 53 qui achemine le trafic vers votre environnement Elastic Beanstalk

Un enregistrement Amazon Route 53 contient les paramètres qui contrôlent la façon dont le trafic est acheminé vers votre environnement Elastic Beanstalk. Vous créez un enregistrement CNAME ou un enregistrement d'alias. Cela dépend si le nom de domaine de l'environnement comprend la région, par exemple us-east-2, dans laquelle vous avez déployé l'environnement. Les nouveaux environnements incluent la région dans le nom de domaine, ce qui n'est pas le cas des environnements créés avant le début de l'année 2016. Pour obtenir une comparaison des enregistrements CNAME et d'alias, consultez Choix entre des enregistrements avec ou sans alias.

Si le nom de domaine n'inclut pas la région

Vous devez créer un enregistrement CNAME. Toutefois, en raison des limites imposées par DNS, vous ne pouvez créer des enregistrements CNAME que pour les sous-domaines, et pas pour le nom de domaine racine. Par exemple, si votre nom de domaine est example.com, vous pouvez créer un enregistrement qui achemine le trafic pour acme.example.com vers votre environnement Elastic Beanstalk, mais vous ne pouvez pas créer d'enregistrement qui achemine le trafic pour example.com vers votre environnement Elastic Beanstalk.

Consultez la procédure Pour créer un enregistrement CNAME afin d'acheminer le trafic vers un environnement Elastic Beanstalk.

Si le nom de domaine inclut la région

Vous pouvez créer un enregistrement d'alias. Un enregistrement d'alias est spécifique à Route 53 et présente deux avantages importants par rapport aux enregistrements CNAME :

- Vous pouvez créer des enregistrements d'alias pour le nom de domaine racine ou pour des sous-domaines. Par exemple, si votre nom de domaine est example.com, vous pouvez créer un enregistrement qui achemine les demandes pour example.com ou pour acme.example.com vers votre environnement Elastic Beanstalk.

- Route 53 ne facture pas les demandes qui utilisent un enregistrement d'alias pour acheminer le trafic.

Consultez la procédure Pour créer un enregistrement d'alias Amazon Route 53 pour acheminer le trafic vers un environnement Elastic Beanstalk.

Pour créer un enregistrement CNAME afin d'acheminer le trafic vers un environnement Elastic Beanstalk

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le panneau de navigation, choisissez Zones hébergées.
3. Choisissez le nom de la zone hébergée à utiliser pour acheminer le trafic vers votre environnement Elastic Beanstalk.
4. Choisissez Créer un registre.
5. Choisissez Switch to quick create (Passer à la création rapide)
6. Indiquez l'une des valeurs suivantes :

   Stratégie de routage

   Choisissez la stratégie de routage applicable. Pour de plus amples informations, veuillez consulter Sélection d'une stratégie de routage.

   Nom de l'enregistrement

   Entrez le nom de domaine à utiliser pour acheminer le trafic vers votre environnement Elastic Beanstalk. La valeur par défaut est le nom de la zone hébergée.

   Par exemple, si le nom de la zone hébergée est example.com et si vous souhaitez utiliser acme.example.com pour acheminer le trafic vers votre environnement, entrez acme.

   > **Important**
   >
   > Vous ne pouvez pas créer un enregistrement CNAME portant le même nom que la zone hébergée.

Alias

Si vous utilisez la méthode de création d'enregistrement Quick create (Création rapide), activez Alias.

Valeur/acheminer le trafic vers

Choisissez IP address or another value depending on the record type (Adresse IP ou une autre valeur en fonction du type d'enregistrement) et entrez la valeur que vous obtenez lorsque vous exécutez la procédure dans la rubrique Obtention du nom de domaine pour votre environnement Elastic Beanstalk. Si vous avez utilisé différents comptes pour créer votre zone hébergée Route 53 et votre environnement Elastic Beanstalk. Entrez les attributs CNAME de l'environnement Elastic Beanstalk.

Type de registre

Choisissez CNAME.

TTL (secondes)

Acceptez la valeur par défaut 300.

7. Choisissez Créer des enregistrements.

   Les changements se propagent généralement sur tous les serveurs Route 53 en 60 secondes.

Pour créer un enregistrement d'alias Amazon Route 53 pour acheminer le trafic vers un environnement Elastic Beanstalk

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le panneau de navigation, choisissez Zones hébergées.
3. Choisissez le nom de la zone hébergée à utiliser pour acheminer le trafic vers votre environnement Elastic Beanstalk.
4. Choisissez Créer un registre.
5. Indiquez l’une des valeurs suivantes :

Stratégie de routage

Choisissez la stratégie de routage applicable. Pour de plus amples informations, veuillez consulter Sélection d'une stratégie de routage.

Nom de l'enregistrement

Entrez le nom de domaine à utiliser pour acheminer le trafic vers votre environnement Elastic Beanstalk. La valeur par défaut est le nom de la zone hébergée.

Par exemple, si le nom de la zone hébergée est example.com et si vous souhaitez utiliser acme.example.com pour acheminer le trafic vers votre environnement, entrez acme.

Valeur/acheminer le trafic vers

Choisissez Alias to Elastic Beanstalk environment (Alias vers l'environnement Elastic Beanstalk), puis choisissez la région d'origine du point de terminaison. Choisissez le nom de domaine de l'environnement vers lequel vous souhaitez acheminer le trafic. Il s'agit de la valeur que vous obtenez lorsque vous exécutez la procédure de la rubrique Obtention du nom de domaine pour votre environnement Elastic Beanstalk.

Si vous avez utilisé différents comptes pour créer votre zone hébergée Route 53 et votre environnement Elastic Beanstalk. Entrez l'attribut CNAME de l'environnement Elastic Beanstalk.

Type de registre

Acceptez la valeur par défaut, A — IPv4 adresse.

Évaluer l'état de la cible

Acceptez la valeur par défaut de Yes (Oui).

6. Choisissez Créer des enregistrements.

Les changements se propagent généralement sur tous les serveurs Route 53 en 60 secondes. Lorsque la propagation est terminée, vous êtes en mesure d'acheminer le trafic vers votre environnement Elastic Beanstalk en utilisant le nom de l'enregistrement d'alias que vous créez au cours de cette procédure.

Routage du trafic vers un équilibreur de charge ELB

Si vous hébergez un site Web sur plusieurs EC2 instances Amazon, vous pouvez répartir le trafic vers votre site Web entre les instances à l'aide d'un équilibreur de charge Elastic Load Balancing (ELB). Le service ELB adapte automatiquement l'équilibreur de charge au fur et à mesure que le trafic vers votre site web change au fil du temps. L'équilibreur de charge peut également surveiller l'état de ses instances enregistrées et n'acheminer le trafic de domaine qu'aux instances saines.

Pour acheminer le trafic de domaine vers un équilibreur de charge ELB, utilisez Amazon Route 53 afin de créer un enregistrement d'alias qui pointe sur votre équilibreur de charge. Un enregistrement d'alias est une extension de Route 53 au DNS. Il est similaire à un enregistrement CNAME, mais vous pouvez créer un enregistrement d'alias pour le domaine racine, par exemple, example.com, ainsi que pour les sous-domaines, par exemple www.example.com. (Vous pouvez créer des enregistrements CNAME uniquement pour les sous-domaines.)

> **Note**
>
> Route 53 ne facture pas les requêtes d'alias pour les équilibreurs de charge ELB ou autres ressources AWS .

Prérequis

Pour commencer, vous. devez disposer des éléments suivants :

- Un équilibreur de charge ELB. Vous pouvez utiliser un Classic, Application ou Network Load Balancer ELB. Pour plus d'informations sur la création d'un équilibreur de charge, consultez Prise en main d'Elastic Load Balancing dans le Guide de l'utilisateur Elastic Load Balancing.

  Attribuez à l'équilibreur de charge un nom qui vous aidera à vous souvenir de son objet ultérieurement. Le nom que vous spécifiez lorsque vous créez un équilibreur de charge est le nom que vous choisissez lorsque vous créez un enregistrement d'alias dans la console Route 53.
- Un nom de domaine enregistré. Vous pouvez utiliser Route 53 en tant que bureau d'enregistrement de domaine, ou vous pouvez utiliser un autre bureau d'enregistrement.
- Route 53 en tant que service DNS pour le domaine. Si vous enregistrez votre nom de domaine à l'aide de Route 53, nous configurons automatiquement Route 53 en tant que service DNS pour le domaine.

Pour en savoir plus sur l'utilisation de Route 53 comme fournisseur de service DNS pour votre domaine, consultez Configuration d'Amazon Route 53 en tant que service DNS d'un domaine existant.

Configuration d'Amazon Route 53 pour acheminer le trafic vers un équilibreur de charge ELB

Pour configurer Amazon Route 53 pour acheminer le trafic vers un équilibreur de charge ELB, exécutez la procédure suivante.

Pour acheminer le trafic vers un équilibreur de charge ELB

1. Si vous avez créé la zone hébergée Route 53 et un équilibreur de charge ELB à l'aide du même compte, passez directement à l'étape 2.

   Si vous avez créé la zone hébergée et l'équilibreur de charge ELB à l'aide de différents comptes, exécutez la procédure Obtention du nom DNS d'un équilibreur de charge Elastic Load Balancing pour obtenir le nom DNS de l'équilibreur de charge.
2. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
3. Dans le panneau de navigation, choisissez Zones hébergées.
4. Choisissez le nom de la zone hébergée qui a le nom de domaine que vous souhaitez utiliser pour acheminer le trafic vers votre équilibreur de charge.
5. Choisissez Créer un registre.
6. Indiquez l’une des valeurs suivantes :

   Stratégie de routage

   Choisissez la stratégie de routage applicable. Pour de plus amples informations, veuillez consulter Sélection d'une stratégie de routage.

   Nom de l'enregistrement

   Entrez le nom de domaine ou du sous-domaine que vous souhaitez utiliser pour acheminer le trafic vers votre équilibreur de charge ELB. La valeur par défaut est le nom de la zone hébergée.

Par exemple, si le nom de la zone hébergée est example.com et si vous souhaitez utiliser acme.example.com pour acheminer le trafic vers votre équilibreur de charge, entrez acme.

Alias

Si vous utilisez la méthode de création d'enregistrement Quick create (Création rapide), activez Alias.

Valeur/acheminer le trafic vers

Choisissez Alias to Application and Classic Load Balancer (Alias vers l'application et Classic Load Balancer) ou Alias to Network Load Balancer (Alias vers le dispositif d'équilibrage de charge de réseau, puis choisissez la région d'origine du point de terminaison.

Si vous avez créé la zone hébergée et l'équilibreur de charge ELB avec le même AWS compte, choisissez le nom DNS que vous avez attribué à l'équilibreur de charge lors de sa création.

Si vous avez créé la zone hébergée et l'équilibreur de charge ELB à l'aide de différents comptes, entrez la valeur que vous avez obtenue à l'étape 1 de cette procédure.

> **Note**
>
> La console préajoute dualstack. au nom DNS de l'application et au Classic Load Balancer à partir du même AWS compte uniquement. Lorsqu'un client, tel qu'un navigateur Web, demande l'adresse IP de votre nom de domaine (exemple.com) ou de votre nom de sous-domaine (www.exemple.com), le client peut demander une IPv4 adresse (enregistrement A), une IPv6 adresse (enregistrement AAAA), ou les deux IPv4 et des IPv6 adresses (dans des demandes distinctes avec la première). IPv4 La désignation dualstack. permet à Route 53 de répondre avec l'adresse IP appropriée pour votre équilibreur de charge en fonction du format d'adresse IP que le client a demandé. Vous aurez besoin de préparer dualstack. pour l'application et Classic Load Balancer à partir des différents comptes.

Type de registre

Choisissez A — IPv4 adresse.

Évaluer l'état de la cible

Si vous utilisez Route 53 pour acheminer le trafic en fonction de l'état de vos ressources, choisissez Yes (Oui). Pour plus d'informations sur la vérification de l'état de vos ressources, consultez la page Création de bilans de santé pour Amazon Route 53 .

7. Choisissez Créer des enregistrements.

Les changements se propagent généralement sur tous les serveurs Route 53 en 60 secondes. Lorsque la propagation est terminée, vous êtes en mesure d'acheminer le trafic vers votre équilibreur de charge en utilisant le nom de l'enregistrement d'alias que vous avez créé au cours de cette procédure.

Routage du trafic vers un site Web hébergé dans un compartiment Amazon S3

Amazon Simple Storage Service (Amazon S3) offre un stockage d'objet extrêmement évolutif, durable et sécurisé dans le cloud. Vous pouvez configurer un compartiment S3 pour héberger un site web statique qui peut inclure des pages web et des scripts côté client. (S3 ne prend pas en charge le scripting côté serveur).

Pour acheminer le trafic de domaine vers un compartiment S3, utilisez Amazon Route 53 pour créer un enregistrement d'alias qui pointe vers votre compartiment. Un enregistrement d'alias est une extension de Route 53 au DNS. Il est similaire à un enregistrement CNAME, mais vous pouvez créer un enregistrement d'alias pour le domaine racine, par exemple, example.com, ainsi que pour les sous-domaines, par exemple www.example.com. Vous pouvez créer des enregistrements CNAME uniquement pour les sous-domaines.

> **Note**
>
> Route 53 ne facture pas les requêtes d'alias vers les compartiments S3 ou d'autres AWS ressources.

Prérequis

Pour commencer, vous. devez disposer des éléments suivants. Si vous venez de vous inscrire à Amazon Route 53 ou S3, consultez la section Mise en route avec Amazon Route 53, qui vous guide

tout au long du processus, notamment l'enregistrement d'un nom de domaine, ainsi que la création et la configuration d'un compartiment S3.

- Un compartiment S3 configuré pour héberger un site Web statique.

  Pour de plus amples informations, veuillez consulter la section Configurer un compartiment pour l'hébergement de sites Web dans le Guide de l'utilisateur Amazon Simple Storage Service.

  > **Important**
  >
  > Le compartiment doit avoir le même nom que votre domaine ou sous-domaine. Par exemple, si vous souhaitez utiliser le sous-domaine acme.example.com, le nom du compartiment doit être acme.example.com.

  Vous pouvez acheminer le trafic pour un domaine et ses sous-domaines, comme example.com et www.example.com vers un seul compartiment. Créez un compartiment pour le domaine et chaque sous-domaine et configurez-les tous, sauf un pour rediriger le trafic vers le compartiment restant. Pour de plus amples informations, veuillez consulter Mise en route avec Amazon Route 53.

  > **Note**
  >
  > Un compartiment S3 configuré comme un point de terminaison de site web ne prend pas en charge SSL/TLS. Vous devez donc acheminer le trafic vers la distribution CloudFront et utiliser le compartiment S3 comme origine pour la distribution.
  > Pour obtenir des instructions sur la création d'une CloudFront distribution, voir Création d'une CloudFront distribution et Configuration de noms de domaine alternatifs et de HTTPS dans le Guide de CloudFront l'utilisateur, en plus deAcheminement du trafic vers une CloudFront distribution Amazon à l'aide de votre nom de domaine.

- Un nom de domaine enregistré. Vous pouvez utiliser Route 53 en tant que bureau d'enregistrement de domaine, ou vous pouvez utiliser un autre bureau d'enregistrement.
- Route 53 en tant que service DNS pour le domaine. Si vous enregistrez votre nom de domaine à l'aide de Route 53, nous configurons automatiquement Route 53 en tant que service DNS pour le domaine.

Pour en savoir plus sur l'utilisation de Route 53 comme fournisseur de service DNS pour votre domaine, consultez Configuration d'Amazon Route 53 en tant que service DNS d'un domaine existant.

Configuration d'Amazon Route 53 pour acheminer le trafic vers un compartiment S3

Pour configurer Amazon Route 53 pour acheminer le trafic vers un compartiment S3 configuré pour héberger un site Web statique, exécutez la procédure suivante.

Pour acheminer le trafic vers un compartiment S3

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le panneau de navigation, choisissez Zones hébergées.
3. Choisissez le nom de la zone hébergée qui a le nom de domaine que vous souhaitez utiliser pour acheminer le trafic vers votre compartiment S3.
4. Choisissez Créer un registre.
5. Indiquez l’une des valeurs suivantes :

   Stratégie de routage

   Choisissez la stratégie de routage applicable. Pour de plus amples informations, veuillez consulter Sélection d'une stratégie de routage.

   Nom de l'enregistrement

   Entrez le nom de domaine que vous souhaitez utiliser pour acheminer le trafic vers compartiment S3. La valeur par défaut est le nom de la zone hébergée.

   Par exemple, si le nom de la zone hébergée est example.com et si vous souhaitez utiliser acme.example.com pour acheminer le trafic vers votre compartiment, entrez acme.

   Alias

   Si vous utilisez la méthode de création d'enregistrement Quick create (Création rapide), activez Alias.

Valeur/acheminer le trafic vers

Choisissez Alias to S3 website endpoint (Alias vers le point de terminaison d'un site Web), puis choisissez la région d'origine du point de terminaison.

Choisissez le compartiment ayant le même nom que celui que vous avez indiqué pour Record name (Nom de l'enregistrement).

La liste inclut un compartiment uniquement si le compartiment satisfait aux exigences suivantes :

- Le nom du compartiment est le même que le nom de l'enregistrement que vous créez.
- Le compartiment est configuré comme point de terminaison d'un site web.
- Le bucket a été créé par le AWS compte courant.

  Si vous avez créé le compartiment à l'aide d'un autre AWS compte, entrez le nom de la région dans laquelle vous avez créé votre compartiment S3. Pour consulter le format correct du nom de la région, reportez-vous à la colonne Point de terminaison du site Web dans le tableau Points de terminaison du site Web Amazon S3 dans le Référence générale d'Amazon Web Services.

Type de registre

Choisissez A — IPv4 adresse.

Évaluer l'état de la cible

Acceptez la valeur par défaut de Yes (Oui).

6. Choisissez Créer des enregistrements.

   Les changements se propagent généralement sur tous les serveurs Route 53 en 60 secondes. Lorsque la propagation est terminée, vous êtes en mesure d'acheminer le trafic vers votre compartiment S3 en utilisant le nom de l'enregistrement d'alias que vous avez créé au cours de cette procédure.

Acheminer le trafic vers un point de terminaison d'interface Amazon Virtual Private Cloud à l'aide de votre nom de domaine

Vous pouvez l'utiliser AWS PrivateLink pour accéder à certains services via un point de terminaison d'interface Amazon Virtual Private Cloud (Amazon VPC). Ces services incluent certains AWS

services, des services hébergés par d'autres AWS clients et partenaires VPCs, ainsi que des services AWS Marketplace partenaires pris en charge.

Pour acheminer le trafic du domaine vers un point de terminaison d'interface, utilisez Amazon Route 53 pour créer un enregistrement d'alias. Un enregistrement d'alias est une extension de Route 53 au DNS. Il est similaire à un enregistrement CNAME, mais vous pouvez créer un enregistrement d'alias pour le domaine racine, par exemple, example.com, ainsi que pour les sous-domaines, par exemple www.example.com. Vous pouvez créer des enregistrements CNAME uniquement pour les sous-domaines.

> **Note**
>
> Route 53 ne facture pas les requêtes d'alias destinées aux points de terminaison d'interface ou à d'autres AWS ressources.

Rubriques

- Prérequis
- Configuration d'Amazon Route 53 pour acheminer le trafic vers un point de terminaison d'interface Amazon VPC.

Prérequis

Pour commencer, vous. devez disposer des éléments suivants :

- Un point de terminaison d'interface Amazon VPC. Pour de plus amples informations, consultez Points de terminaison VPC (AWS PrivateLink) dans le Guide de l'utilisateur Amazon VPC.
- Un nom de domaine enregistré. Vous pouvez utiliser Amazon Route 53 en tant que bureau d'enregistrement de domaine, ou vous pouvez utiliser un autre bureau d'enregistrement.
- Route 53 en tant que service DNS pour le domaine. Si vous enregistrez votre nom de domaine à l'aide de Route 53, nous configurons automatiquement Route 53 en tant que service DNS pour le domaine.

  Pour en savoir plus sur l'utilisation de Route 53 comme fournisseur de service DNS pour votre domaine, consultez Configuration d'Amazon Route 53 en tant que service DNS d'un domaine existant.

Configuration d'Amazon Route 53 pour acheminer le trafic vers un point de terminaison d'interface Amazon VPC.

Pour configurer Amazon Route 53 pour acheminer le trafic vers un point de terminaison d'interface Amazon VPC, exécutez la procédure suivante.

Pour acheminer le trafic vers un point de terminaison d'interface Amazon VPC

1. Si vous avez créé la zone hébergée Route 53 et le point de terminaison d'interface Amazon VPC à l'aide du même compte, passez à l'étape 2.

   Si vous avez créé la zone hébergée et le point de terminaison d'interface à l'aide de différents comptes, obtenez le nom de service pour le point de terminaison d'interface :

   a. Connectez-vous à la console Amazon VPC AWS Management Console et ouvrez-la à l'adresse. https://console.aws.amazon.com/vpc/
   b. Dans le volet de navigation, choisissez Points de terminaison.
   c. Dans le volet droit, choisissez le point de terminaison vers lequel vous souhaitez acheminer le trafic Internet.
   d. Dans le volet inférieur, obtenez la valeur de nom DNS, par exemple, vpce-0fd00dd593example-dexample.cloudtrail.us-west-2.vpce.amazonaws.com.
2. Ouvrez la console Route 53 à l'adresse https://console.aws.amazon.com/route53/.
3. Dans le panneau de navigation, choisissez Zones hébergées.
4. Choisissez le nom de la zone hébergée qui a le nom de domaine que vous souhaitez utiliser pour acheminer le trafic vers votre point de terminaison d'interface.
5. Choisissez Créer un registre.
6. Indiquez l’une des valeurs suivantes :

   Stratégie de routage

   Choisissez la stratégie de routage applicable. Pour de plus amples informations, veuillez consulter Sélection d'une stratégie de routage.

   Nom de l'enregistrement

   Entrez le nom de domaine que vous souhaitez utiliser pour acheminer le trafic vers votre point de terminaison d'interface Amazon VPC.

Alias

Si vous utilisez la méthode de création d'enregistrement Quick create (Création rapide), activez Alias.

Valeur/acheminer le trafic vers

Choisissez Alias to VPC endpoint (Alias vers point de terminaison d'un VPC), puis choisissez la région d'origine du point de terminaison.

La façon dont vous spécifiez la valeur pour les points de terminaison varie selon que vous avez créé la zone hébergée et le point de terminaison de l'interface en utilisant le même AWS compte ou des comptes différents :

- Même compte : choisissez la liste et trouvez la catégorie Amazon VPC endpoints (Points de terminaison d'un VPC Amazon). Ensuite, choisissez le nom DNS du point de terminaison d'interface vers lequel vous souhaitez acheminer le trafic Internet.
- Différents comptes : entrez la valeur que vous avez obtenue à l'étape 1 de cette procédure.

Type de registre

Choisissez A — IPv4 adresse.

Évaluer l'état de la cible

Acceptez la valeur par défaut de Yes (Oui).

7. Choisissez Créer des enregistrements.

   Les changements se propagent généralement sur tous les serveurs Route 53 en 60 secondes. Lorsque la propagation est terminée, vous êtes en mesure d'acheminer le trafic vers votre point de terminaison d'interface en utilisant le nom de l'enregistrement d'alias que vous avez créé au cours de cette procédure.

Acheminement du trafic vers Amazon WorkMail

Vous pouvez utiliser Route 53 pour acheminer le trafic vers votre domaine de WorkMail messagerie Amazon. Le nom de votre zone hébergée Route 53 (par exemple exemple.com) doit correspondre au nom d'un WorkMail domaine Amazon.

> **Note**
>
> Vous pouvez acheminer le trafic vers un WorkMail domaine Amazon uniquement pour les zones hébergées publiquement.

Pour acheminer le trafic vers Amazon WorkMail, effectuez les quatre procédures suivantes.

Pour configurer Amazon Route 53 en tant que service DNS et ajouter une WorkMail organisation Amazon et un domaine de messagerie

1. Si vous n'avez pas enregistré le nom de domaine que vous souhaitez utiliser dans vos adresses e-mail (par exemple, john@example.com), enregistrez le domaine maintenant afin de vérifier qu'il est disponible. Pour de plus amples informations, veuillez consulter Enregistrement d'un nouveau domaine.

   Si Amazon Route 53 n'est pas le service DNS du domaine de messagerie que vous avez ajouté à Amazon WorkMail, migrez le service DNS du domaine vers Route 53. Pour de plus amples informations, veuillez consulter Configuration d'Amazon Route 53 en tant que service DNS d'un domaine existant.
2. Ajoutez une WorkMail organisation Amazon et un domaine de messagerie. Pour plus d'informations, consultez Getting started pour les nouveaux utilisateurs dans le manuel Amazon WorkMail Administrator Guide.

Pour créer un enregistrement TXT Route 53 pour Amazon WorkMail

1. Dans le volet de navigation de la WorkMail console Amazon, sélectionnez Domains.
2. Choisissez le nom du domaine de messagerie, tel que exemple.com, que vous souhaitez utiliser pour acheminer le trafic vers Amazon WorkMail.
3. Ouvrez la console Route 53 dans un autre onglet du navigateur.
4. Dans la console Route 53, procédez comme suit :
   a. Dans le panneau de navigation, choisissez Hosted zones (Zones hébergées).
   b. Choisissez le nom de la zone hébergée que vous souhaitez utiliser pour votre domaine de WorkMail messagerie Amazon.

5. Dans la WorkMail console Amazon, dans la section Étape 1 : Vérifier la propriété du domaine, accédez à la colonne Nom d'hôte et copiez la partie de la valeur qui précède le nom de domaine de votre e-mail.

   Par exemple, si votre domaine de WorkMail messagerie Amazon est example.com et que la valeur de Hostname est _amazonses.example.com, copiez _amazonses.

6. Dans la console Route 53, procédez comme suit :

   a. Choisissez Create record (Créer un enregistrement), puis choisissez Simple routing (Routage simple).

   b. Pour Record name (Nom de l'enregistrement), collez la valeur que vous avez copiée à l'étape 5.

   c. Sous Record type (Type d'enregistrement), choisissez TXT – Text (TXT – Texte).

7. Dans la WorkMail console Amazon, pour l'enregistrement TXT, copiez la valeur de la colonne Value, y compris les guillemets.

8. Dans la console Route 53, procédez comme suit :

   a. Pour Value/Route traffic to (Valeur/acheminer le trafic vers), choisissez IP address or another value depending on the record type (Adresse IP ou une autre valeur en fonction du type d'enregistrement) et collez la valeur que vous avez copiée à l'étape 7.

      Ne modifiez aucun autre paramètre.

   b. Sélectionnez Create (Créer).

Pour créer un enregistrement MX Route 53 pour Amazon WorkMail

1. Dans la WorkMail console Amazon, dans la section Étape 2 : finaliser la configuration du domaine, accédez à la ligne dont le type d'enregistrement est MX et copiez la valeur de la colonne Valeur.

2. Dans la console Route 53, procédez comme suit :

   a. Choisissez Créer un registre.

   b. Pour Value/Route traffic to (Valeur/acheminer le trafic vers), choisissez IP address or another value depending on the record type (Adresse IP ou une autre valeur en fonction du type d'enregistrement) et collez la valeur que vous avez copiée à l'étape 1.

c. Pour Record type (Type d'enregistrement), choisissez MX – Mail Exchange (MX – Échange de courrier).

   Ne modifiez aucun autre paramètre.

d. Choisissez Créer des enregistrements.

Pour créer quatre enregistrements Route 53 CNAME pour Amazon WorkMail

1. Dans la WorkMail console Amazon, dans la section Étape 2 : Finaliser la configuration du domaine, accédez à la première ligne contenant un type d'enregistrement CNAME. Dans la colonne Hostname, copiez la partie qui précède votre nom de domaine de messagerie.

   Par exemple, si votre domaine de WorkMail messagerie Amazon est example.com et que la valeur de Hostname est autodiscover.example.com, copiez autodiscover.

2. Dans la console Route 53, procédez comme suit :

   a. Choisissez Créer un registre.

   b. Pour Record name (Nom de l'enregistrement), collez la valeur que vous avez copiée à l'étape 1.

   c. Pour Record type (Type d'enregistrement), choisissez CNAME – Canonical Name (CNAME – Nom canonique).

3. Dans la WorkMail console Amazon, dans la première ligne dont le type d'enregistrement est CNAME, copiez la valeur de la colonne Value.

4. Dans la console Route 53, procédez comme suit :

   a. Pour Value/Route traffic to (Valeur/acheminer le trafic vers), choisissez IP address or another value depending on the record type (Adresse IP ou une autre valeur en fonction du type d'enregistrement) et collez la valeur que vous avez copiée à l'étape 3.

      Ne modifiez aucun autre paramètre.

   b. Choisissez Créer des enregistrements.

5. Répétez les étapes 1 à 4 pour les enregistrements CNAME restants répertoriés dans la WorkMail console Amazon.

Acheminement du trafic vers le point de terminaison du domaine Amazon OpenSearch Service

Amazon OpenSearch Service est un service géré qui facilite le déploiement, l'exploitation et le dimensionnement de OpenSearch clusters dans le AWS Cloud. Un domaine de OpenSearch service est synonyme de cluster OpenSearch de services. Les domaines sont des clusters qui contiennent les paramètres, les types d'instances, le nombre d'instances et les ressources de stockage que vous spécifiez. Pour plus d'informations, consultez la section Qu'est-ce qu'Amazon OpenSearch Service dans le manuel Amazon OpenSearch Service Developer Guide.

Prérequis

Pour commencer, vous devez disposer des éléments suivants :

Un domaine de OpenSearch service doté d'un nom de domaine personnalisé, tel que exemple.com, qui correspond au nom de l'enregistrement Route 53 que vous souhaitez créer.

Pour plus d’informations, consultez les rubriques suivantes :

- Pour démarrer, consultez le manuel Amazon OpenSearch Service Developer Guide.
- Création d'un point de terminaison personnalisé dans le manuel Amazon OpenSearch Service Developer Guide.

Configuration d'Amazon Route 53 pour acheminer le trafic vers un point de terminaison OpenSearch de domaine Amazon Service

Pour utiliser Route 53 pour acheminer le trafic vers le OpenSearch service, vous devez d'abord obtenir le point de terminaison de domaine fourni par le OpenSearch service. Ce point de terminaison à double pile n'est fourni que si le point de terminaison personnalisé est activé sur un domaine de OpenSearch service en mode réseau à double pile. Pour plus d'informations, consultez la section Créer un point de terminaison personnalisé dans le manuel Amazon OpenSearch Service Developer Guide.

Pour acheminer le trafic vers un point de terminaison OpenSearch de service

1. Accédez à la console https://aws.amazon.comet choisissez Se connecter à la console.
2. Sous Analytics, sélectionnez Amazon OpenSearch Service.

3. Sous Clusters gérés, sélectionnez Domaines.
4. Sur la page Domaines, choisissez le nom du domaine vers lequel vous souhaitez acheminer le trafic.
5. Sur la page détaillée du domaine, copiez la valeur du point de terminaison de domaine v2 (double pile).
6. Ouvrez la console Route 53 à l'adresse https://console.aws.amazon.com/route53/.
7. Dans le panneau de navigation, choisissez Zones hébergées.
8. Choisissez le nom lié de la zone hébergée pour le domaine que vous souhaitez utiliser pour acheminer le trafic vers votre point de terminaison OpenSearch de service. Le nom de domaine doit correspondre au point de terminaison personnalisé défini dans OpenSearch Service.
9. Choisissez Créer un registre.

   Vous pouvez utiliser l'assistant pour créer les enregistrements ou choisir Switch to quick create (Passer à la création rapide).
10. Indiquez l'une des valeurs suivantes :

    Stratégie de routage

    Choisissez la stratégie de routage applicable. Pour de plus amples informations, veuillez consulter Sélection d'une stratégie de routage.

    Nom de l'enregistrement

    Entrez le nom de domaine que vous souhaitez utiliser pour acheminer le trafic vers le point de terminaison OpenSearch de votre domaine de service. La valeur par défaut est le nom de la zone hébergée.

    Par exemple, si le nom de la zone hébergée est example.com et si vous souhaitez utiliser acme.example.com pour acheminer le trafic vers votre distribution, entrez acme.

    Alias

    Si vous utilisez la méthode de création d'enregistrement Quick create (Création rapide), activez Alias.

    Valeur/acheminer le trafic vers

    Choisissez le point de terminaison OpenSearch du domaine Alias to Service. Choisissez la région dans laquelle le domaine de OpenSearch service a été créé, puis choisissez la valeur que vous avez obtenue à l'étape 5.

Type de registre

Choisissez A — IPv4 adresse, AAAA — IPv6 adresse ou les deux pour la double pile.

Évaluer l'état de la cible

Acceptez la valeur par défaut de Yes (Oui).

11. Choisissez Créer des enregistrements.

Acheminement du trafic vers le point de terminaison du domaine du service Amazon VPC Lattice

Amazon VPC Lattice est un service de mise en réseau d'applications entièrement géré que vous utilisez pour connecter, sécuriser et surveiller les services et les ressources de votre application. Vous pouvez utiliser VPC Lattice avec un seul cloud privé virtuel (VPC) ou sur plusieurs comptes VPCs . Pour plus d'informations, consultez la section Qu'est-ce qu'Amazon VPC Lattice dans le guide de l'utilisateur d'Amazon VPC Lattice.

Prérequis

Pour commencer, vous devez disposer des éléments suivants :

Un domaine de service VPC Lattice doté d'un nom de domaine personnalisé, tel que exemple.com, qui correspond au nom de l'enregistrement Route 53 que vous souhaitez créer.

Pour plus d'informations, consultez Associer un nom de domaine personnalisé à votre service dans le guide de l'utilisateur Amazon VPC Lattice.

Configuration d'Amazon Route 53 pour acheminer le trafic vers un point de terminaison de domaine du service VPC Lattice

Pour utiliser Route 53 pour acheminer le trafic vers le domaine de service Amazon VPC Lattice, vous devez d'abord obtenir le point de terminaison du service de domaine fourni par VPC Lattice. Pour plus d'informations, consultez Associer un nom de domaine personnalisé à votre service dans le guide de l'utilisateur Amazon VPC Lattice.

Pour acheminer le trafic vers le point de terminaison du domaine de service VPC Lattice

1. Accédez à la console https://aws.amazon.comet choisissez Se connecter à la console.

2. Sous Mise en réseau et diffusion de contenu, choisissez VPC.
3. Sous PrivateLink et Lattice, choisissez Lattice Services.
4. Créez un service VPC Lattice ou sélectionnez un service VPC Lattice existant.

> **Note**
>
> Lorsque vous créez un service VPC Lattice, vous devez spécifier une configuration de domaine personnalisée et fournir un nom de domaine personnalisé. Si vous choisissez un service existant, celui-ci doit également disposer d'un domaine personnalisé.

5. Sous Configuration du domaine, copiez la valeur du nom de domaine personnalisé.
6. Ouvrez la console Route 53 à l'adresse https://console.aws.amazon.com/route53/.
7. Dans le panneau de navigation, choisissez Zones hébergées.
8. Choisissez le nom lié de la zone hébergée pour le domaine que vous souhaitez utiliser pour acheminer le trafic vers le point de terminaison de votre domaine de service VPC Lattice. Le nom de domaine doit correspondre au point de terminaison de domaine personnalisé défini dans VPC Lattice.
9. Choisissez Créer un registre.

   Vous pouvez utiliser l'assistant pour créer les enregistrements ou choisir Switch to quick create (Passer à la création rapide).
10. Indiquez l’une des valeurs suivantes :

    Stratégie de routage

    Choisissez la stratégie de routage applicable. Pour de plus amples informations, veuillez consulter Sélection d'une stratégie de routage.

    Nom de l'enregistrement

    Entrez le nom de domaine que vous souhaitez utiliser pour acheminer le trafic vers le point de terminaison de votre domaine de service VPC Lattice. La valeur par défaut est le nom de la zone hébergée.

    Par exemple, si le nom de la zone hébergée est example.com et si vous souhaitez utiliser acme.example.com pour acheminer le trafic vers votre distribution, entrez acme.

Alias

Si vous utilisez la méthode de création d'enregistrement Quick create (Création rapide), activez Alias.

Valeur/acheminer le trafic vers

Choisissez Alias to VPC Lattice service. Choisissez la région dans laquelle le domaine de service VPC Lattice a été créé, puis choisissez la valeur que vous avez obtenue à l'étape 5.

Type de registre

Choisissez A — IPv4 adresse, AAAA — IPv6 adresse, ou les deux pour une double pile.

Évaluer l'état de la cible

Acceptez la valeur par défaut de Yes (Oui).

11. Choisissez Créer des enregistrements.

Acheminement du trafic vers d'autres AWS ressources

Voici la liste des rubriques abordées dans d'autres guides sur l'utilisation de Route 53 pour acheminer le trafic vers ces services.

- Utilisation de AWS Cloud Map dans le guide de l'utilisateur AWS Cloud Map .
- Gérez les domaines personnalisés dans le guide du AWS App Runner développeur.
- Utilisation de Route 53 en tant que fournisseur DNS dans le Guide de l'utilisateur AWS Transfer Family .
- Utilisation de Route 53 pour pointer un domaine vers une instance Amazon Lightsail.

Création de bilans de santé pour Amazon Route 53

Les surveillances de l'état Amazon Route 53 surveillent l'état et les performances de vos applications web, de vos serveurs web et d'autres ressources. Chaque surveillance de l'état que vous créez vous permet de surveiller un des éléments suivants :

- L'état d'une ressource spécifiée, telle qu'un serveur web.
- Le statut d'autres surveillances de l'état.
- État d'une CloudWatch alarme Amazon.
- En outre, avec Amazon Application Recovery Controller (ARC), vous pouvez configurer des vérifications de l'état du contrôle du routage avec des enregistrements de basculement DNS afin de gérer le basculement du trafic pour votre application. Pour en savoir plus, consultez le guide du développeur Amazon Application Recovery Controller (ARC).

Pour obtenir un aperçu des types de surveillance de l'état, consultez Types de surveillances de l'état Amazon Route 53. Pour plus d'informations sur la création de surveillances de l'état, consultez Création et mise à jour de surveillances de l'état.

Après avoir créé une surveillance de l'état, vous pouvez obtenir son statut, recevoir des notifications lorsque le statut change et configurer le basculement DNS :

Obtention du statut de la surveillance de l'état et réception de notifications

Vous pouvez également afficher le statut actuel et le statut récent de vos surveillances de l'état sur la console Route 53. Vous pouvez également utiliser des contrôles de santé par programmation via l'une des API AWS SDKs Route 53 ou AWS Tools for Windows PowerShell l'API Route 53. AWS Command Line Interface

Si vous souhaitez recevoir une notification lorsque l'état d'un bilan de santé change, vous pouvez configurer une CloudWatch alarme Amazon pour chaque bilan de santé.

Pour plus d'informations sur l'affichage du statut d'une surveillance de l'état et sur la réception de notifications, consultez Surveillance du statut de la vérification de l'état et obtention de notifications.

Configuration du basculement DNS

Si vous disposez de plusieurs ressources qui exécutent la même fonction, vous pouvez configurer le basculement DNS de sorte que Route 53 achemine le trafic d'une ressource non saine vers une

ressource saine. Par exemple, si l'un de vos deux serveurs web devient non sain, Route 53 peut acheminer le trafic vers l'autre. Pour de plus amples informations, veuillez consulter Configuration du basculement DNS.

Rubriques

- Types de surveillances de l'état Amazon Route 53
- Comment Amazon Route 53 détermine si une surveillance de l'état est saine
- Création, mise à jour et suppression de surveillances de l'état
- Configuration du basculement DNS
- Attribution de noms et balisage des surveillances de l'état
- Utilisation des surveillances de l'état avec les versions de l'API Amazon Route 53 antérieures à la version 2012-12-12

Types de surveillances de l'état Amazon Route 53

Les types de surveillances de l'état Amazon Route 53 que vous pouvez créer sont les suivants :

Surveillances de l'état qui surveillent un point de terminaison

Vous pouvez configurer une surveillance de l'état qui surveille un point de terminaison que vous spécifiez par adresse IP ou par nom de domaine. À intervalles réguliers que vous spécifiez, Route 53 envoie des demandes automatiques via Internet à votre application, à votre serveur ou à d'autres ressources pour vérifier qu'ils sont accessibles, disponibles et qu'ils fonctionnent. Facultatif : vous pouvez configurer une surveillance de l'état pour que les demandes soient similaires à celles de vos utilisateurs, par exemple demander une page web à partir d'une URL spécifique.

Surveillances de l'état qui surveillent d'autres surveillances de l'état (surveillances de l'état calculées)

Vous pouvez créer une surveillance de l'état qui surveille si Route 53 considère les autres surveillances de l'état comme saines ou non saines. Cela peut être utile quand vous disposez de plusieurs ressources qui exécutent la même fonction, par exemple plusieurs serveurs web, et que votre principale préoccupation est de savoir si un nombre minimum de vos ressources sont saines. Vous pouvez créer une surveillance de l'état pour chaque ressource sans configurer de notification pour ces vérifications. Vous pouvez ensuite créer une surveillance de l'état qui surveille le statut des autres surveillances de l'état et vous informe uniquement quand le nombre de ressources web disponibles est inférieur à un seuil défini.

Des bilans de santé qui surveillent les CloudWatch alarmes

Vous pouvez créer des CloudWatch alarmes qui surveillent l'état des CloudWatch métriques, telles que le nombre d'événements de lecture limités pour une base de données Amazon DynamoDB ou le nombre d'hôtes Elastic Load Balancing considérés comme sains. Après avoir créé une alarme, vous pouvez créer un bilan de santé qui surveille le même flux de données que celui qui CloudWatch surveille l'alarme.

Pour améliorer la résilience et la disponibilité, Route 53 n'attend pas que l' CloudWatchalarme passe à l'`ALARM`état. L'état d'un bilan de santé passe de sain à mauvais état en fonction du flux de données et des critères de l' CloudWatch alarme.

Route 53 prend en charge les CloudWatch alarmes dotées des fonctionnalités suivantes :

- Métriques de résolution standard. Les métriques haute résolution ne sont pas prises en charge. Pour plus d'informations, consultez la section Mesures haute résolution dans le guide de l' CloudWatch utilisateur Amazon.
- Statistiques : moyenne, minimale, maximale, somme et SampleCount. Les statistiques étendues ne sont pas prises en charge.
- Route 53 ne prend pas en charge les alarmes « M sur N ». Pour plus d'informations, consultez la section Évaluation d'une alarme dans le CloudWatch guide Amazon.
- Un bilan de santé ne peut surveiller qu'une CloudWatch alarme qui existe dans le même AWS compte que le bilan de santé.
- Route 53 ne prend pas en charge les alarmes qui utilisent des métriques mathématiques pour interroger plusieurs CloudWatch métriques.

Contrôleur de routage Amazon Application Recovery Controller (ARC)

Les contrôles de santé dans ARC sont associés aux commandes de routage, qui sont de simples commutateurs marche/arrêt. Vous configurez chaque surveillance de l'état du contrôle de routage au moyen d'un enregistrement DNS de basculement. Vous pouvez ensuite simplement mettre à jour vos contrôles de routage dans ARC pour rediriger le trafic et faire basculer vos applications, par exemple entre des zones de disponibilité ou AWS des régions. Pour plus d'informations, consultez la section Contrôle du routage dans ARC dans le guide du développeur ARC.

Comment Amazon Route 53 détermine si une surveillance de l'état est saine

La méthode qu'Amazon Route 53 utilise pour déterminer si une surveillance de l'état est saine dépend du type de surveillance de l'état.

Rubriques

- Comment Route 53 détermine le statut des surveillances de l'état qui surveillent un point de terminaison
- Comment Route 53 détermine le statut des surveillances de l'état qui surveillent d'autres surveillances de l'état
- Comment Route 53 détermine l'état des bilans de santé qui surveillent les CloudWatch alarmes

Comment Route 53 détermine le statut des surveillances de l'état qui surveillent un point de terminaison

Route 53 dispose d'outils de surveillance de l'état situés dans différents emplacements dans le monde. Lorsque vous créez une surveillance de l'état qui surveille un point de terminaison, les outils de surveillance de l'état commencent à envoyer des demandes au point de terminaison que vous spécifiez afin de déterminer si ce dernier est sain. Vous pouvez choisir les emplacements qui seront utilisés par Route 53, et vous pouvez spécifier l'intervalle entre les vérifications : toutes les 10 secondes ou toutes les 30 secondes. Notez que les outils de surveillance de l'état Route 53 de différents centres de données ne sont pas coordonnés. C'est la raison pour laquelle vous verrez parfois plusieurs demandes par seconde, quel que soit l'intervalle choisi, puis quelques secondes sans surveillance de l'état.

Chaque surveillance de l'état évalue l'état du point de terminaison en fonction de deux valeurs :

- Temps de réponse. Une ressource peut être lente à répondre ou peut échouer pour répondre à une demande de surveillance de l'état pour différentes raisons. Par exemple, la ressource est arrêtée pour des raisons de maintenance, elle fait l'objet d'une attaque par déni de service distribué (DDoS) ou le réseau est en panne.
- Indique si le point de terminaison répond à un nombre spécifié de surveillances de l'état consécutives (seuil d'échec)

Route 53 regroupe les données des outils de surveillance de l'état et détermine si le point de terminaison est sain :

- Si plus de 18 % des outils de surveillance de l'état signalent qu'un point de terminaison est sain, Route 53 le considère sain.
- Si 18 % des outils de surveillance de l'état ou moins signalent qu'un point de terminaison est sain, Route 53 le considère non sain.

La valeur de 18 % a été choisie afin de s'assurer que des outils de surveillance de l'état situés dans plusieurs régions considèrent que le point de terminaison est sain. De cette manière, un point de terminaison ne peut pas être considéré non sain uniquement parce que les conditions du réseau ont isolé le point de terminaison de certains emplacements de vérification de l'état. Cette valeur pourra faire l'objet d'une modification dans une version ultérieure.

Le temps de réponse qu'un outil de surveillance de l'état utilise pour déterminer si un point de terminaison est sain dépend du type de surveillance de l'état :

- Surveillances de l'état HTTP et HTTPS – Route 53 doit être en mesure d'établir une connexion TCP avec le point de terminaison dans les quatre secondes. En outre, le point de terminaison doit répondre par un code d'état HTTP 2xx ou 4xx dans les deux secondes qui suivent la connexion.

  > **Note**
  >
  > Les contrôles de santé HTTPS ne valident pas SSL/TLS les certificats. Ils n'échouent donc pas si un certificat n'est pas valide ou a expiré.

- Surveillances de l'état TCP) – Route 53 doit être en mesure d'établir une connexion TCP avec le point de terminaison dans les dix secondes.
- Surveillances de l'état HTTP et HTTPS avec correspondance de chaîne – Comme pour les surveillances de l'état HTTP et HTTPS, Route 53 doit être en mesure d'établir une connexion TCP avec le point de terminaison dans les quatre secondes, et le point de terminaison doit répondre par un code d'état HTTP 2xx ou 3xx dans les deux secondes après la connexion.

  Une fois qu'un outil de surveillance de l'état Route 53 a reçu le code de statut HTTP, il doit recevoir le corps de la réponse du point de terminaison dans les deux secondes qui suivent. Route 53 recherche dans le corps de réponse une chaîne que vous spécifiez. La chaîne doit figurer intégralement dans les 5 120 premiers octets du corps de la réponse. Si ce n'est pas le cas, la

surveillance de l'état échoue pour le point de terminaison. Si vous utilisez la console Route 53, vous spécifiez la chaîne dans le champ Search String (Chaîne de recherche). Si vous utilisez l'API Route 53, vous spécifiez la chaîne dans l'élément `SearchString` lorsque vous créez la surveillance de l'état.

Pour les contrôles de santé qui surveillent un point de terminaison (à l'exception des contrôles de santé TCP), si la réponse du point de terminaison inclut des en-têtes, ceux-ci doivent être au format défini en RFC723 0, Hypertext Transfer Protocol (HTTP/1.1) : syntaxe et routage des messages, section 3.2, « Champs d'en-tête ».

Route 53 considère qu'une nouvelle surveillance de l'état est saine jusqu'à obtenir suffisamment de données pour déterminer le véritable état, sain ou non sain. Si vous choisissez l'option d'inverser le statut de la surveillance de l'état, Route 53 considère qu'une nouvelle surveillance de l'état est non saine, jusqu'à obtenir suffisamment de données.

Comment Route 53 détermine le statut des surveillances de l'état qui surveillent d'autres surveillances de l'état

Une surveillance de l'état peut surveiller le statut des autres surveillances de l'état ; ce type de surveillance de l'état est appelé surveillance de l'état calculée. La surveillance de l'état qui effectue le suivi est la surveillance de l'état parent et les surveillances de l'état qui sont surveillées sont les surveillances de l'état enfants. Une surveillance de l'état parent peut surveiller jusqu'à l'intégrité de 255 surveillances de l'état enfants. La surveillance fonctionne comme suit :

- Route 53 ajoute le nombre de surveillances de l'état enfants qui sont considérées comme saines.
- Route 53 compare ensuite ce nombre au nombre de surveillances de l'état enfants devant être saines pour que le statut de la surveillance de l'état parent soit considéré comme sain.

Pour plus d'informations, consultez Autres surveillances de l'état calculée dans Valeurs que vous spécifiez lors de la création ou de la mise à jour de surveillances de l'état.

Route 53 considère qu'une nouvelle surveillance de l'état est saine jusqu'à obtenir suffisamment de données pour déterminer le véritable état, sain ou non sain. Si vous choisissez l'option d'inverser le statut de la surveillance de l'état, Route 53 considère qu'une nouvelle surveillance de l'état est non saine, jusqu'à obtenir suffisamment de données. Si vous inversez le bilan de santé, Route 53 considère qu'un terminal sain est malsain et vice versa.

Comment Route 53 détermine l'état des bilans de santé qui surveillent les CloudWatch alarmes

Lorsque vous créez un bilan de santé basé sur une CloudWatch alarme, Route 53 surveille le flux de données pour l'alarme correspondante au lieu de surveiller l'état de l'alarme. Si le flux de données indique que l'état de l'alarme est OK, la surveillance de l'état est considérée comme saine. Si le flux de données indique que l'état de l'alarme est Alarme, la surveillance de l'état est considérée comme non saine. Si le flux de données ne fournit pas de suffisamment d'informations pour déterminer l'état de l'alarme, le statut de la surveillance de l'état dépend de la valeur de Statut de surveillance de l'état : sain, non sain ou dernier statut connu. (Dans l'API Route 53, ce paramètre est `InsufficientDataHealthStatus`.)

Route 53 ne prend pas en charge les CloudWatch alarmes entre comptes.

> **Note**
>
> Étant donné que les contrôles de santé Route 53 surveillent les flux de CloudWatch données plutôt que l'état des CloudWatch alarmes, vous ne pouvez pas forcer le changement de statut d'un contrôle de santé à l'aide de l'opération CloudWatch SetAlarmStateAPI.

Route 53 considère qu'une nouvelle surveillance de l'état est saine jusqu'à obtenir suffisamment de données pour déterminer le véritable état, sain ou non sain. Si vous choisissez l'option d'inverser le statut de la surveillance de l'état, Route 53 considère qu'une nouvelle surveillance de l'état est non saine, jusqu'à obtenir suffisamment de données. Si vous inversez le bilan de santé, Route 53 considère qu'un terminal sain est malsain et vice versa.

Création, mise à jour et suppression de surveillances de l'état

> **Important**
>
> Si vous procédez à la mise à jour ou à la suppression de surveillances de l'état associées à des enregistrements, passez en revue les tâches de Mise à jour ou suppression de surveillances de l'état lorsque le basculement DNS est configuré avant de poursuivre.

Cette section couvre les sujets suivants liés à la gestion des bilans de santé de Route 53 :

1. Création et mise à jour des bilans de santé :
   - Découvrez comment créer et mettre à jour des bilans de santé à l'aide de la console Route 53.
   - Comprenez les valeurs que vous devez spécifier lors de la création ou de la mise à jour des bilans de santé, telles que la surveillance des terminaux, le protocole, l'adresse IP, le nom de domaine et les options de configuration avancées.
2. Valeurs affichées lors de la création d'un bilan de santé :
   - Découvrez les valeurs affichées par la console Route 53 en fonction de vos entrées lors de la création d'un bilan de santé, telles que l'URL complète ou l'adresse IP et le port.
3. Mise à jour des contrôles de santé en cas de modification des CloudWatch alarmes :
   - Découvrez comment mettre à jour un bilan de santé lorsque vous modifiez les paramètres de l' CloudWatch alarme associée.
4. Supprimer les bilans de santé :
   - Suivez la procédure pour supprimer les bilans de santé à l'aide de la console Route 53.
5. Mise à jour ou suppression des contrôles de santé lorsque le basculement du DNS est configuré :
   - Découvrez les tâches recommandées à effectuer lors de la mise à jour ou de la suppression des contrôles de santé associés aux enregistrements DNS afin de garantir une configuration de routage et de basculement correcte.
6. Configuration des règles du routeur et du pare-feu :
   - Découvrez comment configurer les règles de votre routeur et de votre pare-feu pour autoriser le trafic entrant provenant des vérificateurs de santé de Route 53, afin de garantir la réussite des contrôles de santé.

En suivant les informations fournies dans cette section, vous pouvez créer, mettre à jour et supprimer efficacement les contrôles de santé de Route 53, gérer leur configuration et garantir une intégration correcte avec les politiques de routage et de basculement du DNS.

Rubriques

- Création et mise à jour de surveillances de l'état
- Valeurs que vous spécifiez lors de la création ou de la mise à jour de surveillances de l'état
- Valeurs qu'Amazon Route 53 affiche lors de la création d'une surveillance de l'état
- Mise à jour des bilans de santé lorsque vous modifiez les paramètres des CloudWatch alarmes (bilans de santé qui surveillent uniquement une CloudWatch alarme)
- Activation ou désactivation des bilans de santé

- Contrôles de santé inversés
- Suppression de surveillances de l'état
- Mise à jour ou suppression de surveillances de l'état lorsque le basculement DNS est configuré
- Configuration des règles de pare-feu et de routeur pour les surveillances de l'état Amazon Route 53

Création et mise à jour de surveillances de l'état

La procédure suivante décrit comment créer et mettre à jour les surveillances de l'état à l'aide de la console Route 53.

> **Note**
>
> Nous mettons à jour la console de vérification de l'état de santé de Route 53. Pendant la période de transition, vous pouvez continuer à utiliser l'ancienne console.

Choisissez l'onglet correspondant à la console que vous utilisez.

- Nouvelle console
- Ancienne console

New console

Pour créer ou mettre à jour un bilan de santé

1. Si vous mettez à jour des surveillances de l'état déjà associées à des enregistrements, exécutez les tâches recommandées dans Mise à jour ou suppression de surveillances de l'état lorsque le basculement DNS est configuré.
2. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
3. Dans le volet de navigation, sélectionnez Health Checks.
4. Si vous souhaitez mettre à jour un bilan de santé existant, choisissez l'identifiant associé au bilan de santé, puis choisissez Modifier.

   Si vous souhaitez créer un bilan de santé, choisissez Créer un bilan de santé.

5. Entrez les valeurs applicables. Notez que certaines valeurs ne peuvent pas être modifiées après la création d'une surveillance de l'état. Pour de plus amples informations, veuillez consulter Valeurs que vous spécifiez lors de la création ou de la mise à jour de surveillances de l'état.
6. Choisissez Créer une vérification de l'état.

> **Note**
>
> Route 53 considère qu'une nouvelle surveillance de l'état est saine jusqu'à obtenir suffisamment de données pour déterminer le véritable état, sain ou non sain.

7. Associez une ou plusieurs surveillances de l'état à un ou plusieurs enregistrements Route 53. Pour plus d'informations sur la création et la mise à jour d'enregistrements, consultez Utilisation des enregistrements.

Old console

Pour créer ou mettre à jour un bilan de santé

1. Si vous mettez à jour des surveillances de l'état déjà associées à des enregistrements, exécutez les tâches recommandées dans Mise à jour ou suppression de surveillances de l'état lorsque le basculement DNS est configuré.
2. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
3. Dans le volet de navigation, sélectionnez Health Checks.
4. Si vous souhaitez mettre à jour une surveillance de l'état existante, sélectionnez la vérification appropriée, puis choisissez Modifier la surveillance de l'état.

   Si vous souhaitez créer une surveillance de l'état, choisissez Créer une surveillance de l'état. Pour plus d'informations sur chaque paramètre, déplacez le pointeur de la souris sur une étiquette pour afficher l'info-bulle.
5. Entrez les valeurs applicables. Notez que certaines valeurs ne peuvent pas être modifiées après la création d'une surveillance de l'état. Pour de plus amples informations, veuillez consulter Valeurs que vous spécifiez lors de la création ou de la mise à jour de surveillances de l'état.
6. Choisissez Create Health Check.

> **Note**
>
> Route 53 considère qu'une nouvelle surveillance de l'état est saine jusqu'à obtenir suffisamment de données pour déterminer le véritable état, sain ou non sain. Si vous choisissez l'option d'inverser le statut de la surveillance de l'état, Route 53 considère qu'une nouvelle surveillance de l'état est non saine, jusqu'à obtenir suffisamment de données.

7. Associez une ou plusieurs surveillances de l'état à un ou plusieurs enregistrements Route 53. Pour plus d'informations sur la création et la mise à jour d'enregistrements, consultez Utilisation des enregistrements.

Valeurs que vous spécifiez lors de la création ou de la mise à jour de surveillances de l'état

Lorsque vous créez ou mettez à jour les surveillances de l'état, vous spécifiez les valeurs applicables. Notez que vous ne pouvez pas modifier certaines valeurs après la création d'une surveillance de l'état.

Rubriques

- Surveillance d'un point de terminaison
- Autres surveillances de l'état calculée
- Surveillance d'une alarme CloudWatch
- Configuration avancée (option « Monitor an endpoint » uniquement)
- Être informé en cas d'échec d'une surveillance de l'état

Nom

Facultatif, mais recommandé : nom que vous souhaitez attribuer à la surveillance de l'état. Si vous spécifiez une valeur pour Nom, Route 53 ajoute une balise à la surveillance de l'état, attribue la valeur Nom à la clé de balise et affecte la valeur que vous spécifiez à la valeur de la balise. La valeur de la balise Nom s'affiche dans la liste des surveillances de l'état dans la console Route 53, ce qui vous permet de distinguer facilement les surveillances de l'état les unes des autres.

Pour plus d'informations sur le balisage et les surveillances de l'état, consultez Attribution de noms et balisage des surveillances de l'état.

Eléments à surveiller

Si vous souhaitez que cette surveillance de l'état surveille un point de terminaison ou le statut d'autres surveillances de l'état :

- Point de terminaison – Route 53 surveille l'état d'un point de terminaison que vous spécifiez. Vous pouvez spécifier le point de terminaison en fournissant un nom de domaine ou une adresse IP et un port.

  > **Note**
  >
  > Si vous spécifiez un point de AWS terminaison autre que le terminal, des frais supplémentaires s'appliquent. Pour plus d'informations, notamment pour obtenir une définition des points de terminaison AWS , consultez la section relative aux surveillances de l'état sur la page Tarification Route 53.

- Statut d'autres surveillances de l'état (surveillance de l'état calculée) – Route 53 détermine si cette surveillance de l'état est saine en fonction du statut d'autres surveillances de l'état que vous spécifiez. Vous aussi spécifier le nombre de surveillances de l'état dont le résultat doit être sain pour que cette surveillance de l'état soit considérée comme saine.
- État du flux de données CloudWatch d'alarme — Route 53 détermine si ce contrôle de santé est sain en surveillant le flux de données pour détecter une CloudWatch alarme.

Surveillance d'un point de terminaison

> **Note**
>
> Nous mettons à jour la console de vérification de l'état de santé de Route 53. Pendant la période de transition, vous pouvez continuer à utiliser l'ancienne console.

Choisissez l'onglet correspondant à la console que vous utilisez.

- Nouvelle console
- Ancienne console

New console

Si vous souhaitez que cette surveillance de l'état surveille un point de terminaison, spécifiez les valeurs suivantes :

- Spécifiez les points de terminaison par
- Adresse IP
- Nom de domaine

Spécification du point de terminaison par

Si vous souhaitez spécifier le point de terminaison à l'aide d'une adresse IP ou à l'aide d'un nom de domaine.

Une fois que vous avez créé une surveillance de l'état, vous ne pouvez pas modifier la valeur du champ Spécifier un point de terminaison par.

Adresse IP (uniquement pour l'option « Specify endpoint by IP address » [Spécifier le point de terminaison par adresse IP])

Choisissez le protocole dans le menu déroulant, entrez l'adresse IP, le port et le chemin dans la zone de texte.

- Le protocole peut être l'un des suivants :

  HTTP – Route 53 tente d'établir une connexion TCP. En cas de réussite, Route 53 envoie une demande HTTP et attend un code d'état HTTP 2xx ou 3xx.

- HTTPS – Route 53 tente d'établir une connexion TCP. En cas de réussite, Route 53 envoie une demande HTTPS et attend un code d'état HTTP 2xx ou 3xx.

  > **Important**
  >
  > Si vous choisissez HTTPS, le point de terminaison doit prendre en charge le protocole TLS v1.0, v1.1 ou v1.2.

  Si vous choisissez HTTPS comme valeur pour Protocol, des frais s'appliquent. Pour en savoir plus, consultez Tarification Route 53.

- TCP – Route 53 tente d'établir une connexion TCP.

Pour de plus amples informations, veuillez consulter Comment Amazon Route 53 détermine si une surveillance de l'état est saine.

Une fois que vous avez créé une surveillance de l'état, vous ne pouvez pas modifier la valeur de Protocol.

Pour l'adresse IP, vous pouvez saisir l' IPv6 adresse IPv4 OR du point de terminaison sur lequel vous souhaitez que Route 53 effectue des contrôles de santé, si vous avez choisi Spécifier le point de terminaison par adresse IP.

Route 53 ne peut pas vérifier l'état de points de terminaison pour lesquels l'adresse IP se trouve dans des plages locales, privées, non routables ou multicast. Pour plus d'informations sur les adresses IP pour lesquelles vous ne pouvez pas créer de surveillances de l'état, consultez les documents suivants :

- RFC 5735, Adresses à usage spécial IPv4
- RFC 6598, IPv4 Préfixe réservé à l'IANA pour l'espace d'adressage partagé.
- RFC 5156, Adresses à usage spécial IPv6

Si le point de terminaison est une EC2 instance Amazon, nous vous recommandons de créer une adresse IP élastique, de l'associer à votre EC2 instance et de spécifier l'adresse IP élastique. Ceci permet de s'assurer que l'adresse IP de votre instance ne changera jamais. Pour plus d'informations, consultez la section Adresses IP élastiques (EIP) dans le guide de l' EC2 utilisateur Amazon.

Si vous supprimez l' EC2 instance Amazon, assurez-vous de supprimer également le bilan de santé associé à l'EIP. Pour de plus amples informations, veuillez consulter Bonnes pratiques relatives aux vérifications de l'état d'Amazon Route 53.

> **Note**
>
> Si vous spécifiez un point de AWS terminaison autre que le terminal, des frais supplémentaires s'appliquent. Pour plus d'informations, notamment pour obtenir une définition des points de terminaison AWS , consultez la section relative aux surveillances de l'état sur la page Tarification Route 53.

Pour le port, vous entrez le port du point de terminaison sur lequel vous souhaitez que Route 53 effectue des contrôles de santé.

Pour le chemin (protocoles HTTP et HTTPS uniquement), entrez le chemin que vous souhaitez que Route 53 demande lors des vérifications de santé. Le chemin peut être n'importe quelle valeur pour laquelle votre point de terminaison renverra un code d'état H TTP de 2xx ou 3xx lorsque le point de terminaison est sain, comme le fichier/.html ? docs/route53-health-check.html. You can also include query string parameters, for example, /welcome language=jp&login=y. Si vous n'incluez pas de barre oblique (/) en tête, Route 53 en ajoute automatiquement une.

Nom de domaine (uniquement pour l'option « Specify endpoint by domain name » [Spécifier le point de terminaison par nom de domaine], tous les protocoles)

Le nom de domaine (example.com) ou nom de sous-domaine (backend.example.com) du point de terminaison sur lequel vous souhaitez que Route 53 effectue les surveillances de l'état, si vous choisissez Spécifier le point de terminaison par nom de domaine.

Si vous choisissez de spécifier le point de terminaison par nom de domaine, Route 53 envoie une requête DNS pour résoudre le nom de domaine indiqué dans Domain name (Nom de domaine) selon l'intervalle spécifié dans Request interval (Intervalle entre les demandes). À l'aide d'une adresse IP renvoyée par DNS, Route 53 vérifie ensuite l'état du point de terminaison.

> **Note**
>
> Si vous spécifiez le point de terminaison par nom de domaine, Route 53 l'utilise uniquement IPv4 pour envoyer des bilans de santé au point de terminaison. S'il n'existe aucun enregistrement de type A pour le nom que vous spécifiez dans le champ Nom de domaine, la surveillance de l'état échoue en renvoyant l'erreur « échec de la résolution DNS ».

Si vous voulez vérifier l'état de basculement, de géolocalisation, de proximité géographique, de latence, de multivaleur ou l'état des enregistrements pondérés et si vous choisissez de spécifier le point de terminaison par nom de domaine, nous vous recommandons de créer une surveillance de l'état distincte pour chaque point de terminaison. Par exemple, créez une surveillance de l'état pour chaque serveur HTTP qui diffuse du contenu pour www.example.com. Pour la valeur du champ Nom de domaine, indiquez le nom de domaine du serveur (par exemple, us-east-2-www.example.com), et non pas le nom des enregistrements (www.example.com).

> **Important**
>
> Dans cette configuration, si vous créez une surveillance de l'état pour laquelle la valeur du champ Nom de domaine correspond au nom des enregistrements et si vous associez ensuite la surveillance de l'état à ces enregistrements, les résultats de la surveillance de l'état seront imprévisibles.

En outre, si la valeur de Protocol (Protocole) est HTTP ou HTTPS, Route 53 transmet la valeur de Domain name (Nom de domaine) dans l'en-tête `Host` comme décrit dans la rubrique Host name (Nom d'hôte), ci-avant dans la liste. Si la valeur de Protocol (Protocole) est TCP, Route 53 ne transmet pas d'en-tête `Host`.

> **Note**
>
> Si vous spécifiez un point de AWS terminaison autre que le terminal, des frais supplémentaires s'appliquent. Pour plus d'informations, notamment pour obtenir une définition des points de terminaison AWS , consultez la section relative aux surveillances de l'état sur la page Tarification Route 53.

Old console

Si vous souhaitez que cette surveillance de l'état surveille un point de terminaison, spécifiez les valeurs suivantes :

- Spécification du point de terminaison par
- Protocole
- Adresse IP
- Nom d'hôte
- Port
- Nom de domaine
- Chemin

Spécification du point de terminaison par

Si vous souhaitez spécifier le point de terminaison à l'aide d'une adresse IP ou à l'aide d'un nom de domaine.

Une fois que vous avez créé une surveillance de l'état, vous ne pouvez pas modifier la valeur du champ Spécifier un point de terminaison par.

Protocole

Méthode que vous souhaitez que Route 53 utilise pour vérifier l'état de votre point de terminaison :

- HTTP – Route 53 tente d'établir une connexion TCP. En cas de réussite, Route 53 envoie une demande HTTP et attend un code d'état HTTP 2xx ou 3xx.
- HTTPS – Route 53 tente d'établir une connexion TCP. En cas de réussite, Route 53 envoie une demande HTTPS et attend un code d'état HTTP 2xx ou 3xx.

  > **Important**
  >
  > Si vous choisissez HTTPS, le point de terminaison doit prendre en charge le protocole TLS v1.0, v1.1 ou v1.2.

  Si vous choisissez HTTPS comme valeur pour Protocol, des frais s'appliquent. Pour en savoir plus, consultez Tarification Route 53.
- TCP – Route 53 tente d'établir une connexion TCP.

Pour de plus amples informations, veuillez consulter Comment Amazon Route 53 détermine si une surveillance de l'état est saine.

Une fois que vous avez créé une surveillance de l'état, vous ne pouvez pas modifier la valeur de Protocol.

Adresse IP (uniquement pour l'option « Specify endpoint by IP address » [Spécifier le point de terminaison par adresse IP])

IPv6 Adresse IPv4 ou du point de terminaison sur lequel vous souhaitez que Route 53 effectue des contrôles de santé, si vous avez choisi Spécifier le point de terminaison par adresse IP.

Route 53 ne peut pas vérifier l'état de points de terminaison pour lesquels l'adresse IP se trouve dans des plages locales, privées, non routables ou multicast. Pour plus d'informations

sur les adresses IP pour lesquelles vous ne pouvez pas créer de surveillances de l'état, consultez les documents suivants :

- RFC 5735, Adresses à usage spécial IPv4
- RFC 6598, IPv4 Préfixe réservé à l'IANA pour l'espace d'adressage partagé.
- RFC 5156, Adresses à usage spécial IPv6

Si le point de terminaison est une EC2 instance Amazon, nous vous recommandons de créer une adresse IP élastique, de l'associer à votre EC2 instance et de spécifier l'adresse IP élastique. Ceci permet de s'assurer que l'adresse IP de votre instance ne changera jamais. Pour plus d'informations, consultez la section Adresses IP élastiques (EIP) dans le guide de l' EC2 utilisateur Amazon.

Si vous supprimez l' EC2 instance Amazon, assurez-vous de supprimer également le bilan de santé associé à l'EIP. Pour de plus amples informations, veuillez consulter Bonnes pratiques relatives aux vérifications de l'état d'Amazon Route 53.

> **Note**
>
> Si vous spécifiez un point de AWS terminaison autre que le terminal, des frais supplémentaires s'appliquent. Pour plus d'informations, notamment pour obtenir une définition des points de terminaison AWS , consultez la section relative aux surveillances de l'état sur la page Tarification Route 53.

Nom d'hôte (uniquement pour l'option « Specify endpoint by IP address » [Spécifier le point de terminaison par adresse IP], protocoles HTTP et HTTPS uniquement)

La valeur que vous souhaitez que Route 53 transmette dans l'en-tête `Host` des surveillances de l'état HTTP et HTTPS. Il s'agit généralement du nom DNS complet du site web sur lequel vous souhaitez que Route 53 procède aux surveillances de l'état. Lorsque Route 53 vérifie l'état d'un point de terminaison, voici comment l'en-tête `Host` est construit :

- Si vous spécifiez la valeur **`80`** pour Port et HTTP pour Protocol (Protocole), Route 53 transmet au point de terminaison un en-tête `Host` qui contient la valeur de Host name (Nom d'hôte).
- Si vous spécifiez la valeur **`443`** pour Port et HTTPS pour Protocol (Protocole), Route 53 transmet au point de terminaison un en-tête `Host` qui contient la valeur de Host name (Nom d'hôte).

- Si vous spécifiez une autre valeur pour le port et HTTP ou HTTPS pour le protocole, Route 53 transmet au point de terminaison un `Host` en-tête contenant la valeur *`Host name`* :*`Port`*.

Si vous choisissez de spécifier le point de terminaison par adresse IP et que vous ne spécifiez pas de valeur pour Host name (Nom d'hôte), Route 53 remplace la valeur IP address (Adresse IP) dans l'en-tête `Host` de chacun des cas précédents.

Port

Port sur le point de terminaison sur lequel vous souhaitez que Route 53 exécute des surveillances de l'état.

Nom de domaine (uniquement pour l'option « Specify endpoint by domain name » [Spécifier le point de terminaison par nom de domaine], tous les protocoles)

Le nom de domaine (example.com) ou nom de sous-domaine (backend.example.com) du point de terminaison sur lequel vous souhaitez que Route 53 effectue les surveillances de l'état, si vous choisissez Spécifier le point de terminaison par nom de domaine.

Si vous choisissez de spécifier le point de terminaison par nom de domaine, Route 53 envoie une requête DNS pour résoudre le nom de domaine indiqué dans Domain name (Nom de domaine) selon l'intervalle spécifié dans Request interval (Intervalle entre les demandes). À l'aide d'une adresse IP renvoyée par DNS, Route 53 vérifie ensuite l'état du point de terminaison.

> **Note**
>
> Si vous spécifiez le point de terminaison par nom de domaine, Route 53 l'utilise uniquement IPv4 pour envoyer des bilans de santé au point de terminaison. S'il n'existe aucun enregistrement de type A pour le nom que vous spécifiez dans le champ Nom de domaine, la surveillance de l'état échoue en renvoyant l'erreur « échec de la résolution DNS ».

Si vous voulez vérifier l'état de basculement, de géolocalisation, de proximité géographique, de latence, de multivaleur ou l'état des enregistrements pondérés et si vous choisissez de spécifier le point de terminaison par nom de domaine, nous vous recommandons de créer une surveillance de l'état distincte pour chaque point de terminaison. Par exemple, créez une surveillance de l'état pour chaque serveur HTTP qui diffuse du contenu pour

www.example.com. Pour la valeur du champ Nom de domaine, indiquez le nom de domaine du serveur (par exemple, us-east-2-www.example.com), et non pas le nom des enregistrements (www.example.com).

> **Important**
>
> Dans cette configuration, si vous créez une surveillance de l'état pour laquelle la valeur du champ Nom de domaine correspond au nom des enregistrements et si vous associez ensuite la surveillance de l'état à ces enregistrements, les résultats de la surveillance de l'état seront imprévisibles.

En outre, si la valeur de Protocol (Protocole) est HTTP ou HTTPS, Route 53 transmet la valeur de Domain name (Nom de domaine) dans l'en-tête `Host` comme décrit dans la rubrique Host name (Nom d'hôte), ci-avant dans la liste. Si la valeur de Protocol (Protocole) est TCP, Route 53 ne transmet pas d'en-tête `Host`.

> **Note**
>
> Si vous spécifiez un point de AWS terminaison autre que le terminal, des frais supplémentaires s'appliquent. Pour plus d'informations, notamment pour obtenir une définition des points de terminaison AWS , consultez la section relative aux surveillances de l'état sur la page Tarification Route 53.

Chemin (protocoles HTTP et HTTPS uniquement)

Chemin d'accès que vous souhaitez que Route 53 demande lors de l'exécution des surveillances de l'état. Le chemin peut être toute valeur pour laquelle votre point de terminaison renverra un code de statut HTTP `2xx` ou `3xx` quand le point de terminaison est sain, par exemple, le fichier `/docs/route53-health-check.html`. Vous pouvez également inclure des paramètres de chaîne de requête, par exemple, `/welcome.html?language=jp&login=y`. Si vous n'incluez pas une barre oblique (`/`) au début, Route 53 en ajoute automatiquement une.

Autres surveillances de l'état calculée

> **Note**
>
> Nous mettons à jour la console de vérification de l'état de santé de Route 53. Pendant la période de transition, vous pouvez continuer à utiliser l'ancienne console.

Choisissez l'onglet correspondant à la console que vous utilisez.

- Nouvelle console
- Ancienne console

New console

Si vous souhaitez que cette surveillance de l'état surveille le statut d'autres surveillances de l'état, spécifiez les valeurs suivantes :

- Health bilans à surveiller
- Signalez en bonne santé lorsque

Health bilans à surveiller

Surveillances de l'état que vous souhaitez que Route 53 surveille pour déterminer l'état de cette surveillance de l'état.

Vous pouvez ajouter jusqu'à 256 surveillances de l'état à Surveillances de l'état à surveiller. Pour supprimer une surveillance de l'état de la liste, sélectionnez x à la droite de l'élément en surbrillance pour cette surveillance de l'état.

> **Note**
>
> Vous ne pouvez pas configurer une surveillance de l'état calculée pour surveiller l'état d'autres surveillances de l'état calculées.

Si vous désactivez une surveillance de l'état qui est surveillée par une surveillance de l'état calculée, Route 53 considère la surveillance de l'état désactivée comme saine, étant donné qu'il calcule si la surveillance de l'état calculée est saine. Si vous souhaitez que la surveillance

de l'état désactivée soit considérée comme non saine, activez la case à cocher Inverser le statut de surveillance de l'état.

Signalez en bonne santé lorsque

Calcul que vous souhaitez que Route 53 exécute pour déterminer si cette surveillance de l'état est saine :

- Signaler comme sain quand au moins x sur y sur certaines surveillances de l'état sont saines) – Route 53 considère cette surveillance de l'état saine lorsque le nombre de surveillances de l'état ajoutées dans Surveillances de l'état à surveiller sont saines. Remarques :
  - Si vous spécifiez un nombre supérieur au nombre de surveillances de l'état indiquées dans Surveillances de l'état à surveiller, Route 53 considère cette vérification non saine dans tous les cas.
  - Si vous spécifiez 0, Route 53 considère cette surveillance de l'état comme saine dans tous les cas.
- Signaler comme sain quand toutes les surveillances de l'état sont saines (ET) – Route 53 considère cette surveillance de l'état saine uniquement lorsque l'ensemble des surveillances de l'état ajoutées à Surveillances de l'état à surveiller sont saines.
- Signaler comme sain quand une ou plusieurs surveillances de l'état sont saines (OU) – Route 53 considère cette surveillance de l'état saine lorsqu'au moins l'une des Surveillances de l'état à surveiller est saine.

Old console

Si vous souhaitez que cette surveillance de l'état surveille le statut d'autres surveillances de l'état, spécifiez les valeurs suivantes :

- Health bilans à surveiller
- Signalez en bonne santé lorsque
- Inverser le statut de surveillance de l'état
- Désactivées

Health bilans à surveiller

Surveillances de l'état que vous souhaitez que Route 53 surveille pour déterminer l'état de cette surveillance de l'état.

Vous pouvez ajouter jusqu'à 256 surveillances de l'état à Surveillances de l'état à surveiller. Pour supprimer une surveillance de l'état de la liste, sélectionnez x à la droite de l'élément en surbrillance pour cette surveillance de l'état.

> **Note**
>
> Vous ne pouvez pas configurer une surveillance de l'état calculée pour surveiller l'état d'autres surveillances de l'état calculées.

Si vous désactivez une surveillance de l'état qui est surveillée par une surveillance de l'état calculée, Route 53 considère la surveillance de l'état désactivée comme saine, étant donné qu'il calcule si la surveillance de l'état calculée est saine. Si vous souhaitez que la surveillance de l'état désactivée soit considérée comme non saine, activez la case à cocher Inverser le statut de surveillance de l'état.

Signalez en bonne santé lorsque

Calcul que vous souhaitez que Route 53 exécute pour déterminer si cette surveillance de l'état est saine :

- Signaler comme sain quand au moins x sur y sur certaines surveillances de l'état sont saines) – Route 53 considère cette surveillance de l'état saine lorsque le nombre de surveillances de l'état ajoutées dans Surveillances de l'état à surveiller sont saines. Remarques :
  - Si vous spécifiez un nombre supérieur au nombre de surveillances de l'état indiquées dans Surveillances de l'état à surveiller, Route 53 considère cette vérification non saine dans tous les cas.
  - Si vous spécifiez 0, Route 53 considère cette surveillance de l'état comme saine dans tous les cas.
- Signaler comme sain quand toutes les surveillances de l'état sont saines (ET) – Route 53 considère cette surveillance de l'état saine uniquement lorsque l'ensemble des surveillances de l'état ajoutées à Surveillances de l'état à surveiller sont saines.
- Signaler comme sain quand une ou plusieurs surveillances de l'état sont saines (OU) – Route 53 considère cette surveillance de l'état saine lorsqu'au moins l'une des Surveillances de l'état à surveiller est saine.

Inverser l'état du bilan de santé (ancienne console uniquement)

Pour inverser un bilan de santé sur la nouvelle console, consultez Contrôles de santé inversés.

Décidez si vous voulez que Route 53 inverse le statut d'une surveillance de l'état. Si vous sélectionnez cette option, Route 53 considère que les surveillances de l'état ne sont pas saines lorsque le statut est sain, et vice versa.

Désactivé (ancienne console uniquement)

Pour désactiver un contrôle de santé sur la nouvelle console, consultez Activation ou désactivation des bilans de santé.

Empêche Route 53 de poursuivre l'exécution de surveillances de l'état. Lorsque vous désactivez une surveillance de l'état, Route 53 arrête de regrouper le statut des surveillances de l'état référencées.

Lorsque vous désactivez une surveillance de l'état, Route 53 considère que le statut de la surveillance de l'état est toujours sain. Si vous avez configuré le basculement DNS, Route 53 continue à acheminer le trafic vers les ressources correspondantes. Si vous souhaitez arrêter d'acheminer le trafic vers une ressource, inversez le bilan de santé.

> **Note**
>
> Les frais pour une surveillance de l'état sont toujours applicables même lorsque la surveillance de l'état est désactivée.

Surveillance d'une alarme CloudWatch

> **Note**
>
> Nous mettons à jour la console de vérification de l'état de santé de Route 53. Pendant la période de transition, vous pouvez continuer à utiliser l'ancienne console.

Choisissez l'onglet correspondant à la console que vous utilisez.

- Nouvelle console
- Ancienne console

New console

Si vous souhaitez que ce bilan de santé surveille l'état d'une CloudWatch alarme, spécifiez les valeurs suivantes :

- CloudWatch alarme
- Statut de la surveillance de l'état

CloudWatch alarme

Choisissez l' CloudWatch alarme que vous souhaitez que Route 53 utilise pour déterminer si ce bilan de santé est correct. L' CloudWatch alarme doit être Compte AWS identique au bilan de santé.

> **Note**
>
> Route 53 prend en charge les CloudWatch alarmes dotées des fonctionnalités suivantes :
>
> - Métriques de résolution standard. Les métriques haute résolution ne sont pas prises en charge. Pour plus d'informations, consultez la section Mesures haute résolution dans le guide de l' CloudWatch utilisateur Amazon.
> - Statistiques : `Average`, `Minimum`, `Maximum`, `Sum` et `SampleCount`. Les statistiques étendues ne sont pas prises en charge.
> - Route 53 ne prend pas en charge les alarmes « M sur N ». Pour plus d'informations, consultez la section Évaluation d'une alarme dans le CloudWatch guide Amazon.
>
> Route 53 ne prend pas en charge les alarmes qui utilisent des métriques mathématiques pour interroger plusieurs CloudWatch métriques.

Si vous souhaitez créer une alarme, effectuez les opérations suivantes :

1. Sélectionnez Créer. La CloudWatch console apparaît dans un nouvel onglet du navigateur.
2. Entrez les valeurs applicables. Pour plus d'informations, consultez la section Créer ou modifier une CloudWatch alarme dans le guide de CloudWatch l'utilisateur Amazon.
3. Revenez à l'onglet de navigateur dans lequel apparaît la console Route 53.
4. Cliquez sur le bouton d'actualisation situé à côté de la liste des CloudWatchalarmes.

5. Choisissez la nouvelle alarme dans la liste.

> **Important**
>
> Si vous modifiez les paramètres de l' CloudWatch alarme après avoir créé un bilan de santé, vous devez le mettre à jour. Pour de plus amples informations, veuillez consulter Mise à jour des bilans de santé lorsque vous modifiez les paramètres des CloudWatch alarmes (bilans de santé qui surveillent uniquement une CloudWatch alarme).

Statut de la surveillance de l'état

Choisissez l'état du bilan de santé (sain, malsain ou dernier état connu) lorsque CloudWatch les données sont insuffisantes pour déterminer l'état de l'alarme que vous avez choisie pour l'CloudWatchalarme. Si vous choisissez d'utiliser le dernier état connu, Route 53 utilise l'état du bilan de santé enregistré lors de la dernière analyse de données suffisantes pour déterminer l'état de l'alarme. CloudWatch Pour les nouvelles surveillances de l'état n'ayant aucun dernier statut connu, le statut par défaut de la surveillance de l'état est « sain ».

La valeur du statut Health check fournit un statut temporaire lorsque le flux de données d'une CloudWatch métrique est brièvement indisponible. (Route 53 surveille les flux de données pour CloudWatch détecter les métriques, et non l'état de l'alarme correspondante.) Si la métrique est indisponible fréquemment ou pendant de longues périodes (plus de quelques heures), nous vous recommandons de ne pas utiliser le dernier statut connu.

Old console

Si vous souhaitez que ce bilan de santé surveille l'état d'une CloudWatch alarme, spécifiez les valeurs suivantes :

- CloudWatch alarme
- Statut de la surveillance de l'état
- Inverser le statut de surveillance de l'état
- Désactivées

CloudWatch alarme

Choisissez l' CloudWatch alarme que vous souhaitez que Route 53 utilise pour déterminer si ce bilan de santé est correct. L' CloudWatch alarme doit être Compte AWS identique au bilan de santé.

> **Note**
>
> Route 53 prend en charge les CloudWatch alarmes dotées des fonctionnalités suivantes :
>
> - Métriques de résolution standard. Les métriques haute résolution ne sont pas prises en charge. Pour plus d'informations, consultez la section Mesures haute résolution dans le guide de l' CloudWatch utilisateur Amazon.
> - Statistiques : `Average`, `Minimum`, `Maximum`, `Sum` et `SampleCount`. Les statistiques étendues ne sont pas prises en charge.
> - Route 53 ne prend pas en charge les alarmes « M sur N ». Pour plus d'informations, consultez la section Évaluation d'une alarme dans le CloudWatch guide Amazon.
>
> Route 53 ne prend pas en charge les alarmes qui utilisent des métriques mathématiques pour interroger plusieurs CloudWatch métriques.

Si vous souhaitez créer une alarme, effectuez les opérations suivantes :

1. Sélectionnez Créer. La CloudWatch console apparaît dans un nouvel onglet du navigateur.
2. Entrez les valeurs applicables. Pour plus d'informations, consultez la section Créer ou modifier une CloudWatch alarme dans le guide de CloudWatch l'utilisateur Amazon.
3. Revenez à l'onglet de navigateur dans lequel apparaît la console Route 53.
4. Cliquez sur le bouton d'actualisation situé à côté de la liste des CloudWatchalarmes.
5. Choisissez la nouvelle alarme dans la liste.

> **Important**
>
> Si vous modifiez les paramètres de l' CloudWatch alarme après avoir créé un bilan de santé, vous devez le mettre à jour. Pour de plus amples informations, veuillez consulter Mise à jour des bilans de santé lorsque vous modifiez les paramètres des

CloudWatch alarmes (bilans de santé qui surveillent uniquement une CloudWatch alarme).

Statut de la surveillance de l'état

Choisissez l'état du bilan de santé (sain, malsain ou dernier état connu) lorsque CloudWatch les données sont insuffisantes pour déterminer l'état de l'alarme que vous avez choisie pour l'CloudWatchalarme. Si vous choisissez d'utiliser le dernier état connu, Route 53 utilise l'état du bilan de santé enregistré lors de la dernière analyse de données suffisantes pour déterminer l'état de l'alarme. CloudWatch Pour les nouvelles surveillances de l'état n'ayant aucun dernier statut connu, le statut par défaut de la surveillance de l'état est « sain ».

La valeur du statut Health check fournit un statut temporaire lorsque le flux de données d'une CloudWatch métrique est brièvement indisponible. (Route 53 surveille les flux de données pour CloudWatch détecter les métriques, et non l'état de l'alarme correspondante.) Si la métrique est indisponible fréquemment ou pendant de longues périodes (plus de quelques heures), nous vous recommandons de ne pas utiliser le dernier statut connu.

Inverser l'état du bilan de santé (ancienne console uniquement)

Pour inverser un bilan de santé sur la nouvelle console, consultezContrôles de santé inversés.

Décidez si vous voulez que Route 53 inverse le statut d'une surveillance de l'état. Si vous sélectionnez cette option, Route 53 considère que les surveillances de l'état ne sont pas saines lorsque le statut est sain, et vice versa.

Désactivé (ancienne console uniquement)

Pour désactiver un contrôle de santé sur la nouvelle console, consultezActivation ou désactivation des bilans de santé.

Empêche Route 53 de poursuivre l'exécution de surveillances de l'état. Lorsque vous désactivez un bilan de santé, Route 53 arrête de surveiller les CloudWatch métriques correspondantes.

Lorsque vous désactivez une surveillance de l'état, Route 53 considère que le statut de la surveillance de l'état est toujours sain. Si vous avez configuré le basculement DNS, Route 53 continue à acheminer le trafic vers les ressources correspondantes. Si vous souhaitez arrêter d'acheminer le trafic vers une ressource, inversez le bilan de santé.

> **Note**
>
> Les frais pour une surveillance de l'état sont toujours applicables même lorsque la surveillance de l'état est désactivée.

Configuration avancée (option « Monitor an endpoint » uniquement)

> **Note**
>
> Nous mettons à jour la console de vérification de l'état de santé de Route 53. Pendant la période de transition, vous pouvez continuer à utiliser l'ancienne console.

- Nouvelle console
- Ancienne console

New console

- Intervalle entre les demandes
- Seuil d'échec
- Correspondance de chaînes
- Chaînes de recherche
- Graphiques de latence
- Activer le SNI
- Nom d'hôte

Intervalle entre requêtes

Nombre de secondes entre le moment où chaque outil de surveillance de l'état Route 53 obtient une réponse de votre point de terminaison et le moment où il envoie la demande de surveillance de l'état suivante. Si vous choisissez un intervalle de 30 secondes, chaque outil de surveillance de l'état Route 53 dans les centres de données du monde entier envoie à votre point de terminaison une demande de surveillance de l'état toutes les 30 secondes. En moyenne, votre point de terminaison reçoit une demande de surveillance de l'état toutes

les deux secondes. Si vous choisissez un intervalle de 10 secondes, le point de terminaison recevra une demande plusieurs fois par seconde.

Notez que les outils de surveillance de l'état Route 53 de différents centres de données ne sont pas coordonnés. C'est la raison pour laquelle vous verrez parfois plusieurs demandes par seconde, quel que soit l'intervalle choisi, puis quelques secondes sans surveillance de l'état.

Une fois que vous avez créé une surveillance de l'état, vous ne pouvez pas modifier la valeur de Intervalle entre les demandes.

> **Note**
>
> Si vous choisissez Rapide (10 secondes) pour la valeur de Intervalle entre les demandes, des frais s'appliquent. Pour en savoir plus, consultez Tarification Route 53.

Seuil d'échec

Nombre de surveillances de l'état consécutives pour lesquelles un point de terminaison doit réussir ou échouer pour que Route 53 modifie le statut actuel du point de terminaison en non sain ou sain, ou vice versa. Pour de plus amples informations, veuillez consulter Comment Amazon Route 53 détermine si une surveillance de l'état est saine.

Recherche de chaîne (HTTP et HTTPS uniquement)

Si vous souhaitez que Route 53 détermine l'état d'un point de terminaison en envoyant une demande HTTP ou HTTPS au point de terminaison et en recherchant une chaîne spécifiée dans le corps de réponse. Si le corps de la réponse contient la valeur que vous spécifiez dans Search string (Recherche de chaîne), Route 53 considère que le point de terminaison est sain. Dans le cas contraire, ou si le point de terminaison ne répond pas, Route 53 considère que le point de terminaison n'est pas sain. La chaîne de recherche doit figurer intégralement dans les 5 120 premiers octets du corps de la réponse.

Une fois que vous avez créé une surveillance de l'état, vous ne pouvez pas modifier la valeur String matching.

> **Note**
>
> Si vous choisissez la valeur Yes pour String matching, des frais s'appliquent. Pour en savoir plus, consultez Tarification Route 53.

Comment les outils de surveillance de l'état gèrent une réponse compressée

Si le point de terminaison est un serveur web qui renvoie une réponse compressée, l'outil de surveillance de l'état Route 53 décompresse la réponse avant de rechercher la chaîne de recherche spécifiée uniquement si le serveur web a compressé la réponse à l'aide d'un algorithme de compression pris en charge par les surveillances de l'état. Les outils de surveillance de l'état prennent en charge les algorithmes de compression suivants :

- Gzip
- Deflate

Si la réponse est compressée à l'aide d'un autre algorithme, l'outil de surveillance de l'état ne peut pas décompresser la réponse avant de rechercher la chaîne. Dans ce cas, la recherche échoue presque toujours, et Route 53 considère que le point de terminaison n'est pas sain.

Chaîne de recherche (uniquement lorsque l'option « String matching » [Recherche de chaîne] est activée)

Chaîne que vous souhaitez que Route 53 procède à une recherche dans le corps de la réponse à partir de votre point de terminaison. La longueur maximale est de 255 caractères.

Route 53 prend cette situation en compte lors de la recherche de la valeur de Search string (Chaîne de recherche) dans le corps de la réponse.

Graphiques de latence

Choisissez si vous souhaitez que Route 53 mesure la latence entre les vérificateurs de santé de plusieurs AWS régions et votre terminal. Si vous choisissez cette option, les graphiques de CloudWatch latence apparaissent dans l'onglet Latency de la page Health checks de la console Route 53. Si les outils de surveillance de l'état Route 53 ne parviennent pas à se connecter au point de terminaison, Route 53 ne peut pas afficher de graphique de la latence pour ce point de terminaison.

Une fois que vous avez créé une surveillance de l'état, vous ne pouvez pas modifier la valeur de Mesures de latence.

> **Note**
>
> Si vous configurez Route 53 pour mesurer la latence entre les outils de surveillance de l'état et votre point de terminaison, des frais s'appliquent. Pour en savoir plus, consultez Tarification Route 53.

Activer SNI (HTTPS uniquement)

Spécifiez si vous souhaitez que Route 53 envoie le nom d'hôte au point de terminaison dans le message `client_hello` lors de la négociation TLS. Cela permet au point de terminaison de répondre à la demande HTTPS avec le SSL/TLS certificat applicable.

Certains points de terminaison nécessitent que les requêtes HTTPS incluent le nom d'hôte dans le message client_hello. Si vous n'activez pas le SNI, l'état du bilan de santé peut indiquer un échec. Le message d'erreur dépend de la façon dont le serveur est configuré pour répondre à la demande ne contenant aucune information SNI. Un bilan de santé peut également présenter un état d'échec pour d'autres raisons. Si SNI est activé et que l'erreur persiste, vérifiez la configuration SSL/TLS sur votre point de terminaison et vérifiez la validité de votre certificat.

Notez les critères suivants :

- Le point de terminaison doit prendre en charge SNI.
- Le SSL/TLS certificat sur votre terminal inclut un nom de domaine dans le `Common Name` champ et éventuellement plusieurs autres dans le `Subject Alternative Names` champ. L'un des noms de domaines du certificat doit correspondre à la valeur spécifiée pour Host name (Nom d'hôte).

Régions des outils de surveillance de l'état

Indiquez si vous voulez que Route 53 vérifie l'état du point de terminaison à l'aide d'outils de surveillance de l'état dans les régions recommandées ou à l'aide d'outils de surveillance de l'état dans les régions que vous spécifiez.

Si vous mettez à jour une surveillance de l'état pour supprimer une région qui a effectué des surveillances de l'état, Route 53 continue d'effectuer des vérifications de cette région pendant 1 heure au plus. Cela garantit que certains outils de surveillance de l'état vérifient toujours le point de terminaison (par exemple, si vous remplacez trois régions par quatre régions différentes).

Si vous choisissez Customize (Personnaliser), cliquez sur le signe x correspondant à une région pour la supprimer. Cliquez sur l'espace au bas de la liste pour rajouter une région à la liste. Vous devez spécifier au moins trois régions.

Nom d'hôte (uniquement pour l'option « Specify endpoint by IP address » [Spécifier le point de terminaison par adresse IP], protocoles HTTP et HTTPS uniquement)

La valeur que vous souhaitez que Route 53 transmette dans l'en-tête `Host` des surveillances de l'état HTTP et HTTPS. Il s'agit généralement du nom DNS complet du site web sur lequel vous souhaitez que Route 53 procède aux surveillances de l'état. Lorsque Route 53 vérifie l'état d'un point de terminaison, voici comment l'en-tête `Host` est construit :

- Si vous spécifiez la valeur **`80`** pour Port et HTTP pour Protocol (Protocole), Route 53 transmet au point de terminaison un en-tête `Host` qui contient la valeur de Host name (Nom d'hôte).
- Si vous spécifiez la valeur **`443`** pour le port et le protocole HTdTPS pour le protocole, Route 53 transmet au point de terminaison un `Host` en-tête contenant la valeur du nom d'hôte.
- Si vous spécifiez une autre valeur pour le port et HTTP ou HTTPS pour le protocole, Route 53 transmet au point de terminaison un `Host` en-tête contenant la valeur *`Host name`* :*`Port`*.

Si vous choisissez de spécifier le point de terminaison par adresse IP et que vous ne spécifiez pas de valeur pour Host name (Nom d'hôte), Route 53 remplace la valeur IP address (Adresse IP) dans l'en-tête `Host` de chacun des cas précédents.

Old console

Si vous sélectionnez l'option pour surveiller un point de terminaison, vous pouvez également spécifier les paramètres suivants :

- Intervalle entre les demandes
- Seuil d'échec
- Correspondance de chaînes
- Chaîne de recherche
- Graphique de latence
- Activer le SNI
- Health Checker Regions
- Inverser le statut de surveillance de l'état
- Désactivées

Intervalle entre requêtes

Nombre de secondes entre le moment où chaque outil de surveillance de l'état Route 53 obtient une réponse de votre point de terminaison et le moment où il envoie la demande de surveillance de l'état suivante. Si vous choisissez un intervalle de 30 secondes, chaque outil de surveillance de l'état Route 53 dans les centres de données du monde entier envoie à votre point de terminaison une demande de surveillance de l'état toutes les 30 secondes. En moyenne, votre point de terminaison reçoit une demande de surveillance de l'état toutes les deux secondes. Si vous choisissez un intervalle de 10 secondes, le point de terminaison recevra une demande plusieurs fois par seconde.

Notez que les outils de surveillance de l'état Route 53 de différents centres de données ne sont pas coordonnés. C'est la raison pour laquelle vous verrez parfois plusieurs demandes par seconde, quel que soit l'intervalle choisi, puis quelques secondes sans surveillance de l'état.

Une fois que vous avez créé une surveillance de l'état, vous ne pouvez pas modifier la valeur de Intervalle entre les demandes.

> **Note**
>
> Si vous choisissez Rapide (10 secondes) pour la valeur de Intervalle entre les demandes, des frais s'appliquent. Pour en savoir plus, consultez Tarification Route 53.

Seuil d'échec

Nombre de surveillances de l'état consécutives pour lesquelles un point de terminaison doit réussir ou échouer pour que Route 53 modifie le statut actuel du point de terminaison en non sain ou sain, ou vice versa. Pour de plus amples informations, veuillez consulter Comment Amazon Route 53 détermine si une surveillance de l'état est saine.

Recherche de chaîne (HTTP et HTTPS uniquement)

Si vous souhaitez que Route 53 détermine l'état d'un point de terminaison en envoyant une demande HTTP ou HTTPS au point de terminaison et en recherchant une chaîne spécifiée dans le corps de réponse. Si le corps de la réponse contient la valeur que vous spécifiez dans Search string (Recherche de chaîne), Route 53 considère que le point de terminaison est sain. Dans le cas contraire, ou si le point de terminaison ne répond pas, Route 53 considère que le point de terminaison n'est pas sain. La chaîne de recherche doit figurer intégralement dans les 5 120 premiers octets du corps de la réponse.

Une fois que vous avez créé une surveillance de l'état, vous ne pouvez pas modifier la valeur String matching.

> **Note**
>
> Si vous choisissez la valeur Yes pour String matching, des frais s'appliquent. Pour en savoir plus, consultez Tarification Route 53.

Comment les outils de surveillance de l'état gèrent une réponse compressée

Si le point de terminaison est un serveur web qui renvoie une réponse compressée, l'outil de surveillance de l'état Route 53 décompresse la réponse avant de rechercher la chaîne de recherche spécifiée uniquement si le serveur web a compressé la réponse à l'aide d'un algorithme de compression pris en charge par les surveillances de l'état. Les outils de surveillance de l'état prennent en charge les algorithmes de compression suivants :

- Gzip
- Deflate

Si la réponse est compressée à l'aide d'un autre algorithme, l'outil de surveillance de l'état ne peut pas décompresser la réponse avant de rechercher la chaîne. Dans ce cas, la recherche échoue presque toujours, et Route 53 considère que le point de terminaison n'est pas sain.

Chaîne de recherche (uniquement lorsque l'option « String matching » [Recherche de chaîne] est activée)

Chaîne que vous souhaitez que Route 53 procède à une recherche dans le corps de la réponse à partir de votre point de terminaison. La longueur maximale est de 255 caractères.

Route 53 prend cette situation en compte lors de la recherche de la valeur de Search string (Chaîne de recherche) dans le corps de la réponse.

Graphiques de latence

Choisissez si vous souhaitez que Route 53 mesure la latence entre les vérificateurs de santé de plusieurs AWS régions et votre terminal. Si vous choisissez cette option, les graphiques de CloudWatch latence apparaissent dans l'onglet Latency de la page Health checks de la console Route 53. Si les outils de surveillance de l'état Route 53 ne parviennent pas à se connecter au point de terminaison, Route 53 ne peut pas afficher de graphique de la latence pour ce point de terminaison.

Une fois que vous avez créé une surveillance de l'état, vous ne pouvez pas modifier la valeur de Mesures de latence.

> **Note**
>
> Si vous configurez Route 53 pour mesurer la latence entre les outils de surveillance de l'état et votre point de terminaison, des frais s'appliquent. Pour en savoir plus, consultez Tarification Route 53.

Activer SNI (HTTPS uniquement)

Spécifiez si vous souhaitez que Route 53 envoie le nom d'hôte au point de terminaison dans le message `client_hello` lors de la négociation TLS. Cela permet au point de terminaison de répondre à la demande HTTPS avec le SSL/TLS certificat applicable.

Certains points de terminaison exigent que les demandes HTTPS incluent le nom d'hôte dans le message `client_hello`. Si vous n'activez pas le SNI, l'état du bilan de santé peut indiquer un échec. Le message d'erreur dépend de la façon dont le serveur est configuré pour répondre à la demande ne contenant aucune information SNI. Un bilan de santé peut également présenter un état d'échec pour d'autres raisons. Si le SNI est activé et que le message d'erreur persiste, vérifiez la SSL/TLS configuration sur votre terminal et confirmez que votre certificat est valide.

Notez les critères suivants :

- Le point de terminaison doit prendre en charge SNI.
- Le SSL/TLS certificat sur votre terminal inclut un nom de domaine dans le `Common Name` champ et éventuellement plusieurs autres dans le `Subject Alternative Names` champ. L'un des noms de domaines du certificat doit correspondre à la valeur spécifiée pour Host name (Nom d'hôte).

Régions des outils de surveillance de l'état

Indiquez si vous voulez que Route 53 vérifie l'état du point de terminaison à l'aide d'outils de surveillance de l'état dans les régions recommandées ou à l'aide d'outils de surveillance de l'état dans les régions que vous spécifiez.

Si vous mettez à jour une surveillance de l'état pour supprimer une région qui a effectué des surveillances de l'état, Route 53 continue d'effectuer des vérifications de cette région pendant 1 heure au plus. Cela garantit que certains outils de surveillance de l'état vérifient toujours

le point de terminaison (par exemple, si vous remplacez trois régions par quatre régions différentes).

Si vous choisissez Customize (Personnaliser), cliquez sur le signe x correspondant à une région pour la supprimer. Cliquez sur l'espace au bas de la liste pour rajouter une région à la liste. Vous devez spécifier au moins trois régions.

Inverser l'état du bilan de santé (ancienne console uniquement)

Pour inverser un bilan de santé sur la nouvelle console, consultez Contrôles de santé inversés.

Décidez si vous voulez que Route 53 inverse le statut d'une surveillance de l'état. Si vous choisissez cette option, Route 53 considère qu'un bilan de santé n'est pas sain lorsque l'état est sain et vice versa. Par exemple, il se peut que vous vouliez que Route 53 considère une surveillance de l'état comme non saine si vous configurez une correspondance de chaîne et que le point de terminaison retourne une valeur spécifiée.

Désactivé (ancienne console uniquement)

Pour désactiver un contrôle de santé sur la nouvelle console, consultez Activation ou désactivation des bilans de santé.

Empêche Route 53 de poursuivre l'exécution de surveillances de l'état. Lorsque vous désactivez une surveillance de l'état, Route 53 arrête de tenter d'établir une connexion TCP avec le point de terminaison.

Lorsque vous désactivez une surveillance de l'état, Route 53 considère que le statut de la surveillance de l'état est toujours sain. Si vous avez configuré le basculement DNS, Route 53 continue à acheminer le trafic vers les ressources correspondantes. Si vous souhaitez arrêter d'acheminer le trafic vers une ressource, inversez le bilan de santé.

> **Note**
>
> Les frais pour une surveillance de l'état sont toujours applicables même lorsque la surveillance de l'état est désactivée.

Être informé en cas d'échec d'une surveillance de l'état

Utilisez les options suivantes pour configurer les notifications par e-mail lorsqu'une surveillance de l'état échoue :

- Create alarm
- Send notification to
- Topic name
- Recipient email addresses

Créer une alarme (uniquement lors de la création de surveillances de l'état)

Spécifiez si vous souhaitez créer une CloudWatch alarme par défaut. Si vous choisissez Oui, vous CloudWatch envoie une notification Amazon SNS lorsque le statut de ce point de terminaison devient défectueux et que Route 53 considère que le point de terminaison est défectueux pendant une minute.

> **Note**
>
> Si vous CloudWatch souhaitez vous envoyer une autre notification Amazon SNS lorsque le statut redevient sain, vous pouvez créer une autre alarme après avoir créé le bilan de santé. Pour plus d'informations, consultez la section Création d' CloudWatch alarmes Amazon dans le guide de CloudWatch l'utilisateur Amazon.

Si vous souhaitez créer une alarme pour une surveillance de l'état existante, ou si vous souhaitez recevoir des notifications lorsque Route 53 considère que le point de terminaison n'est pas sain pendant environ une minute (la valeur par défaut), sélectionnez Non et ajoutez une alarme après avoir créé la surveillance de l'état. Pour de plus amples informations, veuillez consulter Surveillance des bilans de santé à l'aide CloudWatch.

Envoyer une notification à (uniquement lors de la création d'une alarme)

Spécifiez si vous CloudWatch souhaitez envoyer des notifications à une rubrique Amazon SNS existante ou à une nouvelle rubrique :

- Rubrique SNS existante – Sélectionnez le nom de la rubrique dans la liste. La rubrique doit résider dans la région USA Est (Virginie du Nord).
- Nouvelle rubrique SNS – Indiquez le nom de la rubrique dans Topic name (Nom de la rubrique) et saisissez les adresses e-mail auxquelles vous souhaitez envoyer des notifications dans Recipients (Destinataires). Séparez plusieurs adresses par une virgule, un point-virgule ou un espace.

  Route 53 crée alors la rubrique dans la région USA Est (Virginie du Nord).

Topic name (uniquement lors de la création d'une rubrique SNS)

Si vous avez spécifié New SNS Topic, entrez le nom de la nouvelle rubrique.

Recipient email addresses (uniquement lors de la création d'une rubrique SNS)

Si vous avez spécifié New SNS topic, saisissez les adresses e-mail auxquelles vous souhaitez envoyer des notifications. Séparez les noms par des virgules (,), des points virgules (;) ou de espaces.

Valeurs qu'Amazon Route 53 affiche lors de la création d'une surveillance de l'état

La page Créer une surveillance de l'état affiche les valeurs suivantes en fonction des valeurs que vous avez saisies :

URL

Soit l'URL complète (pour les surveillances de l'état HTTP ou HTTPS) soit l'adresse IP et le port (pour les surveillances de l'état TCP) auxquels Route 53 envoie les demandes lors de l'exécution des surveillances de l'état.

Type de surveillance de l'état

Soit Basic ou Basic + additional options, en fonction des paramètres que vous avez spécifiés pour cette surveillance de l'état. Pour plus d'informations sur la tarification des options supplémentaires, consultez Tarification Route 53.

Mise à jour des bilans de santé lorsque vous modifiez les paramètres des CloudWatch alarmes (bilans de santé qui surveillent uniquement une CloudWatch alarme)

Si vous créez un bilan de santé Route 53 qui surveille le flux de données pour détecter une CloudWatch alarme, puis que vous mettez à jour les paramètres de l' CloudWatch alarme, Route 53 ne met pas automatiquement à jour les paramètres d'alarme dans le bilan de santé. Si vous souhaitez que la surveillance de l'état commence à utiliser les nouveaux paramètres de l'alarme, vous devez mettre à jour la surveillance de l'état.

> **Note**
>
> Pour mettre à jour une surveillance de l'état par programmation, vous pouvez utiliser l'API `UpdateHealthCheck`. Spécifiez simplement les valeurs actuelles pour `AlarmIdentifier` et`Region`, et Route 53 obtiendra les derniers paramètres à partir de CloudWatch. Pour plus d'informations, consultez UpdateHealthCheckle manuel Amazon Route 53 API Reference.

> **Note**
>
> Nous mettons à jour la console de vérification de l'état de santé de Route 53. Pendant la période de transition, vous pouvez continuer à utiliser l'ancienne console.

Choisissez l'onglet correspondant à la console que vous utilisez.

- Nouvelle console
- Ancienne console

New console

Pour mettre à jour un bilan de santé avec de nouveaux paramètres CloudWatch d'alarme

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation, choisissez Health checks.
3. Sélectionnez l'identifiant associé pour le bilan de santé que vous souhaitez mettre à jour.
4. Choisissez Modifier.

   Une note explique que l' CloudWatch alarme du bilan de santé a changé. Le champ Détails contient les nouveaux paramètres de l'alarme.
5. Choisissez Enregistrer.

Old console

Pour mettre à jour un bilan de santé avec de nouveaux paramètres CloudWatch d'alarme (console)

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation, sélectionnez Health Checks.
3. Cochez la case correspondant à la surveillance de l'état à mettre à jour.
4. Choisissez Modifier la surveillance de l'état.

   Une note explique que l' CloudWatch alarme du bilan de santé a changé. Le champ Détails contient les nouveaux paramètres de l'alarme.
5. Choisissez Enregistrer.

Activation ou désactivation des bilans de santé

La désactivation d'un bilan de santé empêche Route 53 d'effectuer des bilans de santé. Lorsque vous désactivez une surveillance de l'état, Route 53 arrête de regrouper le statut des surveillances de l'état référencées. Lorsque vous désactivez une surveillance de l'état, Route 53 considère que le statut de la surveillance de l'état est toujours sain. Si vous avez configuré le basculement DNS, Route 53 continue à acheminer le trafic vers les ressources correspondantes. Si vous souhaitez arrêter d'acheminer le trafic vers une ressource, modifiez la valeur de Inverted.

> **Note**
>
> Nous mettons à jour la console de vérification de l'état de santé de Route 53. Pendant la période de transition, vous pouvez continuer à utiliser l'ancienne console.

Vous pouvez désactiver ou activer un contrôle de santé sur l'ancienne console lorsque vous créez ou modifiez le bilan de santé. Pour de plus amples informations, veuillez consulter Valeurs que vous spécifiez lors de la création ou de la mise à jour de surveillances de l'état.

Pour désactiver les contrôles de santé sur la nouvelle console, effectuez la procédure suivante.

Pour désactiver ou activer un contrôle de santé (nouvelle console uniquement)

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation, choisissez Health checks.
3. Dans la colonne Actions, sélectionnez les trois points, puis Désactiver ou Activer.

   Vous pouvez également sélectionner l'identifiant associé au bilan de santé que vous souhaitez désactiver ou activer.
4. Dans le tableau Configuration, le champ État indique si le contrôle de santé est activé ou désactivé.
5. Choisissez Désactiver ou Activer pour désactiver ou activer le contrôle de santé.

Contrôles de santé inversés

Si vous inversez un bilan de santé, Route 53 considère que le bilan de santé n'est pas sain lorsque l'état est sain et vice versa.

> **Note**
>
> Nous mettons à jour la console de vérification de l'état de santé de Route 53. Pendant la période de transition, vous pouvez continuer à utiliser l'ancienne console.

Vous pouvez inverser un bilan de santé sur l'ancienne console lorsque vous créez ou modifiez le bilan de santé. Pour de plus amples informations, veuillez consulter Valeurs que vous spécifiez lors de la création ou de la mise à jour de surveillances de l'état.

Pour inverser les contrôles de santé sur la nouvelle console, effectuez la procédure suivante.

Pour inverser un bilan de santé (nouvelle console uniquement)

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation, choisissez Health checks.
3. Dans la colonne Actions, sélectionnez les trois points, puis Inversez.

   Ou sélectionnez l'identifiant associé au bilan de santé que vous souhaitez inverser.

4. Dans le tableau Configuration, le champ Inversé indique si le contrôle de santé est inversé (Oui) ou non (Non).
5. Choisissez Inverser pour inverser le bilan de santé.

   Si vous souhaitez annuler le statut inversé et que le champ Inversé est Oui, sélectionnez à nouveau Inverser.

Suppression de surveillances de l'état

Pour désactiver les contrôles de santé, effectuez la procédure suivante.

> **Note**
>
> Si vous utilisez AWS Cloud Map et que vous avez configuré AWS Cloud Map pour créer un bilan de santé Route 53 lorsque vous enregistrez une instance, vous ne pouvez pas utiliser la console Route 53 pour supprimer le bilan de santé. La surveillance de l'état est automatiquement supprimée lorsque vous annuler l'enregistrement de l'instance. Un délai de plusieurs heures peut être nécessaire avant que la surveillance de l'état n'apparaisse plus dans la console Route 53.

> **Note**
>
> Nous mettons à jour la console de vérification de l'état de santé de Route 53. Pendant la période de transition, vous pouvez continuer à utiliser l'ancienne console.

Choisissez l'onglet correspondant à la console que vous utilisez.

- Nouvelle console
- Ancienne console

New console

Pour supprimer un bilan de santé

1. Si vous supprimez des surveillances de l'état associées à des enregistrements, exécutez les tâches recommandées dans la section Mise à jour ou suppression de surveillances de l'état lorsque le basculement DNS est configuré.
2. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
3. Dans le volet de navigation, choisissez Health checks.
4. Sélectionnez l'identifiant associé au bilan de santé que vous souhaitez supprimer.
5. Sélectionnez Delete (Supprimer).
6. Entrez **`confirm`** dans la zone de texte, puis choisissez Supprimer.

Old console

Pour supprimer une surveillance de l'état (console)

1. Si vous supprimez des surveillances de l'état associées à des enregistrements, exécutez les tâches recommandées dans la section Mise à jour ou suppression de surveillances de l'état lorsque le basculement DNS est configuré.
2. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
3. Dans le volet de navigation, sélectionnez Health Checks.
4. Dans le volet de droite, sélectionnez la surveillance de l'état que vous souhaitez supprimer.
5. Choisissez Delete Health Check.
6. Choisissez Yes, Delete pour confirmer.

Mise à jour ou suppression de surveillances de l'état lorsque le basculement DNS est configuré

Pour mettre à jour ou supprimer des surveillances de l'état associées à des enregistrements, ou modifier des enregistrements associés à des surveillances de l'état, vous devez tenir compte de la façon dont vos modifications affectent le routage des requêtes DNS et la configuration du basculement DNS.

> **Important**
>
> Route 53 ne vous empêche pas de supprimer une surveillance de l'état, même si elle est associée à un ou plusieurs enregistrements. Si vous supprimez une surveillance de l'état et ne mettez pas à jour les enregistrements associés, le statut futur de la surveillance de l'état n'est pas prévisible et peut changer. Cela affectera l'acheminement des requêtes DNS destinées à votre configuration de basculement DNS.

Pour mettre à jour ou supprimer des surveillances de l'état déjà associées à des enregistrements, nous vous recommandons d'effectuer les tâches suivantes :

1. Identifiez les enregistrements associés aux surveillances de l'état. Pour cela, vous devez effectuer l'une des actions suivantes :
   - Passez en revue les enregistrements de chaque zone hébergée à l'aide de la console Route 53. Pour de plus amples informations, veuillez consulter Liste des enregistrements.
   - Exécutez l'action d'API `ListResourceRecordSets` sur chaque zone hébergée et vérifiez la réponse. Pour plus d'informations, consultez ListResourceRecordSetsle manuel Amazon Route 53 API Reference.
2. Évaluez le changement de comportement qu'entraînera la mise à jour ou la suppression des surveillances de l'état, ou la mise à jour d'enregistrements. En fonction de cette évaluation, déterminez les modifications nécessaires.

   Pour plus d'informations, consultez Que se passe-t-il lorsque vous omettez des surveillances de l'état ?
3. Modifiez les surveillances de l'état et les enregistrements selon les besoins. Pour plus d'informations, consultez les rubriques suivantes :
   - Création et mise à jour de surveillances de l'état
   - Modification des enregistrements
4. Supprimez les surveillances de l'état que vous n'utilisez plus, le cas échéant. Pour de plus amples informations, veuillez consulter Suppression de surveillances de l'état.

Configuration des règles de pare-feu et de routeur pour les surveillances de l'état Amazon Route 53

Lorsque Route 53 vérifie l'état d'un point de terminaison, il envoie une demande HTTP, HTTPS ou TCP à l'adresse IP et au port que vous avez spécifiés lorsque vous avez créé la surveillance de l'état. Pour qu'une surveillance de l'état réussisse, les règles de pare-feu et de routeur doivent autoriser le trafic entrant à partir des adresses IP utilisées par les outils de surveillance de l'état Route 53.

Pour la liste actuelle des adresses IP pour les vérificateurs de santé Route 53, pour les serveurs de noms Route 53 et pour les autres AWS services, consultezPlages d'adresses IP de serveurs Amazon Route 53.

Sur Amazon EC2, les groupes de sécurité agissent comme des pare-feux. Pour plus d'informations, consultez les groupes de EC2 sécurité Amazon dans le guide de EC2 l'utilisateur Amazon. Pour configurer vos groupes de sécurité afin d'autoriser les contrôles de santé de Route 53, vous pouvez soit autoriser le trafic entrant provenant de chaque plage d'adresses IP, soit utiliser une liste de préfixes AWS gérée.

Pour utiliser la liste de préfixes AWS-managed, modifiez votre groupe de sécurité afin d'autoriser le `<region>` trafic entrant en provenance de `com.amazonaws.<region>.route53-healthchecks` Région AWS votre EC2 instance ou ressource Amazon. Si vous utilisez les contrôles de santé de la Route 53 pour vérifier les IPv6 points de terminaison, vous devez également autoriser le trafic entrant en provenance de. `com.amazonaws.<region>.ipv6.route53-healthchecks`

Pour plus d'informations sur les listes de AWS préfixes gérées par -managées, consultez la section Travailler avec des listes de AWS préfixes -gérées dans le guide de l'utilisateur Amazon VPC.

> **Important**
>
> Lorsque vous ajoutez des adresses IP à une liste d'adresses IP autorisées, ajoutez toutes les adresses IP de la plage CIDR pour chaque AWS région que vous avez spécifiée lors de la création des bilans de santé, ainsi que la plage CIDR globale. Il se peut que vous constatiez que les demandes de vérification proviennent d'une seule adresse IP au sein d'une région. Toutefois, cette adresse IP peut être modifiée à n'importe quel moment en une autre des adresses IP de cette région.
>
> Si vous souhaitez vous assurer d'inclure à la fois les adresses IP actuelles et anciennes de l'outil de surveillance de l'état, ajoutez toutes les plages d'adresses IP /26 et /18 à la liste autorisée. Pour bénéficier de la liste complète, consultez AWS IP address ranges (Plages d'adresses IP) dans le Références générales AWS.

Lorsque vous ajoutez la liste de AWS préfixes -managed à votre groupe de sécurité entrant, toutes les plages nécessaires sont automatiquement ajoutées.

Configuration du basculement DNS

Lorsque vous disposez de plusieurs ressources qui exécutent la même fonction, par exemple plusieurs serveurs HTTP ou plusieurs serveurs de messagerie, vous pouvez configurer Amazon Route 53 pour qu'il vérifie l'état de vos ressources et réponde aux requêtes DNS en utilisant uniquement les ressources saines. Supposons par exemple que votre site web, example.com, soit hébergé sur 6 serveurs, deux dans chacun des trois centres de données répartis dans le monde. Vous pouvez configurer Route 53 pour qu'il vérifie l'état de ces serveurs et réponde aux requêtes DNS pour example.com en utilisant uniquement les serveurs qui sont actuellement sains.

Route 53 peut vérifier l'état de vos ressources dans des configurations simples et complexes :

- Dans les configurations simples, vous créez un groupe d'enregistrements dont le nom et le type sont identiques : par exemple, un groupe d'enregistrements pondérés de type A pour example.com. Vous configurez ensuite Route 53 pour vérifier l'état des ressources correspondantes. Route 53 répond aux requêtes DNS en fonction de l'état de vos ressources. Pour de plus amples informations, veuillez consulter Fonctionnement des surveillances de l'état dans les configurations Amazon Route 53 simples.
- Dans les configurations plus complexes, vous créez une arborescence d'enregistrements qui acheminent le trafic en fonction de plusieurs critères. Par exemple, si la latence de vos utilisateurs est votre principal critère, vous pouvez utiliser des enregistrements d'alias de latence pour acheminer le trafic vers la région qui fournit la latence optimale. Les enregistrements d'alias de latence peuvent avoir des enregistrements pondérés dans chaque région en tant que cible de l'alias. Les enregistrements pondérés peuvent acheminer le trafic vers EC2 les instances en fonction du type d'instance. Comme pour une configuration simple, vous pouvez configurer Route 53 pour acheminer le trafic en fonction de l'état de vos ressources. Pour de plus amples informations, veuillez consulter Fonctionnement des surveillances de l'état dans les configurations Amazon Route 53 complexes.

Rubriques

- Liste des tâches pour configurer le basculement DNS
- Fonctionnement des surveillances de l'état dans les configurations Amazon Route 53 simples

- Fonctionnement des surveillances de l'état dans les configurations Amazon Route 53 complexes
- Choix des enregistrements par Amazon Route 53 lorsque la surveillance de l'état est configurée
- Basculement actif-actif et actif-passif
- Configuration du basculement dans une zone hébergée privée
- Prévention des problèmes de basculement par Amazon Route 53

Liste des tâches pour configurer le basculement DNS

Pour utiliser Route 53 pour configurer le basculement DNS, effectuez les tâches suivantes :

1. Élaborez un diagramme complet de votre configuration et indiquez le type d'enregistrement que vous créez (alias pondéré, basculement, latence, etc.) pour chaque nœud. Dans la partie supérieure de l'arborescence, placez les enregistrements du nom de domaine, comme example.com, que vos utilisateurs utilisent pour accéder à votre site web ou à une application web.

   Les types d'enregistrements qui apparaissent dans votre diagramme d'arborescence dépendent de la complexité de la configuration :

   - Dans une configuration simple, votre diagramme n'inclut pas d'enregistrements d'alias ou les enregistrements d'alias acheminent le trafic directement à une ressource, telle qu'un équilibreur de charge ELB, au lieu d'un autre enregistrement Route 53. Pour de plus amples informations, veuillez consulter Fonctionnement des surveillances de l'état dans les configurations Amazon Route 53 simples.
   - Dans une configuration complexe, votre diagramme comprendra une combinaison d'enregistrements d'alias (par exemple des alias pondérés et des alias de basculement) et d'enregistrements sans alias dans une arborescence à plusieurs niveaux, comme pour les exemples illustrés dans la rubrique Fonctionnement des surveillances de l'état dans les configurations Amazon Route 53 complexes.

   > **Note**
   >
   > Pour créer rapidement et facilement des enregistrements pour les configurations de routage complexes et associer ces enregistrements à des surveillances de l'état, vous pouvez utiliser l'éditeur visuel de flux de trafic et enregistrer la configuration en tant que stratégie de trafic. Vous pouvez ensuite associer la stratégie de trafic à un ou plusieurs noms de domaine (par exemple, example.com) ou noms de sous-domaine

(par exemple, www.example.com), dans la même zone hébergée ou dans plusieurs zones hébergées. En outre, vous pouvez restaurer les mises à jour si la nouvelle configuration ne fonctionne pas comme vous l'aviez prévu. Pour de plus amples informations, veuillez consulter Utiliser Traffic Flow pour acheminer le trafic DNS.

Pour plus d'informations, consultez la documentation de suivante :

- Sélection d'une stratégie de routage
- Choix entre des enregistrements avec ou sans alias

2. Créez des contrôles de santé pour les ressources pour lesquelles vous ne pouvez pas créer d'enregistrements d'alias, telles que EC2 les serveurs Amazon et les serveurs de messagerie exécutés dans votre centre de données. Vous allez associer ces surveillances de l'état à vos enregistrements sans alias.

   Pour de plus amples informations, veuillez consulter Création, mise à jour et suppression de surveillances de l'état.

3. Si nécessaire, configurez des règles de pare-feu et de routeur afin que Route 53 puisse envoyer des demandes régulières aux points de terminaison que vous avez spécifiés dans vos surveillances de l'état. Pour de plus amples informations, veuillez consulter Configuration des règles de pare-feu et de routeur pour les surveillances de l'état Amazon Route 53.

4. Créez tous les enregistrements sans alias dans le diagramme et associez les surveillances de l'état que vous avez créées à l'étape 2 aux enregistrements applicables.

   Si vous configurez le basculement DNS dans une configuration qui n'inclut pas d'enregistrements d'alias, ignorez les tâches restantes.

5. Créez les enregistrements d'alias qui acheminent le trafic vers les AWS ressources, telles que les équilibreurs de charge et CloudFront les distributions ELB. Si vous souhaitez que Route 53 passe à une autre branche de l'arborescence quand une ressource n'est pas saine, définissez la valeur du paramètre Evaluate Target Health (Évaluer l'état de la cible) sur Yes (Oui) pour chacun de vos enregistrements d'alias. (Evaluate Target Health n'est pas pris en charge pour certaines AWS ressources.)

6. À partir de la base de l'arborescence créée à l'étape 1, créez les enregistrements d'alias qui acheminent le trafic vers les enregistrements que vous avez créés aux étapes 4 et 5. Si vous souhaitez que Route 53 passe à une autre branche de l'arborescence lorsqu'aucun enregistrement sans alias n'est sain dans une branche, définissez la valeur du paramètre

Evaluate Target Health (Évaluer l'état de la cible) sur Yes (Oui) pour chacun de vos enregistrements d'alias.

N'oubliez pas que vous ne pouvez pas créer un enregistrement d'alias acheminant le trafic vers un autre enregistrement tant que vous n'avez pas créé l'autre enregistrement.

Fonctionnement des surveillances de l'état dans les configurations Amazon Route 53 simples

Lorsque vous disposez de deux ou plusieurs ressources assignées à la même fonction, comme deux serveurs web ou plus pour example.com, vous pouvez utiliser les vérifications de contrôle de l'état suivantes pour acheminer le trafic vers les ressources saines uniquement :

Vérifiez l'état des EC2 instances et des autres ressources (enregistrements autres que les alias)

Si vous acheminez le trafic vers des ressources pour lesquelles vous ne pouvez pas créer d'enregistrements d'alias, telles que des EC2 instances, vous créez un enregistrement et un bilan de santé pour chaque ressource. Ensuite, vous associez chaque surveillance de l'état à l'enregistrement applicable. Les surveillances de l'état évaluent régulièrement l'état des ressources correspondantes, et Route 53 achemine le trafic uniquement vers les ressources que les surveillances de l'état signalent comme saines.

Évaluer l'état de santé d'une AWS ressource (alias records)

Si vous utilisez des enregistrements d'alias pour acheminer le trafic vers AWS des ressources sélectionnées, telles que les équilibreurs de charge ELB, vous pouvez configurer Route 53 pour évaluer l'état de santé de la ressource et pour acheminer le trafic uniquement vers les ressources saines. Lorsque vous configurez un enregistrement d'alias pour évaluer l'état d'une ressource, vous n'avez pas besoin de créer une surveillance de l'état pour la ressource.

Voici un aperçu de la manière dont vous configurez Route 53 pour vérifier l'état de vos ressources dans des configurations simples :

1. Vous identifiez les ressources qui doivent être surveillées par Route 53. Par exemple, vous pouvez vouloir surveiller tous les serveurs HTTP qui répondent aux demandes pour example.com.
2. Vous créez des bilans de santé pour les ressources pour lesquelles vous ne pouvez pas créer d'enregistrements d'alias, telles que EC2 les instances ou les serveurs de votre propre centre

de données. Vous spécifiez comment envoyer les demandes de surveillance de l'état à la ressource : le protocole à utiliser (TCP, HTTPS ou HTTP), l'adresse IP et le port à utiliser et, pour les surveillances de l'état HTTP/HTTPS, un nom de domaine et un chemin d'accès.

> **Note**
>
> Si vous utilisez des ressources pour lesquelles vous pouvez créer des enregistrements d'alias, telles que les équilibreurs de charge ELB, ne créez pas de surveillances de l'état pour ces ressources.

Une configuration courante consiste à créer une surveillance de l'état pour chaque ressource et à utiliser la même adresse IP pour le point de terminaison de la surveillance de l'état que pour la ressource. La surveillance de l'état envoie des demandes à l'adresse IP spécifiée.

> **Note**
>
> Route 53 ne peut pas vérifier l'état des ressources dont l'adresse IP se trouve dans des plages locales, privées, non routables ou multicast. Pour plus d'informations sur les adresses IP pour lesquelles vous ne pouvez pas créer de tests de santé, consultez la RFC 5735, IPv4 Adresses à usage spécial, et la RFC 6598, Préfixe réservé à l'IANA pour l'espace d'adressage partagé. IPv4

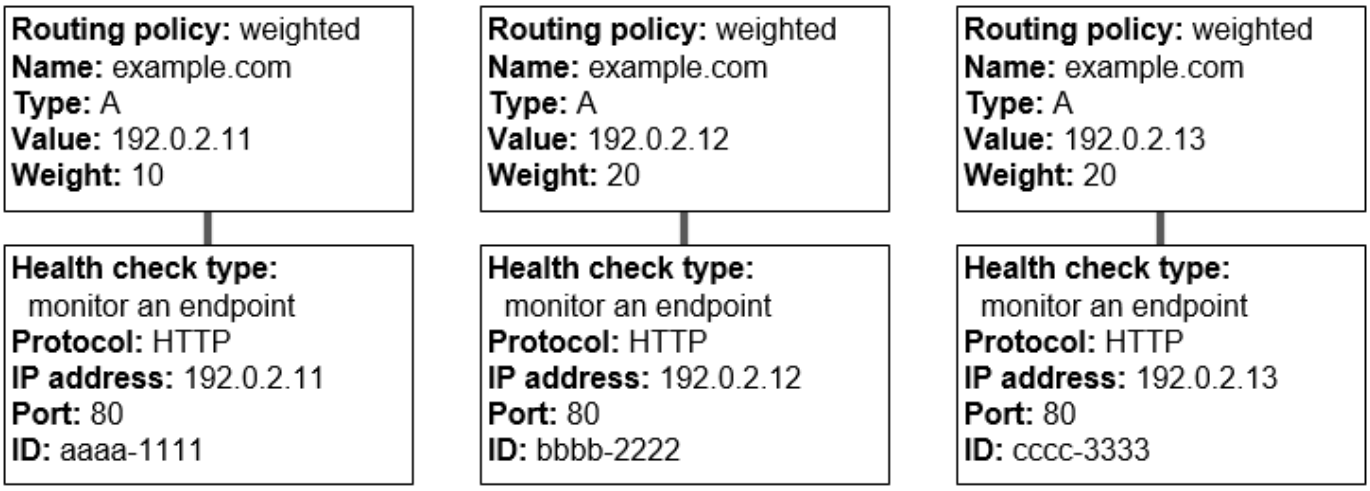
Pour plus d'informations sur la création de surveillances de l'état, consultez Création, mise à jour et suppression de surveillances de l'état.

3. Vous devrez peut-être configurer des règles de pare-feu et de routeur afin que Route 53 puisse envoyer des demandes régulières aux points de terminaison que vous avez spécifiés dans vos surveillances de l'état. Pour de plus amples informations, veuillez consulter Configuration des règles de pare-feu et de routeur pour les surveillances de l'état Amazon Route 53.
4. Vous créez un groupe d'enregistrements pour vos ressources : par exemple, un groupe d'enregistrements pondérés. Vous pouvez combiner des enregistrements avec ou sans alias, mais ils doivent toutes avoir la même valeur pour Name (Nom),Type et Routing Policy (Stratégie de routage).

   La manière dont vous configurez Route 53 pour vérifier l'état de vos ressources varie selon que vous créez des enregistrements d'alias ou des enregistrements sans alias :

- Enregistrements d'alias – Spécifiez Yes (Oui) pour Evaluate Target Health (Évaluer l'état de la cible).
- Enregistrements sans alias – Associez les surveillances de l'état que vous avez créées à l'étape 2 aux enregistrements correspondants.

Lorsque vous avez terminé, votre configuration ressemble au schéma suivant, qui comprend uniquement les enregistrements sans alias.



Pour plus d'informations sur la création de registres à l'aide de la console Route 53, consultez Création d'enregistrements à l'aide de la console Amazon Route 53.

5. Si vous créez des surveillances de l'état, Route 53 envoie périodiquement une demande au point de terminaison pour chaque surveillance de l'état ; il n'effectue pas cette vérification lorsqu'il reçoit une requête DNS. En fonction des réponses, Route 53 décide si les points de terminaison sont sains et utilise ces informations pour déterminer la manière de répondre aux requêtes. Pour de plus amples informations, veuillez consulter Comment Amazon Route 53 détermine si une surveillance de l'état est saine.

   Route 53 ne vérifie pas l'état de la ressource spécifiée dans l'enregistrement, comme l'adresse IP spécifiée dans un enregistrement A pour example.com. Lorsque vous associez une surveillance de l'état à un enregistrement, Route 53 commence à vérifier l'état du point de terminaison que vous avez spécifié dans la surveillance de l'état. Vous pouvez également configurer Route 53 pour surveiller l'état d'autres tests de santé ou surveiller les flux de données pour détecter les CloudWatch alarmes. Pour de plus amples informations, veuillez consulter Types de surveillances de l'état Amazon Route 53.

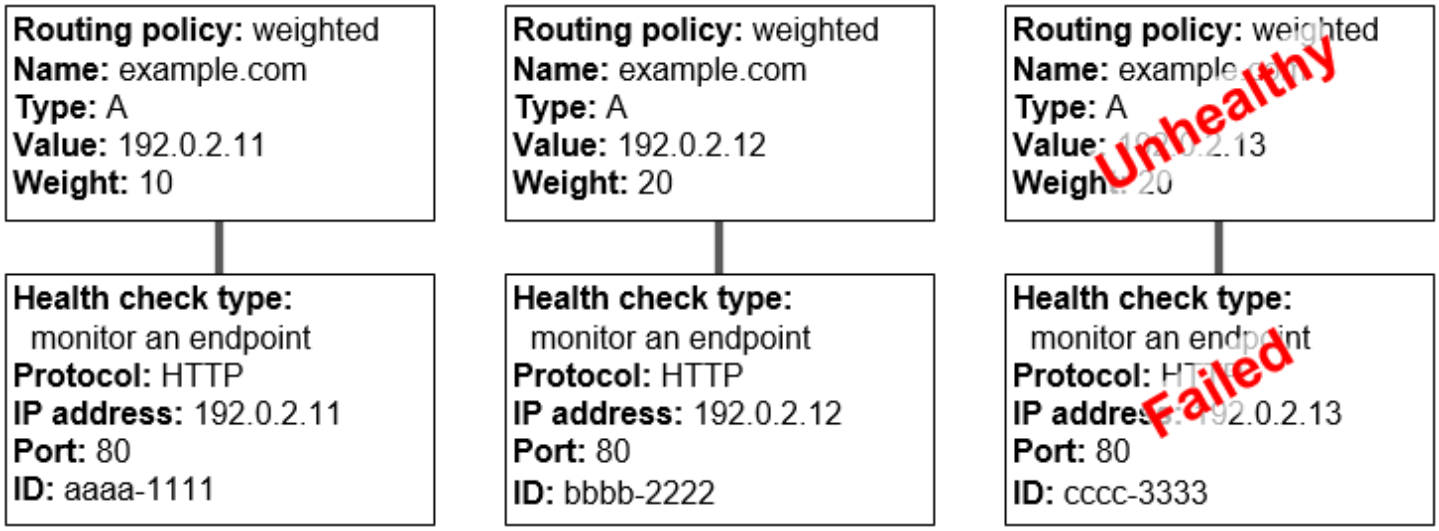
Voici ce qui se produit lorsque Route 53 reçoit une requête pour example.com :

1. Route 53 choisit un enregistrement en fonction de la stratégie de routage. Dans le cas présent, il choisit un enregistrement en fonction de la pondération.
2. Il détermine l'état actuel de l'enregistrement sélectionné à l'aide du statut de la surveillance de l'état pour cet enregistrement.
3. Si l'enregistrement sélectionné n'est pas sain, Route 53 sélectionne un autre enregistrement. Cette fois-ci, l'enregistrement non sain n'est pas pris en compte.

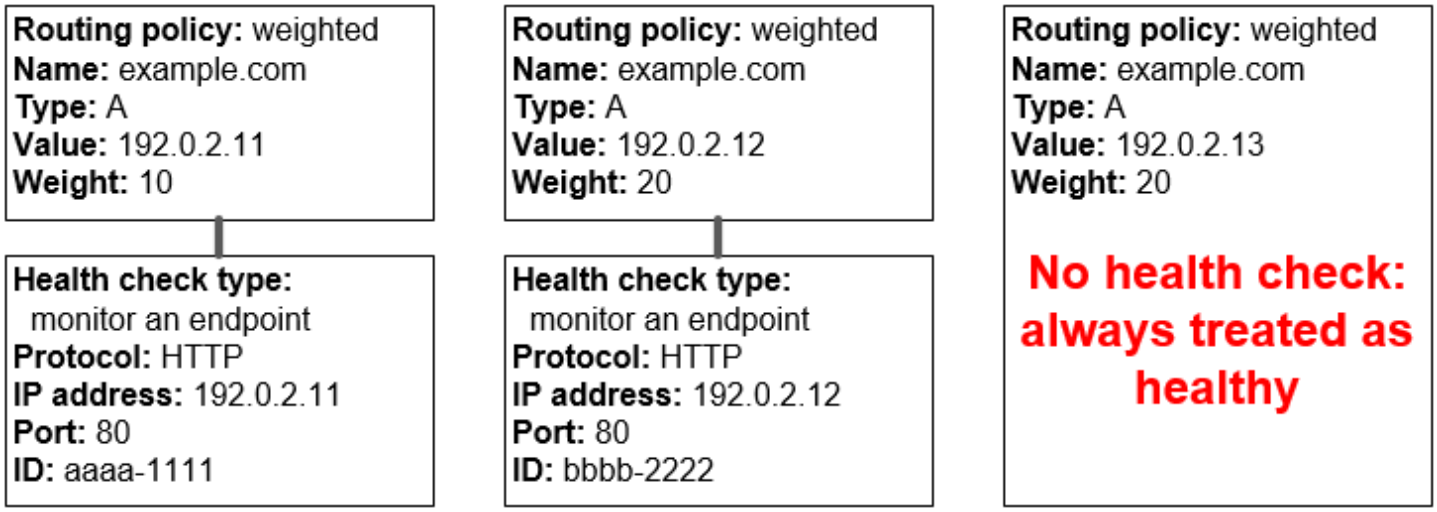
   Pour de plus amples informations, veuillez consulter Choix des enregistrements par Amazon Route 53 lorsque la surveillance de l'état est configurée.
4. Quand Route 53 trouve un enregistrement sain, il répond à la requête avec la valeur applicable, telle que l'adresse IP d'un enregistrement A.

L'exemple suivant montre un groupe d'enregistrements pondérés dans lequel le troisième enregistrement n'est pas sain. Initialement, Route 53 sélectionne un enregistrement en fonction des pondérations des trois enregistrements. Si l'enregistrement non sain est sélectionné en premier, Route 53 sélectionne un enregistrement, en faisant cette fois-ci abstraction de la pondération du troisième enregistrement dans le calcul :

- Lorsque Route 53 sélectionne initialement l'un des trois enregistrements, il répond aux requêtes à l'aide du premier enregistrement environ 20 % du temps, 10/(10 + 20 + 20).
- Lorsque Route 53 détermine que le troisième enregistrement n'est pas sain, il répond aux requêtes à l'aide du premier enregistrement environ 33 % du temps, 10/(10 + 20).



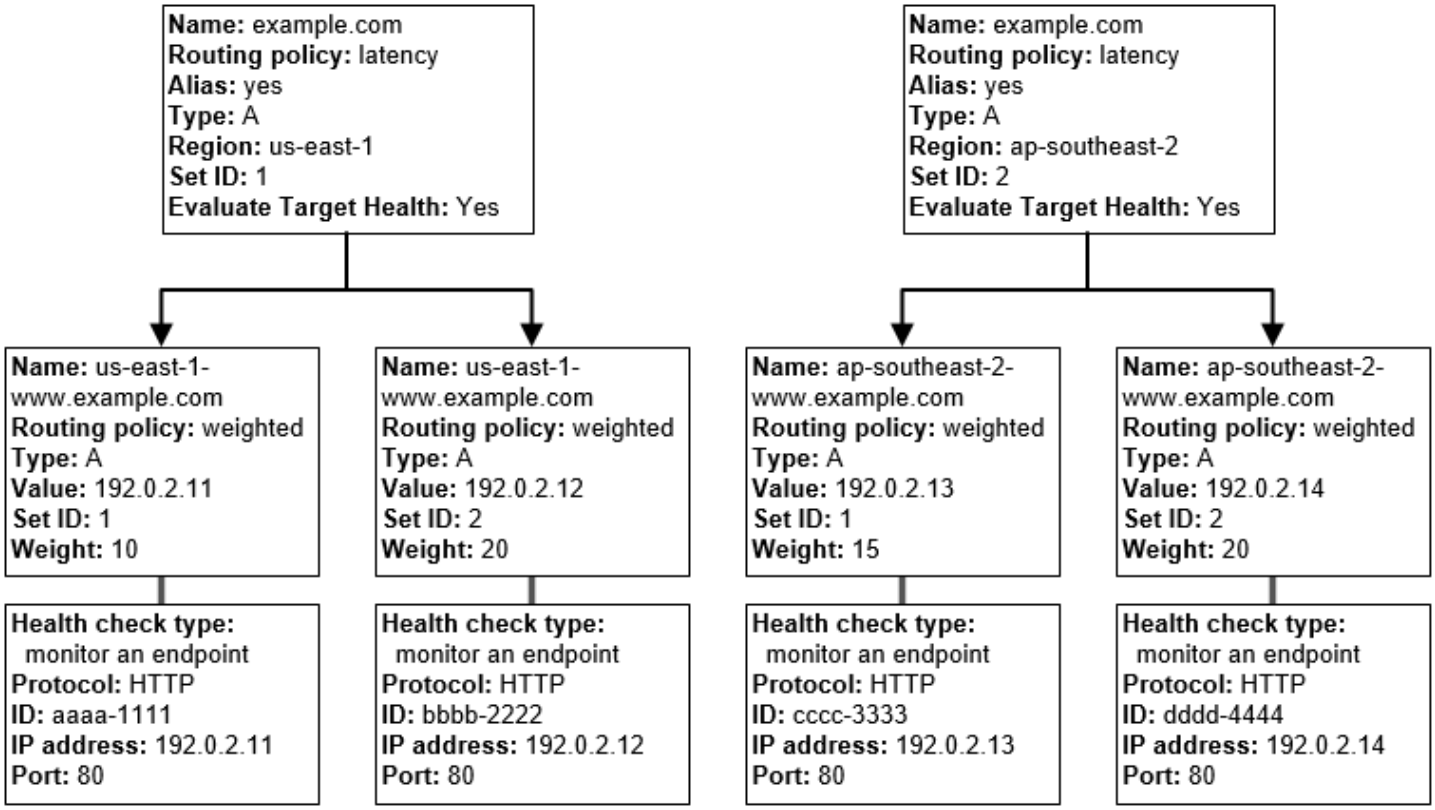
Si vous omettez une surveillance de l'état d'un ou de plusieurs enregistrements d'un groupe d'enregistrements, Route 53 n'a aucun moyen de déterminer l'état de la ressource correspondante. Route 53 traite ces enregistrements comme sains.



Fonctionnement des surveillances de l'état dans les configurations Amazon Route 53 complexes

La vérification de l'état des ressources dans les configurations complexes fonctionne de la même façon que dans les configurations simples. Cependant, dans les configurations complexes, vous utilisez une combinaison d'enregistrements d'alias (par exemple des alias pondérés et des alias de basculement) et d'enregistrements sans alias pour créer un arbre de décision qui vous permet de mieux contrôler la façon dont Route 53 répond aux demandes.

Par exemple, vous pouvez utiliser des enregistrements d'alias de latence pour sélectionner une région à proximité d'un utilisateur et utiliser des enregistrements pondérés pour au moins deux ressources dans chaque région afin d'assurer une protection contre la défaillance d'un point de terminaison unique ou d'une zone de disponibilité. Le schéma suivant illustre cette configuration.



Voici comment Amazon EC2 et Route 53 sont configurés. Commençons au bas de l'arborescence, parce que c'est l'ordre dans lequel vous allez créer les enregistrements :

- Vous avez deux EC2 instances dans chacune des deux régions, us-east-1 et ap-southeast-2. Vous souhaitez que Route 53 achemine le trafic vers vos EC2 instances en fonction de leur état de santé. Vous devez donc créer un bilan de santé pour chaque instance. Vous configurez chaque surveillance de l'état pour envoyer les demandes de surveillance de l'état à l'instance correspondante sur l'adresse IP Elastic de l'instance.

  Comme Route 53 est un service global, vous ne spécifiez pas la région dans laquelle vous souhaitez créer des surveillances de l'état.
- Vous souhaitez acheminer le trafic vers les deux instances de chaque région en fonction du type d'instance et, par conséquent, vous créez un enregistrement pondéré pour chaque instance et attribuer à chaque enregistrement une pondération. (Vous pouvez modifier la pondération

ultérieurement pour acheminer plus ou moins de trafic vers une instance.) Vous associez aussi la surveillance de l'état applicable à chaque instance.

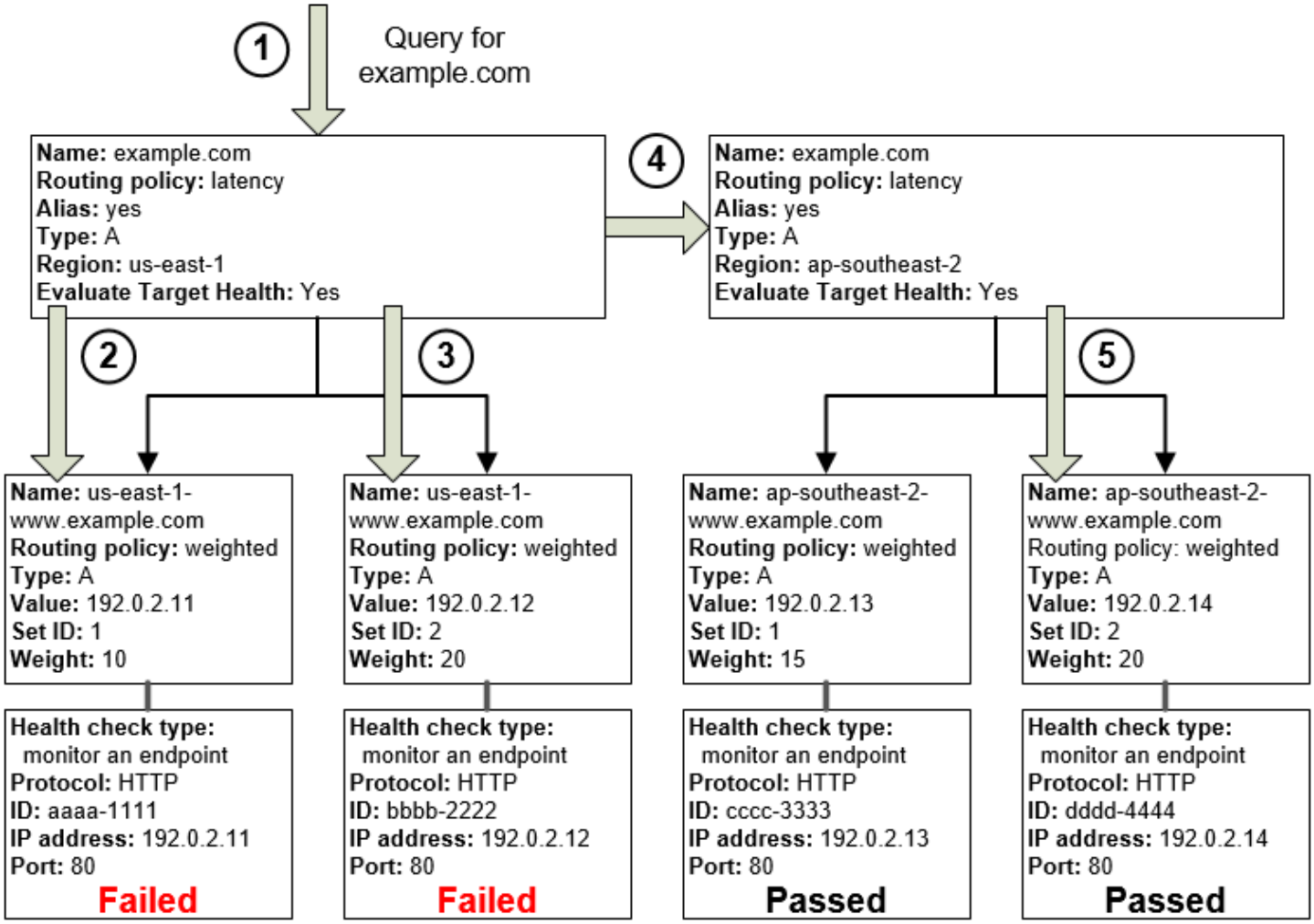
Lorsque vous créez les enregistrements, vous utilisez des noms tels que us-east-1-www.example.com. et ap-southeast-2-www.example.com. Vous attendez de parvenir en haut de l'arborescence pour donner aux enregistrements les noms que vos utilisateurs utilisent pour accéder à votre site web ou application web (example.com, par exemple).

- Comme vous souhaitez acheminer le trafic vers la région qui offre la plus faible latence pour vos utilisateurs, vous choisissez la stratégie de routage de latence pour les enregistrements en haut de l'arborescence.

  Vous souhaitez acheminer le trafic vers les enregistrements de chaque région, et non directement vers les ressources de chaque région (les enregistrements pondérés le font déjà). Par conséquent, vous créez des enregistrements d'alias de latence.

  Lorsque vous créez les enregistrements d'alias, vous leur attribuez le nom que vos utilisateurs doivent employer pour accéder à votre site web ou application web (example.com, par exemple). Les enregistrements d'alias acheminent le trafic d'example.com vers les enregistrements us-east-1-www.example.com et ap-southeast-2-www.example.com.

  Pour les deux enregistrements d'alias de latence, vous définissez la valeur de l'option Évaluer l'état de la cible sur Oui. Cela entraîne Route 53 à déterminer s'il y a des ressources saines dans une région avant d'essayer d'y acheminer le trafic. Si tel n'est pas le cas, Route 53 choisit une ressource saine dans l'autre région.



Le schéma ci-dessus illustre la séquence d'événements suivante :

1. Route 53 reçoit une requête pour example.com. En fonction de la latence pour l'utilisateur effectuant la requête, Route 53 sélectionne un enregistrement d'alias de latence pour la région us-east-1.
2. Route 53 sélectionne un enregistrement pondéré en fonction de la pondération. La valeur du paramètre Evaluate Target Health (Évaluer l'état de la cible) est Yes (Oui) pour l'enregistrement d'alias de latence. De ce fait, Route 53 vérifie l'état de l'enregistrement pondéré sélectionné.
3. La surveillance de l'état a échoué. Route 53 choisit donc un autre enregistrement pondéré en fonction de la pondération et vérifie son état. Cet enregistrement est également non sain.
4. Route 53 se retire de cette branche de l'arborescence, recherche l'enregistrement d'alias de latence offrant la deuxième meilleure latence et choisit l'enregistrement pour ap-southeast-2.

5. Route 53 sélectionne à nouveau un enregistrement en fonction de la pondération, puis vérifie l'état de la ressource sélectionnée. Comme la ressource est saine, Route 53 renvoie la valeur applicable en réponse à la requête.

Rubriques

- Que se passe-t-il lorsque vous associez une surveillance de l'état à un enregistrement d'alias ?
- Que se passe-t-il lorsque vous omettez des surveillances de l'état ?
- Que se passe-t-il lorsque vous définissez le paramètre Evaluate Target Health sur No ?

Que se passe-t-il lorsque vous associez une surveillance de l'état à un enregistrement d'alias ?

Vous pouvez associer une surveillance de l'état à un enregistrement d'alias au lieu de, ou en plus de, définir la valeur du paramètre Évaluer l'état de la cible sur Oui. Cependant, le résultat est généralement plus probant lorsque Route 53 répond aux requêtes en fonction de l'état des ressources sous-jacentes, c'est-à-dire les serveurs HTTP, les serveurs de base de données et autres ressources auxquels vos enregistrements d'alias font référence. Supposons par exemple que la configuration correspond à la configuration suivante :

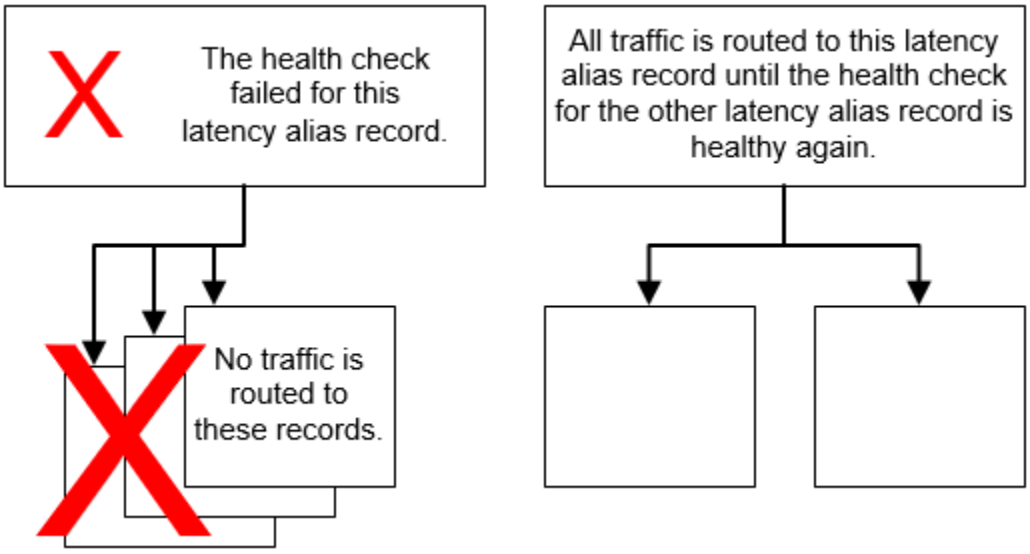
- Vous attribuez une surveillance de l'état à un enregistrement d'alias de latence pour lequel la cible de l'alias est un groupe d'enregistrements pondérés.
- Vous définissez la valeur de l'option Évaluer l'état de la cible sur Oui pour l'enregistrement d'alias de latence.

Dans cette configuration, les deux conditions suivantes doivent être remplies avant que Route 53 renvoie la valeur applicable pour un enregistrement pondéré :

- La surveillance de l'état associée à l'enregistrement d'alias de latence doit être validée.
- Au moins un enregistrement pondéré doit être considéré comme sain, soit parce qu'il est associé à une surveillance de l'état validée, soit parce qu'il n'est associé à aucune surveillance de l'état. Dans ce dernier cas, Route 53 considère toujours que l'enregistrement pondéré est sain.

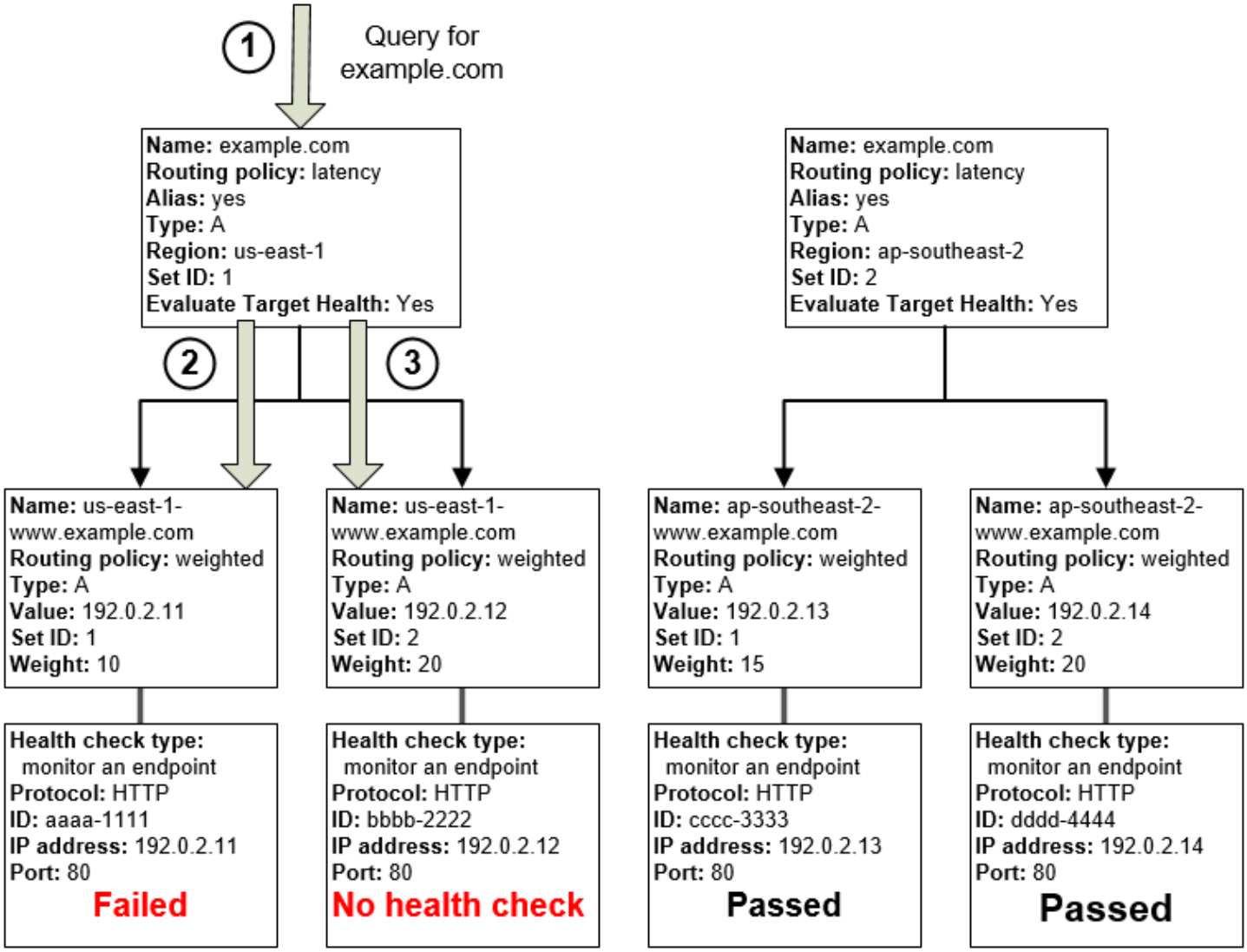
Dans l'illustration suivante, la surveillance de l'état pour l'enregistrement d'alias de latence sur la partie supérieure gauche a échoué. En conséquence, Route 53 ne répond plus aux requêtes à l'aide des enregistrements pondérés auxquels l'enregistrement d'alias de la latence se réfère s'ils sont

tous sains. Route 53 commence à prendre de nouveau en compte ces enregistrements pondérés uniquement lorsque la surveillance de l'état pour l'enregistrement d'alias de la latence redevient saine. (Pour les exceptions, consultez Choix des enregistrements par Amazon Route 53 lorsque la surveillance de l'état est configurée.)



Que se passe-t-il lorsque vous omettez des surveillances de l'état ?

Dans une configuration complexe, il est important d'associer les surveillances de l'état à tous les enregistrements sans alias. Dans l'exemple suivant, il manque une surveillance de l'état sur l'un des enregistrements pondérés de la région us-east-1.



Voici ce qui se produit si vous omettez une surveillance de l'état sur un enregistrement sans alias dans cette configuration :

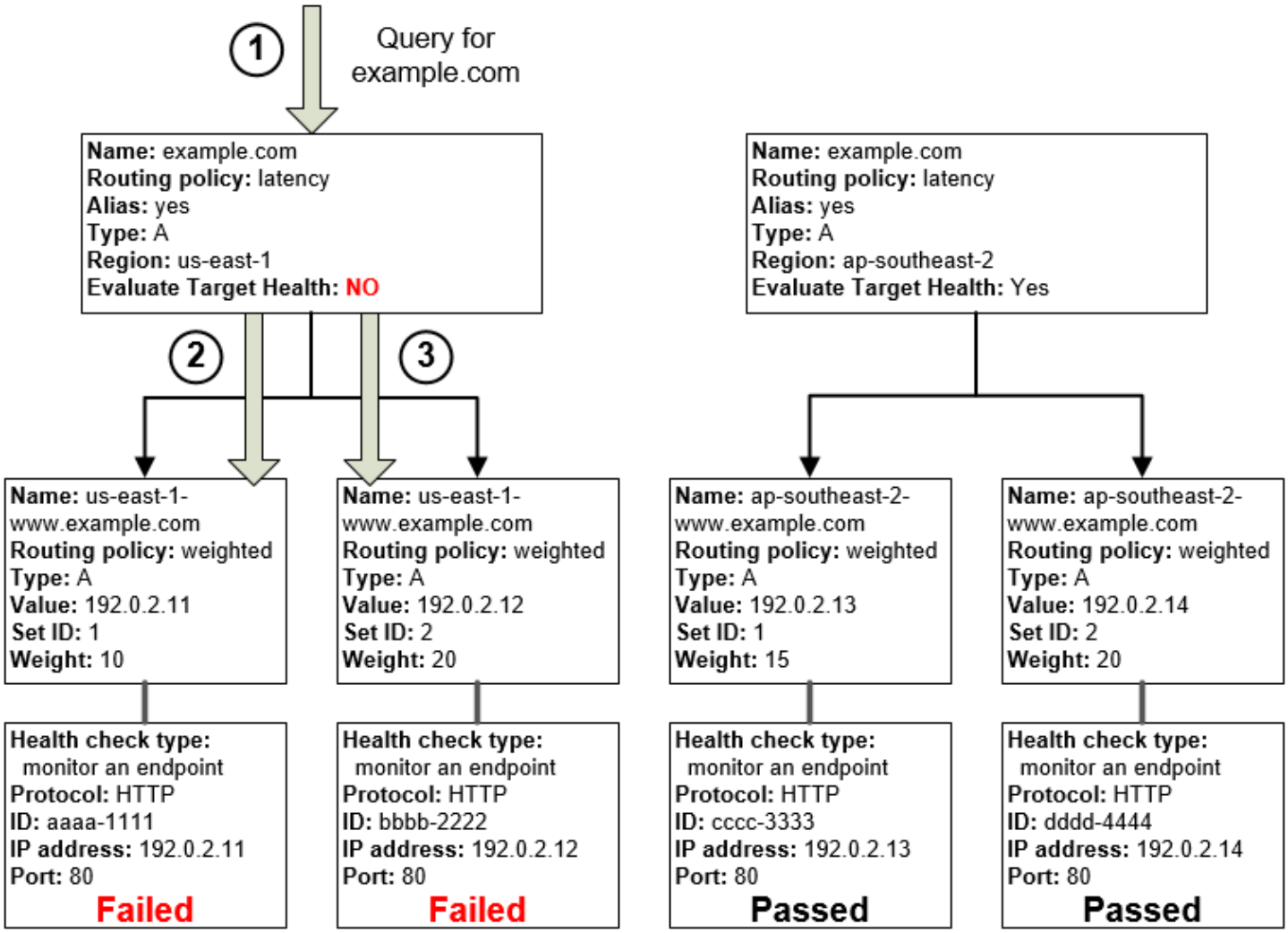
1. Route 53 reçoit une requête pour example.com. En fonction de la latence pour l'utilisateur effectuant la requête, Route 53 sélectionne un enregistrement d'alias de latence pour la région us-east-1.
2. Route 53 recherche dans la cible de l'alias l'enregistrement d'alias de latence et vérifie le statut des surveillances de l'état correspondantes. La surveillance de l'état d'un enregistrement pondéré a échoué. L'enregistrement pondéré n'est donc pas pris en compte.
3. L'autre enregistrement pondéré de la cible de l'alias pour la région us-east-1 ne comporte aucune surveillance de l'état. La ressource correspondante peut être ou ne pas être saine.

Toutefois, sans surveillance de l'état, Route 53 n'a aucun moyen de le savoir. Route 53 suppose que la ressource est saine et renvoie la valeur applicable en réponse à la requête.

Que se passe-t-il lorsque vous définissez le paramètre Evaluate Target Health sur No ?

En général, vous devez définir le paramètre Evaluate Target Health (Évaluer l'état de la cible) sur Yes (Oui) pour tous les enregistrements d'alias d'une arborescence. Si vous définissez le champ Évaluer l'état de la cible sur Non, Route 53 continue à acheminer le trafic vers les enregistrements auxquels un enregistrement d'alias fait référence, même si les surveillances de l'état pour ces enregistrements échouent.

Dans l'exemple suivant, tous les enregistrements pondérés comportent des surveillances de l'état associées, mais le paramètre Évaluer l'état de la cible est défini sur Non pour l'enregistrement d'alias de latence de la région us-east-1 :



Voici ce qui se produit lorsque vous définissez le paramètre Évaluer l'état de la cible sur Non pour un enregistrement d'alias cette configuration :

1. Route 53 reçoit une requête pour example.com. En fonction de la latence pour l'utilisateur effectuant la requête, Route 53 sélectionne un enregistrement d'alias de latence pour la région us-east-1.
2. Route 53 détermine la cible de l'alias pour l'enregistrement d'alias de latence et contrôle les surveillances de l'état correspondantes. Ils sont tous deux en échec.
3. Étant donné que la valeur du paramètre Evaluate Target Health (Évaluer l'état de la cible) est No (Non) pour l'enregistrement d'alias de latence pour la région us-east-1, Route 53 doit choisir un enregistrement dans cette branche au lieu de délaisser cette dernière et de rechercher un enregistrement sain dans la région ap-southeast-2.

Choix des enregistrements par Amazon Route 53 lorsque la surveillance de l'état est configurée

Si vous configurez la surveillance de l'état pour tous les enregistrements d'un groupe d'enregistrements ayant le même nom, le même type (par exemple, A ou AAAA), et la même stratégie de routage (par exemple, pondération ou basculement), Route 53 répond aux requêtes DNS en choisissant un enregistrement sain et en renvoyant la valeur applicable à partir de cet enregistrement.

Par exemple, supposons que vous créiez trois enregistrements A pondérés et que vous attribuiez les surveillances de l'état aux trois. Si la surveillance de l'état pour l'un des enregistrements n'est pas saine, Route 53 répond aux requêtes DNS avec l'adresse IP de l'un des deux autres enregistrements.

Voici comment Route 53 choisit un enregistrement sain :

1. Initialement, Route 53 choisit un enregistrement en fonction de la stratégie de routage et des valeurs que vous spécifiez pour chaque enregistrement. Par exemple, pour les enregistrements pondérés, Route 53 choisit un enregistrement en fonction de la pondération que vous spécifiez pour chaque enregistrement.
2. Route 53 détermine si l'enregistrement est sain :
   - Enregistrement sans alias avec surveillance de l'état associée – Si vous associez une surveillance de l'état à un enregistrement sans alias, Route 53 vérifie le statut actuel de la surveillance de l'état.

Route 53 vérifie périodiquement l'état du point de terminaison spécifié dans une surveillance de l'état. Il n'effectue pas la surveillance de l'état lorsque la requête DNS arrive.

Vous pouvez associer les surveillances de l'état à des enregistrements d'alias, mais nous vous recommandons de n'associer les surveillances de l'état qu'à des enregistrements sans alias. Pour de plus amples informations, veuillez consulter Que se passe-t-il lorsque vous associez une surveillance de l'état à un enregistrement d'alias ?.

- Enregistrement d'alias avec Evaluate Target Health (Évaluer l'état de la cible) défini sur Yes (Oui) – Route 53 vérifie l'état de santé de la ressource à laquelle l'enregistrement d'alias fait référence, par exemple un équilibreur de charge ELB ou un autre enregistrement de la même zone hébergée.

3. Si l'enregistrement est sain, Route 53 répond à la requête avec la valeur applicable, telle qu'une adresse IP.

   Si l'enregistrement n'est pas sain, Route 53 sélectionne un autre enregistrement en utilisant les mêmes critères et répète le processus jusqu'à ce qu'il trouve un enregistrement sain.

Route 53 utilise les critères suivants lors du choix d'un enregistrement :

Les enregistrements sans surveillance de l'état sont toujours sains

Si un enregistrement d'un groupe d'enregistrements ayant les mêmes nom et type ne dispose pas de surveillance de l'état associée, Route 53 le considère toujours comme sain et l'inclut toujours dans les réponses possibles à une requête.

Si aucun enregistrement n'est sain, tous les enregistrements sont sains

Si aucun enregistrement d'un groupe d'enregistrements n'est sain, Route 53 doit renvoyer une réponse aux requêtes DNS, mais il ne dispose d'aucune référence pour choisir un enregistrement plutôt qu'un autre. Dans ce cas, Route 53 considère que tous les enregistrements du groupe sont sains et en sélectionne un en fonction de la stratégie de routage et des valeurs que vous spécifiez pour chaque enregistrement.

Enregistrements pondérés ayant une pondération de 0

Si vous ajoutez les surveillances de l'état à tous les enregistrements d'un groupe d'enregistrements pondérés, mais que vous attribuez des pondérations différentes de zéro à certains enregistrements et des pondérations égales à zéro pour d'autres, les surveillances de

l'état fonctionnent de la même manière que lorsque tous les enregistrements ont des pondérations différentes de zéro, avec les exceptions suivantes :

- Initialement, Route 53 prend uniquement en compte les enregistrements pondérés dont la pondération est différente de zéro, s'il y en a.
- Si tous les enregistrements ayant une pondération supérieure à 0 ne sont pas sains, Route 53 prend en compte les enregistrements dont la pondération est égale à zéro.

Dans la mesure où Route 53 prendra en compte les enregistrements à pondération nulle dans certaines circonstances, il est important de s'assurer que la cible à pondération nulle possède également une réponse viable à une requête DNS.

Pour plus d'informations sur les enregistrements pondérés, consultez la section Surveillance de l'état et routage pondéré.

Enregistrements d'alias

Vous pouvez également configurer la surveillance de l'état pour les enregistrements d'alias en définissant le champ Évaluer l'état de la cible sur Oui pour chaque enregistrement d'alias. Cela entraîne Route 53 à évaluer l'état de la ressource vers laquelle l'enregistrement achemine le trafic : un équilibreur de charge ELB ou un autre enregistrement de la même zone hébergée, par exemple.

Supposons, par exemple, que la cible de l'alias pour un enregistrement d'alias soit un groupe de d'enregistrements pondérés ayant tous des pondérations différentes de zéro :

- Aussi longtemps qu'un de ces enregistrements pondérés est sain, Route 53 considère que l'enregistrement d'alias de latence est sain.
- Si aucun des enregistrements pondérés n'est sain, Route 53 considère que l'enregistrement d'alias n'est pas sain.
- Route 53 arrête de prendre en compte les enregistrements de cette branche de l'arborescence jusqu'à ce qu'au moins un enregistrement pondéré redevienne sain.

Pour de plus amples informations, veuillez consulter Fonctionnement des surveillances de l'état dans les configurations Amazon Route 53 complexes.

Enregistrements de basculement

Les enregistrements de basculement fonctionnent généralement de la même manière que les autres types de routage. Vous créez des surveillances de l'état et les associez à des

enregistrements sans alias, et vous définissez le champ Évaluer l'état de la cible sur Oui pour les enregistrements d'alias. Remarques :

- Les deux enregistrements (principal et secondaire) peuvent être un enregistrement sans alias ou un enregistrement d'alias.
- Si vous associez des surveillances de l'état à l'enregistrement de basculement principal et à l'enregistrement de basculement secondaire, voici comment Route 53 répond aux requêtes :
  - Si Route 53 considère que l'enregistrement principal est sain (si l'état du point de terminaison de la surveillance de l'état est sain), Route 53 renvoie uniquement l'enregistrement principal en réponse à une requête DNS.
  - Si Route 53 considère que l'enregistrement principal n'est pas sain et que l'enregistrement secondaire est sain, Route 53 renvoie l'enregistrement secondaire à la place.
  - Si Route 53 considère que les deux enregistrements (principal et secondaire) ne sont pas sains, Route 53 renvoie l'enregistrement principal.
- Lorsque vous configurez l'enregistrement secondaire, l'ajout d'une surveillance de l'état est facultatif. Si vous ignorez la surveillance de l'état pour l'enregistrement secondaire, et si le point de terminaison de la surveillance de l'état pour l'enregistrement principal n'est pas sain, Route 53 répond toujours aux requêtes DNS à l'aide de l'enregistrement secondaire. C'est le cas même si l'enregistrement secondaire n'est pas sain.

Pour plus d’informations, consultez les rubriques suivantes :

- Configuration du basculement actif-passif à l'aide d'une ressource principale et d'une ressource secondaire
- Configuration du basculement actif-passif à l'aide de plusieurs ressources principales et secondaires

Basculement actif-actif et actif-passif

Vous pouvez utiliser la surveillance de l'état de Route 53 pour définir les configurations de basculement actif-actif et actif-passif. Vous configurez le basculement actif-actif à l'aide d'une stratégie de routage (ou d'une combinaison de stratégies de routage) autre que le basculement, et vous configurez le basculement actif-passif à l'aide de la stratégie de routage de basculement.

Rubriques

- Basculement actif-actif
- Basculement actif-passif

Basculement actif-actif

Utilisez cette configuration de basculement lorsque vous souhaitez que toutes vos ressources soient disponibles la plupart du temps. Lorsqu'une ressource devient indisponible, Route 53 peut détecter qu'elle n'est pas saine et arrêter de l'inclure pour répondre à des requêtes.

Dans un basculement actif-actif, tous les enregistrements qui ont le même nom, le même type (par exemple, A ou AAAA), et la même stratégie de routage (par exemple, pondération ou latence) sont actives, sauf si Route 53 les considère comme non sains. Route 53 peut répondre à une requête DNS à l'aide de n'importe quel enregistrement sain.

Basculement actif-passif

Utilisez une configuration de basculement actif-passif lorsque vous souhaitez qu'une ressource ou un groupe de ressources principal(e) soit disponible la plupart du temps et que vous souhaitez qu'une ressource ou un groupe de ressources secondaire soit mis(e) en attente, au cas où toutes les ressources primaires deviendraient indisponibles. Lorsque Route 53 répond aux requêtes, seules les ressources principales saines sont incluses. Si aucune ressource principale n'est saine, Route 53 inclut uniquement les ressources secondaires saines en réponse aux requêtes DNS.

Rubriques

- Configuration du basculement actif-passif à l'aide d'une ressource principale et d'une ressource secondaire
- Configuration du basculement actif-passif à l'aide de plusieurs ressources principales et secondaires
- Configuration du basculement actif-passif avec des enregistrements pondérés

Configuration du basculement actif-passif à l'aide d'une ressource principale et d'une ressource secondaire

Pour créer une configuration de basculement actif-passif avec un enregistrement principal et un enregistrement secondaire, vous créez simplement les enregistrements et spécifiez Failover (Basculement) pour la stratégie de routage. Lorsque la ressource principale est saine, Route 53 répond aux requêtes DNS à l'aide de l'enregistrement principal. Lorsque la ressource principale n'est pas saine, Route 53 répond aux requêtes DNS à l'aide de l'enregistrement secondaire.

Configuration du basculement actif-passif à l'aide de plusieurs ressources principales et secondaires

Vous pouvez également associer plusieurs ressources à l'enregistrement principal, à l'enregistrement secondaire, ou aux deux. Dans cette configuration, Route 53 considère l'enregistrement de basculement principal comme sain aussi longtemps qu'au moins l'une des ressources associées est saine. Pour de plus amples informations, veuillez consulter Choix des enregistrements par Amazon Route 53 lorsque la surveillance de l'état est configurée.

Pour configurer le basculement actif-passif avec plusieurs ressources pour l'enregistrement principal ou secondaire, exécutez les tâches suivantes.

1. Créez un bilan de santé pour chaque ressource vers laquelle vous souhaitez acheminer le trafic, telle qu'une EC2 instance ou un serveur Web dans votre centre de données.

   > **Note**
   >
   > Si vous acheminez le trafic vers des AWS ressources pour lesquelles vous pouvez créer des enregistrements d'alias, ne créez pas de bilans de santé pour ces ressources. Lorsque vous créez les enregistrements d'alias, vous définissez à la place le champ Evaluate Target Health (Évaluer l'état de la cible) sur Yes (Oui).

   Pour de plus amples informations, veuillez consulter Création et mise à jour de surveillances de l'état.
2. Créez des enregistrements pour vos ressources principales et spécifiez les valeurs suivantes :
   - Attribuez à chaque enregistrement les mêmes nom, type et stratégie de routage. Par exemple, vous pouvez créer trois enregistrements A pondérés qui se nomment tous failover-primary.example.com.
   - Si vous utilisez AWS des ressources pour lesquelles vous pouvez créer des enregistrements d'alias, spécifiez Oui pour Evaluate Target Health.

     Si vous utilisez des ressources pour lesquelles vous ne pouvez pas créer des enregistrements d'alias, associez la surveillance de l'état applicable de l'étape 1 à chaque enregistrement.

   Pour de plus amples informations, veuillez consulter Création d'enregistrements à l'aide de la console Amazon Route 53.
3. Créez des enregistrements pour vos ressources secondaires, le cas échéant, et spécifiez les valeurs suivantes :

- Attribuez à chaque enregistrement les mêmes nom, type et stratégie de routage. Par exemple, vous pouvez créer trois enregistrements A pondérés qui se nomment tous failover-secondary.example.com.
- Si vous utilisez AWS des ressources pour lesquelles vous pouvez créer des enregistrements d'alias, spécifiez Oui pour Evaluate Target Health.

  Si vous utilisez des ressources pour lesquelles vous ne pouvez pas créer des enregistrements d'alias, associez la surveillance de l'état applicable de l'étape 1 à chaque enregistrement.

> **Note**
>
> Certains clients utilisent un serveur web en tant que ressource principale et un compartiment Amazon S3 configuré en tant que point de terminaison de site web comme ressource secondaire. Le compartiment S3 contient un simple message « temporairement indisponible ». Si vous utilisez cette configuration, vous pouvez ignorer cette étape et juste créer un enregistrement d'alias de basculement pour la ressource secondaire à l'étape 4.

4. Créez deux enregistrements d'alias de basculement, un principal et un secondaire, et spécifiez les valeurs suivantes :

   Enregistrement principal

   - Name (Nom) – Spécifiez le nom de domaine (example.com) ou le nom de sous-domaine (www.example.com) pour lequel vous voulez que Route 53 achemine le trafic.
   - Alias – Spécifiez Yes (Oui).
   - Alias Target (Cible d'alias) – Spécifiez le nom des enregistrements que vous avez créés à l'étape 2.
   - Routing Policy (Stratégie de routage) – Spécifiez Failover (Basculement).
   - Failover Record Type (Type d'enregistrement de basculement) – Spécifiez Primary (Principal).
   - Evaluate Target Health (Évaluer l'état de la cible) – Spécifiez Yes (Oui).
   - Associer à la surveillance de l'état – Spécifiez Non.

   Enregistrement secondaire

   - Name (Nom) – Spécifiez le même nom que celui que vous avez spécifié pour l'enregistrement principal.
   - Alias – Spécifiez Yes (Oui).

- Alias Target (Cible d'alias) – Si vous avez créé des enregistrements pour votre ressource secondaire à l'étape 3, spécifiez le nom des enregistrements. Si vous utilisez un compartiment Amazon S3 pour la ressource secondaire, spécifiez le nom DNS du point de terminaison de site web.
- Routing Policy (Stratégie de routage) – Spécifiez Failover (Basculement).
- Failover Record Type (Type d'enregistrement de basculement) – Spécifiez Secondary (Secondaire).
- Evaluate Target Health (Évaluer l'état de la cible) – Spécifiez Yes (Oui).
- Associer à la surveillance de l'état – Spécifiez Non.

Configuration du basculement actif-passif avec des enregistrements pondérés

Vous pouvez également utiliser les enregistrements pondérés pour le basculement actif-passif, avec des avertissements. Si vous spécifiez des pondérations différentes de zéro pour certains enregistrements et des pondérations égales à zéro pour d'autres enregistrements, Route 53 répond aux requêtes DNS en utilisant uniquement les enregistrements sains qui ont des pondérations différentes de zéro. Si aucun enregistrement ayant une pondération supérieure à 0 n'est sain, Route 53 répond aux requêtes en utilisant les enregistrements dont la pondération est égale à zéro.

> **Note**
>
> Tous les enregistrements avec des pondérations différentes de zéro doivent être non sains avant que Route 53 ne commence à répondre aux requêtes DNS à l'aide des enregistrements ayant des pondérations égales à zéro. Cela peut rendre votre application web ou site web peu fiable si la dernière ressource saine, telle qu'un serveur web, ne peut pas gérer l'ensemble du trafic lorsque les autres ressources sont indisponibles.

Configuration du basculement dans une zone hébergée privée

Si vous créez des enregistrements de basculement dans une zone hébergée privée, notez ce qui suit :

- Les outils de surveillance de l'état Route 53 sont en dehors du VPC. Pour vérifier l'état d'un point de terminaison au sein d'un VPC par adresse IP, vous devez affecter une adresse IP publique à l'instance dans le VPC.

- Vous pouvez créer une CloudWatch métrique, associer une alarme à la métrique, puis créer un bilan de santé basé sur le flux de données de l'alarme. Par exemple, vous pouvez créer une CloudWatch métrique qui vérifie l'état de la EC2 `StatusCheckFailed` métrique, ajouter une alarme à la métrique, puis créer un bilan de santé basé sur le flux de données de l'alarme afin de vérifier les instances d'un Virtual Private Cloud (VPC) qui ne possèdent que des adresses IP privées. Pour plus d'informations sur la création de CloudWatch métriques et d'alarmes à l'aide de la CloudWatch console, consultez le guide de CloudWatch l'utilisateur Amazon.

Pour plus d'informations, consultez Utilisation des zones hébergées privées et Surveillance des bilans de santé à l'aide CloudWatch.

Prévention des problèmes de basculement par Amazon Route 53

Les algorithmes de basculement implémentés par Route 53 sont conçus non seulement pour acheminer le trafic vers des points de terminaison sains, mais également pour éviter des scénarios pires provoqués par des applications et des surveillances de l'état mal configurées, des surcharges de point de terminaison et des défaillances de partition.

Rubriques

- Prévention des défaillances en cascades par Amazon Route 53
- Gestion des partitions Internet par Amazon Route 53

Prévention des défaillances en cascades par Amazon Route 53

La première défense contre les défaillances en cascade est le mode de dernier recours dont dispose chaque algorithme de routage de demande (par exemple pondéré et basculement). Dans ce mode spécial, lorsque tous les enregistrements sont considérés comme non sains, l'algorithme Route 53 permet de considérer à nouveau que tous les enregistrements sont sains.

Par exemple, si toutes les instances d'une application, sur plusieurs hôtes, rejettent les demandes de surveillance de l'état, les serveurs DNS Route 53 choisissent une réponse quand même et la renvoient, au lieu de ne renvoyer aucune réponse DNS ou d'envoyer une réponse NXDOMAIN (domaine inexistant). Une application peut répondre aux utilisateurs, mais cependant ne pas réussir les surveillances de l'état. Il s'agit d'une protection contre une configuration défaillante.

De même, si une application est surchargée, et si les surveillances de l'état échouent pour l'un des trois points de terminaison et qu'il est donc exclu des réponses DNS Route 53, Route 53 distribue les

demandes aux deux points de terminaison restants. Si les points de terminaison restants ne sont pas en mesure de gérer la charge supplémentaire et s'ils échouent, Route 53 recommence à répartir les demandes aux trois points de terminaison.

Gestion des partitions Internet par Amazon Route 53

Bien que rares, il existe parfois des partitions Internet qui peuvent être importantes, ce qui signifie que de grandes régions géographiques ne peuvent pas communiquer entre elles via Internet. Au cours de ces partitions, les sites Route 53 peuvent parvenir à des conclusions différentes quant à l'état de santé d'un terminal et peuvent différer de l'état signalé à CloudWatch. Les vérificateurs de santé de la Route 53 de chaque AWS région envoient en permanence le statut des bilans de santé à tous les sites de la Route 53. Au cours des partitions Internet, il est possible que chaque emplacement Route 53 puisse avoir accès à seulement une partie de ces statuts, généralement des régions les plus proches.

Par exemple, pendant une partition Internet qui affecte la connectivité vers et depuis l'Amérique du Sud, les serveurs DNS Route 53 de l'emplacement Amérique du Sud (Sao Paulo) Route 53 peuvent avoir un accès correct aux points de terminaison de la surveillance de l'état dans la région AWS Amérique du Sud (Sao Paulo), mais un accès médiocre aux autres points de terminaison. En même temps, Route 53 de la région USA Est (Ohio) peut avoir un accès médiocre aux points de terminaison de la surveillance de l'état de la région Amérique du Sud (Sao Paulo) et en conclure que les enregistrements correspondant ne sont pas sains.

De telles partitions peuvent donner lieu à des situations où les emplacements Route 53 aboutissent à des conclusions différentes sur l'état de points de terminaison, en fonction de la visibilité locale qu'ils ont sur ces points de terminaison. C'est pour cette raison que chaque emplacement Route 53 considère qu'un point de terminaison est sain lorsque seulement une partie des outils de surveillance de l'état accessibles le considèrent sain.

Attribution de noms et balisage des surveillances de l'état

Vous pouvez ajouter des balises aux surveillances de l'état Amazon Route 53, ce qui vous permet d'attribuer à chaque surveillance de l'état un nom plus explicite que l'ID de la surveillance de l'état. Ce sont les mêmes étiquettes qui AWS Billing and Cost Management permettent d'organiser votre AWS facture. Pour en savoir plus sur l'utilisation des balises pour la répartition des coûts, consultez Utilisation des balises de répartition des coûts pour les rapports de facturation personnalisés dans le Guide de l'utilisateur AWS Billing .

Chaque balise se compose d'une clé (le nom de la balise) et d'une valeur que vous définissez. Lorsque vous ajoutez des balises à une surveillance de l'état, nous vous recommandons d'ajouter une balise qui a les valeurs suivantes pour la clé et la valeur :

- key (Clé) – Name (Nom)
- value (Valeur) – Nom que vous voulez attribuer à la surveillance de l'état

La valeur de la balise Nom s'affiche dans la liste des surveillances de l'état de la console Route 53, ce qui vous permet de distinguer rapidement les surveillances de l'état les unes des autres. Pour voir d'autres balises d'une surveillance de l'état, vous choisissez la surveillance de l'état, puis l'onglet Tags.

Pour plus d'informations sur les balises, consultez les rubriques suivantes :

- Pour ajouter, modifier ou supprimer les balises Nom lorsque vous ajoutez ou modifiez des surveillances de l'état dans la console Route 53, consultez Création et mise à jour de surveillances de l'état.
- Pour obtenir un aperçu du balisage des ressources Route 53, consultez Balisage des ressources Amazon Route 53.

Restrictions liées aux étiquettes

Les restrictions de base suivantes s’appliquent aux balises :

- Nombre maximum de balises par ressource : 50 sur la nouvelle console et 10 sur l'ancienne console.
- Longueur de Key (Clé) maximale – 128 caractères Unicode.
- Longueur de Value (Valeur) maximale – 256 caractères Unicode.
- Valeurs valides pour Key (Clé) et Value (Valeur) – Lettres majuscules et minuscules UTF-8, nombres, espace et les caractères suivants : _ . : / = + - et @
- Les clés et valeurs de balise sont sensibles à la casse
- N'utilisez pas le `aws:` préfixe pour les clés ou les valeurs ; il est réservé à l'usage AWS

Ajout, modification et suppression de balises pour les surveillances de l'état

Les procédures suivantes vous montrent comment utiliser les balises pour vos surveillances de l'état dans la console Route 53.

> **Note**
>
> Nous mettons à jour la console de vérification de l'état de santé de Route 53. Pendant la période de transition, vous pouvez continuer à utiliser l'ancienne console.

Choisissez l'onglet correspondant à la console que vous utilisez.

- Nouvelle console
- Ancienne console

New console

Pour ajouter des balises aux bilans de santé

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation, choisissez Health checks.
3. Sélectionnez l'ID associé au bilan de santé pour lequel vous souhaitez ajouter des balises.
4. Sur la page inférieure, choisissez l'onglet Balises, puis sélectionnez Gérer, puis Ajouter de nouvelles balises.
5. Entrez le nom de la balise dans le champ Clé, puis entrez une valeur dans le champ Valeur.
6. Choisissez Enregistrer.

Pour modifier les balises pour les bilans de santé

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation, choisissez Health checks.
3. Sélectionnez l'identifiant associé à un bilan de santé.

4. Dans le volet inférieur, choisissez l'onglet Tags, puis sélectionnez Gérer.
5. Vous pouvez désormais modifier et ajouter d'autres balises.
6. Choisissez Enregistrer.

Pour supprimer des balises pour les bilans de santé

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation, choisissez Health checks.
3. Sélectionnez l'identifiant associé à un bilan de santé.
4. Dans le volet inférieur, choisissez l'onglet Tags, puis sélectionnez Gérer.
5. Choisissez Supprimer à côté du tag que vous souhaitez supprimer.
6. Choisissez Enregistrer.

Old console

Pour ajouter des balises aux bilans de santé

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation, sélectionnez Health Checks.
3. Sélectionnez une surveillance de l'état, ou plusieurs surveillances de l'état si vous souhaitez leur ajouter la même balise.
4. Dans le volet inférieur, sélectionnez l'onglet Tags, puis Add/Edit Tags.
5. Dans la boîte de dialogue Add/Edit Tags, entrez le nom de la balise dans le champ Key et entrez une valeur dans le champ Value.
6. Choisissez Apply changes.

Pour modifier les balises pour les bilans de santé

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation, sélectionnez Health Checks.
3. Sélectionnez une surveillance de l'état.

Si vous sélectionnez plusieurs surveillances de l'état qui partagent la même balise, vous ne pouvez pas modifier simultanément la valeur de toutes les balises. Veuillez noter cependant que vous pouvez modifier la valeur d'une balise qui s'affiche dans plusieurs surveillances de l'état si vous sélectionnez des surveillances de l'état comportant la balise et au moins une qui ne la comporte pas.

Par exemple, supposons que vous sélectionnez plusieurs surveillances de l'état qui ont une balise Centre de coûts et une qui n'en a pas. Vous choisissez la possibilité d'ajouter une balise, et vous spécifiez Cost Center (Centre de coûts) pour la clé et 777 pour la valeur. Pour les surveillances de l'état sélectionnées qui ont déjà une balise Centre de coûts, Route 53 modifie la valeur pour 777. Pour la seule surveillance de l'état qui n'a pas de balise Centre de coûts, Route 53 en ajoute une et définit la valeur à 777.

4. Dans le volet inférieur, sélectionnez l'onglet Tags, puis Add/Edit Tags.
5. Dans la boîte de dialogue Add/Edit Tags, modifiez la valeur.
6. Choisissez Enregistrer.

Pour supprimer des balises pour les bilans de santé

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation, sélectionnez Health Checks.
3. Sélectionnez une surveillance de l'état, ou plusieurs si vous souhaitez supprimer la même balise de plusieurs vérifications.
4. Dans le volet inférieur, sélectionnez l'onglet Tags, puis Add/Edit Tags.
5. Dans la boîte de dialogue Ajouter/Modifier des balises, choisissez la balise à *X* côté de la balise que vous souhaitez supprimer.
6. Choisissez Enregistrer.

Utilisation des surveillances de l'état avec les versions de l'API Amazon Route 53 antérieures à la version 2012-12-12

Les surveillances de l'état sont prises en charge à compter de la version 2012-12-12 de l'API Amazon Route 53. Si une zone hébergée contient des enregistrements pour lesquels les surveillances de l'état sont configurées, nous vous recommandons d'utiliser uniquement l'API

version 2012-12-12 ou ultérieure. Notez les restrictions suivantes concernant l'utilisation des surveillances de l'état avec les versions antérieures de l'API.

- L'action `ChangeResourceRecordSets` ne permet pas de créer ni de supprimer des enregistrements qui incluent les éléments `EvaluateTargetHealth`, `Failover` ou `HealthCheckId`.
- L'action `ListResourceRecordSets` permet d'afficher des enregistrements qui incluent ces éléments, mais les éléments ne sont pas inclus dans la sortie. Au lieu de cela, l'élément `Value` de la réponse contient un message qui indique que l'enregistrement inclut un attribut non pris en charge.

Surveillance du statut de la vérification de l'état et obtention de notifications

Vous surveillez le statut de vos vérifications de l'état sur la console Amazon Route 53. Vous pouvez également définir des CloudWatch alarmes et recevoir des notifications automatiques lorsque l'état de votre bilan de santé change.

Rubriques

- Affichage du statut des vérifications de l'état et motifs des échecs de vérifications de l'état
- Surveillance de la latence entre les outils de vérification de l'état et votre point de terminaison
- Surveillance des bilans de santé à l'aide CloudWatch

Affichage du statut des vérifications de l'état et motifs des échecs de vérifications de l'état

Dans la console Route 53, vous pouvez afficher le statut (sain ou non sain) de vos vérifications de l'état effectuées par les outils de vérification de l'état Route 53. Pour toutes les vérifications de l'état, excepté pour celles de type « calculées », vous pouvez aussi afficher le motif du dernier échec. Par exemple, les outils de vérification de l'état n'ont pas pu établir de connexion avec le point de terminaison.

> **Note**
>
> Nous mettons à jour la console de vérification de l'état de santé de Route 53. Pendant la période de transition, vous pouvez continuer à utiliser l'ancienne console.

Choisissez l'onglet correspondant à la console que vous utilisez.

- Nouvelle console
- Ancienne console

New console

Pour consulter l'état et le motif du dernier échec d'un bilan de santé

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation, choisissez Health checks.
3. Pour bénéficier d'un aperçu du statut de toutes vos vérifications de l'état (saines ou non saines), consultez la colonne Status (Statut). Pour de plus amples informations, veuillez consulter Comment Amazon Route 53 détermine si une surveillance de l'état est saine.
4. Pour toutes les vérifications de l'état, à l'exception de celles de type « calculées », le statut des outils de vérification de l'état Route 53 vérifiant l'état d'un point de terminaison spécifié est disponible.
5. Choisissez l'identifiant associé au bilan de santé dont vous souhaitez consulter les détails.
6. Dans le volet inférieur, choisissez l'onglet Health checkers.

> **Note**
>
> Les nouvelles vérifications de l'état doivent se propager aux outils de vérification de l'état Route 53 avant que le statut et le motif d'échec s'affichent dans la colonne Status (Statut). Tant que la propagation n'est pas terminée, le message de cette colonne indique qu'aucun statut n'est disponible.

7. Le tableau inclut les valeurs suivantes :

   IP de l'outil de vérification de l'état

   Adresse IP de l'outil de vérification de l'état Route 53 qui a effectué cette vérification.

   Dernière vérification

   La date et l'heure du bilan de santé ou la date et l'heure du dernier échec.

   Statut

   Soit l'état actuel du bilan de santé, soit la raison de l'échec du dernier bilan de santé.

Old console

Pour consulter l'état et le motif du dernier échec d'un bilan de santé

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation, sélectionnez Health Checks.
3. Pour bénéficier d'un aperçu du statut de toutes vos vérifications de l'état (saines ou non saines), consultez la colonne Status (Statut). Pour de plus amples informations, veuillez consulter Comment Amazon Route 53 détermine si une surveillance de l'état est saine.
4. Pour toutes les vérifications de l'état, à l'exception de celles de type « calculées », le statut des outils de vérification de l'état Route 53 vérifiant l'état d'un point de terminaison spécifié est disponible. Sélectionnez la vérification de l'état.
5. Dans le volet inférieur, choisissez l'onglet Health Checkers.

   > **Note**
   >
   > Les nouvelles vérifications de l'état doivent se propager aux outils de vérification de l'état Route 53 avant que le statut et le motif d'échec s'affichent dans la colonne Status (Statut). Tant que la propagation n'est pas terminée, le message de cette colonne indique qu'aucun statut n'est disponible.

6. Indiquez si vous souhaitez afficher le statut actuel de la vérification de l'état, ou la date et l'heure du dernier échec, ainsi que son motif. La table de l'onglet Statut comprend les valeurs suivantes :

   IP de l'outil de vérification de l'état

   Adresse IP de l'outil de vérification de l'état Route 53 qui a effectué cette vérification.

   Dernière vérification

   Date et heure de la vérification de l'état ou date et heure du dernier échec, en fonction de l'option sélectionnée en haut de l'onglet Status.

   Statut

   Statut actuel de la vérification de l'état ou motif du dernier échec, en fonction de l'option sélectionnée en haut de l'onglet Status.

Surveillance de la latence entre les outils de vérification de l'état et votre point de terminaison

Lorsque vous créez un bilan de santé, si vous choisissez de surveiller l'état d'un point de terminaison (et non l'état des autres bilans de santé) et que vous choisissez l'option Graphiques de latence, vous pouvez afficher les valeurs suivantes sur les CloudWatch graphiques de la console Route 53 :

- Le temps moyen, en millisecondes, qui a été nécessaire aux outils de vérification de l'état Route 53 pour établir une connexion TCP avec le point de terminaison
- Le temps moyen, en millisecondes, qui a été nécessaire aux outils de vérification de l'état Route 53 pour recevoir le premier octet de la réponse à une demande HTTP ou HTTPS
- Le temps moyen, en millisecondes, qui a été nécessaire aux outils de vérification de l'état Route 53 pour établir la liaison SSL/TLS

> **Note**
>
> Vous ne pouvez pas activer la surveillance de la latence pour des vérifications de l'état existantes.

> **Important**
>
> Les outils de vérification de l'état sont exécutés sur 16 zones de disponibilité redondantes. Parfois, une zone de disponibilité peut être indisponible en raison de déploiements, de mises à jour, de maintenances, etc. Le système de vérification de l'état de santé est conçu afin de tenir compte de ces indisponibilités sans pour autant affecter le client.

> **Note**
>
> Nous mettons à jour la console de vérification de l'état de santé de Route 53. Pendant la période de transition, vous pouvez continuer à utiliser l'ancienne console.

Choisissez l'onglet correspondant à la console que vous utilisez.

- Nouvelle console
- Ancienne console

New console

Pour afficher le temps de latence entre les vérificateurs de santé Route 53 et votre terminal

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation, choisissez Health checks.
3. Sélectionnez l'identifiant associé au bilan de santé dont vous souhaitez consulter les statistiques. Vous pouvez uniquement afficher les données de latence pour les vérifications de l'état qui surveillent le statut d'un point de terminaison et pour lesquelles l'option Latency graphs est activée.
4. Dans le volet inférieur, choisissez l'onglet Metrics.
5. Sélectionnez la plage de temps et la région géographique pour laquelle vous souhaitez afficher les graphiques de latence.

   Les graphiques affichent le statut de la plage de durée spécifiée :

   TCP connection time (HTTP et TCP uniquement)

   Le temps moyen, en millisecondes, qui a été nécessaire aux outils de vérification de l'état Route 53 de la région géographique sélectionnée pour établir une connexion TCP avec le point de terminaison.

   Time to first byte (HTTP et HTTPS uniquement)

   Le temps moyen, en millisecondes, qui a été nécessaire aux outils de vérification de l'état Route 53 de la région géographique sélectionnée pour recevoir le premier octet de la réponse à une demande HTTP ou HTTPS.

   Time to complete SSL handshake (HTTPS uniquement)

   Le temps moyen, en millisecondes, qui a été nécessaire aux outils de vérification de l'état Route 53 de la région géographique sélectionnée pour établir la liaison SSL/TLS.
6. Pour afficher un graphique plus grand et définir différents paramètres, choisissez les trois points en haut à droite du graphique. Vous pouvez modifier les paramètres suivants :

Statistique

Modifie le calcul CloudWatch effectué sur les données.

Plage de temps

Affiche le statut d'une vérification de l'état sur une période différente, par exemple, pendant la nuit ou la semaine précédente.

Période

Modifie l'intervalle entre les points de données sur le graphique.

Remarques :

- Si vous venez de créer une vérification de l'état, vous devrez peut-être attendre quelques minutes pour que les données apparaissent sur le graphique et pour que les métriques de vérification de l'état apparaissent dans la liste des métriques disponibles.
- Le graphique n'est pas actualisé automatiquement. Pour mettre à jour l'affichage, cliquez sur l'icône ( ).
- En cas d'échec des vérifications de l'état pour une raison quelconque, par exemple un délai d'inactivité des connexions, Route 53 ne peut pas mesurer la latence, et les données de latence ne figureront pas sur le graphique pour la période concernée.

Old console

Pour afficher le temps de latence entre les vérificateurs de santé Route 53 et votre terminal

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation, sélectionnez Health Checks.
3. Sélectionnez les lignes pour les vérifications concernées. Vous pouvez uniquement afficher les données de latence pour les vérifications de l'état qui surveillent le statut d'un point de terminaison et pour lesquelles l'option Latency graphs est activée.
4. Dans le volet inférieur, choisissez l'onglet Latency.

5. Sélectionnez la plage de temps et la région géographique pour laquelle vous souhaitez afficher les graphiques de latence.

   Les graphiques affichent le statut de la plage de durée spécifiée :

   TCP connection time (HTTP et TCP uniquement)

   Le temps moyen, en millisecondes, qui a été nécessaire aux outils de vérification de l'état Route 53 de la région géographique sélectionnée pour établir une connexion TCP avec le point de terminaison.

   Time to first byte (HTTP et HTTPS uniquement)

   Le temps moyen, en millisecondes, qui a été nécessaire aux outils de vérification de l'état Route 53 de la région géographique sélectionnée pour recevoir le premier octet de la réponse à une demande HTTP ou HTTPS.

   Time to complete SSL handshake (HTTPS uniquement)

   Le temps moyen, en millisecondes, qui a été nécessaire aux outils de vérification de l'état Route 53 de la région géographique sélectionnée pour établir la liaison SSL/TLS.

   > **Note**
   >
   > Si vous sélectionnez plusieurs vérifications de l'état, le graphique affiche une ligne de couleur distincte pour chacune.

6. Pour afficher un graphique plus grand et spécifier d'autres paramètres, cliquez sur le graphique. Vous pouvez modifier les paramètres suivants :

   Statistique

   Modifie le calcul CloudWatch effectué sur les données.

   Plage de temps

   Affiche le statut d'une vérification de l'état sur une période différente, par exemple, pendant la nuit ou la semaine précédente.

   Période

   Modifie l'intervalle entre les points de données sur le graphique.

Remarques :

- Si vous venez de créer une vérification de l'état, vous devrez peut-être attendre quelques minutes pour que les données apparaissent sur le graphique et pour que les métriques de vérification de l'état apparaissent dans la liste des métriques disponibles.
- Le graphique n'est pas actualisé automatiquement. Pour mettre à jour l'affichage, cliquez sur l'icône
  ( ).
- En cas d'échec des vérifications de l'état pour une raison quelconque, par exemple un délai d'inactivité des connexions, Route 53 ne peut pas mesurer la latence, et les données de latence ne figureront pas sur le graphique pour la période concernée.

Surveillance des bilans de santé à l'aide CloudWatch

Les bilans de santé de Route 53 s'intègrent aux CloudWatch métriques afin que vous puissiez effectuer les opérations suivantes :

- Vérifier qu'une surveillance de l'état est correctement configurée.
- Passer en revue le statut d'une vérification de l'état sur une période de temps donnée.
- Configurez CloudWatch pour envoyer une alerte Amazon SNS lorsque l'état d'un bilan de santé n'est pas satisfaisant. Notez que plusieurs minutes peuvent s'écouler entre l'échec d'une vérification de l'état et le moment où vous recevez la notification SNS associée.

Pour de plus amples informations, veuillez consulter Comment Amazon Route 53 détermine si une surveillance de l'état est saine.

Rubriques

- Afficher l'état de votre bilan de santé
- Afficher les alarmes de contrôle de santé
- Afficher les statistiques de contrôle de santé sur la CloudWatch console
- Créez une alarme avec une notification SNS

Afficher l'état de votre bilan de santé

> **Note**
>
> Nous mettons à jour la console de vérification de l'état de santé de Route 53. Pendant la période de transition, vous pouvez continuer à utiliser l'ancienne console.

Choisissez l'onglet correspondant à la console que vous utilisez.

- Nouvelle console
- Ancienne console

New console

Pour consulter l'état d'un bilan de santé

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation, choisissez Health checks.
3. Choisissez l'ID associé au bilan de santé dont vous souhaitez consulter les statistiques.
4. Dans le volet inférieur, choisissez l'onglet Metrics.

   Les deux graphiques affichent le statut de la dernière heure à intervalles d'une minute :

   Statut de la surveillance de l’état

   Le graphique illustre l'évaluation Route 53 de l'état du point de terminaison.1 indique que le point de terminaison est sain, et 0 qu'il est non sain.

   Vérifications de l’état rapportant le niveau de santé du point de terminaison (%)

   Pour les vérifications de l'état qui surveillent uniquement un point de terminaison, le graphique affiche le pourcentage d'outils de vérification de l'état Route 53 qui considèrent que le point de terminaison sélectionné est sain.

   Lorsqu'une vérification de l'état est désactivée, cette métrique n'est pas disponible.

Number of healthy child health checks

Pour les vérifications de l'état calculées uniquement, le graphique affiche le nombre de vérifications de l'état enfant pour lesquelles l'état est sain.

5. Pour afficher un graphique plus grand et définir différents paramètres, choisissez les trois points en haut à droite, puis Agrandir. Vous pouvez modifier les paramètres suivants :

   Statistique

   Modifie le calcul CloudWatch effectué sur les données.

   Plage de temps

   Affiche le statut d'une vérification de l'état sur une période différente, par exemple, pendant la nuit ou la semaine précédente.

   Période

   Modifie l'intervalle entre les points de données sur le graphique.

   Remarques :

   - Si vous venez de créer une vérification de l'état, vous devrez peut-être attendre quelques minutes pour que les données apparaissent sur le graphique et pour que les métriques de vérification de l'état apparaissent dans la liste des métriques disponibles.
   - Le graphique n'est pas actualisé automatiquement. Pour mettre à jour l'affichage, cliquez sur l'icône ( ).

Old console

Pour consulter l'état d'un bilan de santé (nouvelle console)

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation, sélectionnez Health Checks.
3. Choisissez les lignes pour les vérifications concernées.
4. Dans le volet inférieur, choisissez l'onglet Monitoring.

Les deux graphiques affichent le statut de la dernière heure à intervalles d'une minute :

Statut de la surveillance de l’état

Le graphique illustre l'évaluation Route 53 de l'état du point de terminaison.1 indique que le point de terminaison est sain, et 0 qu'il est non sain.

Vérifications de l’état rapportant le niveau de santé du point de terminaison (%)

Pour les vérifications de l'état qui surveillent uniquement un point de terminaison, le graphique affiche le pourcentage d'outils de vérification de l'état Route 53 qui considèrent que le point de terminaison sélectionné est sain.

Lorsqu'une vérification de l'état est désactivée, cette métrique n'est pas disponible.

Number of healthy child health checks

Pour les vérifications de l'état calculées uniquement, le graphique affiche le nombre de vérifications de l'état enfant pour lesquelles l'état est sain.

> **Note**
>
> Si vous avez sélectionné plusieurs vérifications de l'état, le graphique affiche une ligne de couleur distincte pour chacune.

5. Pour afficher un graphique plus grand et spécifier d'autres paramètres, cliquez sur le graphique. Vous pouvez modifier les paramètres suivants :

   Statistique

   Modifie le calcul CloudWatch effectué sur les données.

   Plage de temps

   Affiche le statut d'une vérification de l'état sur une période différente, par exemple, pendant la nuit ou la semaine précédente.

   Période

   Modifie l'intervalle entre les points de données sur le graphique.

Remarques :

- Si vous venez de créer une vérification de l'état, vous devrez peut-être attendre quelques minutes pour que les données apparaissent sur le graphique et pour que les métriques de vérification de l'état apparaissent dans la liste des métriques disponibles.
- Le graphique n'est pas actualisé automatiquement. Pour mettre à jour l'affichage, cliquez sur l'icône
  ( ).

Afficher les alarmes de contrôle de santé

> **Note**
>
> Nous mettons à jour la console de vérification de l'état de santé de Route 53. Pendant la période de transition, vous pouvez continuer à utiliser l'ancienne console.

Choisissez l'onglet correspondant à la console que vous utilisez.

- Nouvelle console
- Ancienne console

New console

Pour consulter l'état des CloudWatch alarmes et modifier les alarmes pour Amazon Route 53

1. Dans le volet de navigation de la console Route 53, choisissez Health checks.
2. Choisissez l'ID associé du bilan de santé pour lequel vous souhaitez consulter les alarmes.
3. Sur la page de détails, au bas de la page, choisissez l'onglet Alarmes.

   La liste des alarmes contient toutes les alarmes Route 53 que vous avez créées pour le bilan de santé sélectionné.

   La colonne State affiche le statut actuel de chaque alarme :

OK

CloudWatch a accumulé suffisamment de statistiques à partir des bilans de santé de Route 53 pour déterminer que le terminal n'atteint pas le seuil d'alarme.

DONNÉES INSUFFISANTES

CloudWatch n'a pas accumulé suffisamment de statistiques pour déterminer si le terminal atteint le seuil d'alarme. Ce statut est le statut initial d'une nouvelle alarme. L'état de l'alarme passe également à DONNÉES INSUFFISANTES si CloudWatch les métriques ne sont plus disponibles ou si vous supprimez le bilan de santé sans supprimer l'alarme associée.

ALARME

CloudWatch a accumulé suffisamment de statistiques à partir des bilans de santé de Route 53 pour déterminer que le terminal atteint le seuil d'alarme et pour envoyer une notification à l'adresse e-mail spécifiée.

4. Pour afficher une alarme dans la CloudWatch console, qui fournit des informations plus détaillées sur l'alarme (par exemple, un historique des mises à jour de l'alarme et des changements de statut), choisissez le nom associé à l'alarme. Vous pouvez également modifier l'alarme sur la CloudWatch console.
5. Pour créer une nouvelle CloudWatch alarme sur la CloudWatch console, choisissez Créer une CloudWatch alarme. Pour plus d'informations, voir Rechercher et créer des alarmes recommandées dans le guide de CloudWatch l'utilisateur.

Old console

Pour consulter l'état des CloudWatch alarmes et modifier les alarmes pour Amazon Route 53

1. Dans le panneau de navigation de la console Route 53, choisissez Health Checks (Vérifications de l'état).
2. Sélectionnez la ligne d'une vérification de l'état.
3. Dans le volet des détails (après x Health Checks Selected (Vérifications de l'état sélectionnées)), choisissez l'icône du signe lambda approprié ( ).

La liste des CloudWatch alarmes contient toutes les alarmes Route 53 que vous avez créées à l'aide du AWS compte courant.

La colonne State affiche le statut actuel de chaque alarme :

OK

CloudWatch a accumulé suffisamment de statistiques à partir des bilans de santé de Route 53 pour déterminer que le terminal n'atteint pas le seuil d'alarme.

DONNÉES INSUFFISANTES

CloudWatch n'a pas accumulé suffisamment de statistiques pour déterminer si le terminal atteint le seuil d'alarme. Ce statut est le statut initial d'une nouvelle alarme. L'état de l'alarme passe également à DONNÉES INSUFFISANTES si CloudWatch les métriques ne sont plus disponibles ou si vous supprimez le bilan de santé sans supprimer l'alarme associée.

ALARME

CloudWatch a accumulé suffisamment de statistiques à partir des bilans de santé de Route 53 pour déterminer que le terminal atteint le seuil d'alarme et pour envoyer une notification à l'adresse e-mail spécifiée.

4. Pour afficher ou modifier les paramètres d'une alarme, choisissez le nom de l'alarme.
5. Pour afficher une alarme dans la CloudWatch console, qui fournit des informations plus détaillées sur l'alarme (par exemple, un historique des mises à jour de l'alarme et des changements de statut), choisissez Afficher dans la colonne Autres options de l'alarme.
6. Pour afficher toutes les CloudWatch alarmes que vous avez créées à l'aide du AWS compte actuel, y compris les alarmes relatives à d'autres AWS services, choisissez Afficher toutes les CloudWatch alarmes.
7. Pour afficher tous les CloudWatch indicateurs disponibles, y compris les indicateurs qui ne sont pas actuellement utilisés par le AWS compte actuel, choisissez Afficher tous les CloudWatch indicateurs.

Afficher les statistiques de contrôle de santé sur la CloudWatch console

Pour afficher les métriques de Route 53 sur la CloudWatch console

1. Connectez-vous à la CloudWatch console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Modifiez la région actuelle sur USA Est (Virginie du Nord). Les métriques Route 53 ne sont pas disponibles si vous sélectionnez une autre région que la région actuelle.
3. Dans le panneau de navigation, sélectionnez Metrics (Métriques).
4. Sous l'onglet Toutes les métriques, choisissez Route 53.
5. Choisissez Health Check Metrics (Métriques de surveillance d'état).
6. Vous pouvez également configurer les notifications SNS sur la CloudWatch console. Pour plus d'informations, consultez la section Création d'alarmes recommandées dans le guide de CloudWatch l'utilisateur.

Créez une alarme avec une notification SNS

> **Note**
>
> La procédure suivante s'applique uniquement à l'ancienne console. La nouvelle console vous dirige vers la CloudWatch console pour créer des alarmes. Pour plus d'informations, voir Rechercher et créer des alarmes recommandées dans le guide de CloudWatch l'utilisateur.

Pour recevoir une notification Amazon SNS lorsque l'état d'un bilan de santé n'est pas satisfaisant (ancienne console)

1. Dans le panneau de navigation de la console Route 53, choisissez Health Checks (Vérifications de l'état).
2. Choisissez la ligne pour la vérification concernée.
3. Dans le volet inférieur, choisissez l'onglet Alarms.

   Le tableau répertorie les alarmes que vous avez déjà créées pour cette vérification de l'état.
4. Sélectionnez Create Alarm (Créer une alerte).
5. Indiquez l’une des valeurs suivantes :

Nom de l'alarme

Entrez le nom que Route 53 doit afficher dans la colonne Name (Nom) de l'onglet Alarms (Alarmes).

Description de l'alarme

(Facultatif) Entrez une description de l'alarme. Cette valeur apparaît dans la CloudWatch console.

Send notification

Choisissez si vous souhaitez que Route 53 vous envoie une notification si le statut de cette vérification de l'état déclenche une alarme.

Notification target (uniquement lorsque la valeur de « Send notification » est « Yes »)

Si vous souhaitez CloudWatch envoyer une notification à une rubrique SNS existante, choisissez-la dans la liste.

Si vous souhaitez CloudWatch envoyer une notification mais pas à une rubrique SNS existante, effectuez l'une des opérations suivantes :

- Si vous souhaitez CloudWatch envoyer une notification par e-mail, choisissez une nouvelle rubrique SNS et poursuivez cette procédure.
- Si vous souhaitez CloudWatch envoyer une notification par une autre méthode, ouvrez un nouvel onglet de navigateur, accédez à la console Amazon SNS et créez le nouveau sujet. Revenez ensuite à la console Route 53, choisissez le nom de la nouvelle rubrique dans la liste Notification target (Cible de notification) et poursuivez cette procédure.

Nom de la rubrique (uniquement lorsque vous choisissez de créer une nouvelle rubrique Amazon SNS)

Saisissez le nom de la nouvelle rubrique Amazon SNS.

Adresses e-mail des destinataires (uniquement lorsque vous choisissez de créer une nouvelle rubrique Amazon SNS)

Entrez l'adresse e-mail à laquelle vous voulez que Route 53 envoie une notification SNS quand une vérification de l'état déclenche une alarme.

Cible d'alarme

Sélectionnez la valeur que vous voulez que Route 53 évalue pour cette vérification de l'état :

- Health check status (Statut de vérification de l'état) – Les outils de vérification de l'état Route 53 indiquent si la vérification est saine ou non saine
- Health checkers that report the endpoint healthy (%) (Outils de vérification de l'état qui indiquent que le point de terminaison est sain (%) (vérifications de l'état qui surveillent uniquement un point de terminaison) – Le pourcentage des outils de vérification de l'état Route 53 indiquant que le statut de la vérification est sain
- Number of healthy child health checks (Nombre de vérifications de l'état enfants saines) (vérifications de l'état calculées uniquement) – Le nombre de vérifications de l'état enfants d'une vérification de l'état calculée indiquant que le statut de cette vérification est sain
- TCP connection time (Temps de connexion TCP) (vérifications de l'état HTTP et TCP uniquement) – Le temps, en millisecondes, qui a été nécessaire aux outils de vérification de l'état Route 53 pour établir une connexion TCP avec le point de terminaison
- Time to complete SSL handshake (Temps pour établir la liaison SSL) (vérifications de l'état HTTPS uniquement) – Le temps, en millisecondes, qui a été nécessaire aux outils de vérification de l'état Route 53 pour établir la liaison SSL/TLS
- Time to first byte (Délai jusqu'au premier octet) (vérifications de l'état HTTP et HTTPS uniquement) – Le temps, en millisecondes, qui a été nécessaire aux outils de vérification de l'état Route 53 pour recevoir le premier octet de la réponse à une demande HTTP ou HTTPS

Cible d'alarme

Pour les cibles d'alarme basées sur la latence (temps de connexion TCP, délai nécessaire pour terminer la prise de contact SSL, temps écoulé jusqu'au premier octet), choisissez si vous souhaitez CloudWatch calculer la latence pour les vérificateurs de santé Route 53 dans une région spécifique ou pour toutes les régions (mondial).

Notez que si vous sélectionnez une région, Route 53 mesure la latence seulement deux fois par minute, et le nombre de tests sera moins important que si vous sélectionnez toutes les régions. Par conséquent, les valeurs éloignées risquent d'être plus fréquentes. Pour éviter les notifications d'alarme intempestives, nous vous recommandons de spécifier un plus grand nombre de périodes consécutives d'échec de la vérification de l'état avant l'envoi d'une notification par CloudWatch .

Remplir une condition

Utilisez les paramètres suivants pour déterminer à quel moment une alarme CloudWatch doit être déclenchée.

Cible d'alarme	Condition recommandée	Description
Statut de la surveillance de l'état	Minimum < 1	Les outils de vérification de l'état Route 53 signalent qu'un point de terminaison n'est pas sain.
Vérifications de l'état rapportant le niveau de santé du point de terminaison (%)	Moyenne < pourcentage souhaité	Vérifications de l'état qui surveillent uniquement un point de terminaison – Route 53 considère que le statut d'une vérification de l'état n'est pas sain lorsque moins de 18 % des outils de vérification de l'état indiquent que le statut est sain. Ne choisissez pas Sample Count (Nombre d'échantillons) pour cette métrique, car la plage du nombre d'échantillons peut changer au fur et à mesure que Route 53 ajoute d'autres régions pour la vérification de l'état. La valeur Moyenne représentera toujours avec précision le pourcentage d'outils de vérification de l'état qui indiquent le statut d'une vérification de l'état.
Number of healthy child health checks	Minimum nombre souhaité de vérifications de l'état enfant saines	La statistique Minimum renvoie la valeur la plus prudente et représente le pire cas.
TCP connection time	Average > temps souhaité en millisecondes	Average est une valeur plus constante que les autres statistiques.
Time to complete SSL handshake	Average > temps souhaité en millisecondes	Average est une valeur plus constante que les autres statistiques.

Cible d'alarme	Condition recommandée	Description
Time to first byte	Average > temps souhaité en millisecondes	Average est une valeur plus constante que les autres statistiques.

Pendant au moins des périodes ***x*** consécutives de ***y*** minutes/hours/day

Spécifiez combien de fois à la suite la valeur spécifiée doit satisfaire au critère avant que Route 53 n'envoie une notification. Spécifiez ensuite la longueur de la période.

6. Lorsque vous choisissez Create (Créer), Amazon SNS vous envoie un e-mail avec les informations relatives à la nouvelle rubrique SNS.
7. Dans l'e-mail, choisissez Confirm subscription (Confirmer l'abonnement). Vous devez confirmer votre abonnement pour commencer à recevoir CloudWatch des notifications.

Utilisation du pare-feu DNS pour filtrer le trafic DNS sortant

Avec Route 53 Resolver DNS Firewall, vous pouvez filtrer et réguler le trafic DNS sortant pour votre cloud privé virtuel (VPC). Pour ce faire, créez des collections réutilisables de règles de filtrage dans les groupes de règles de pare-feu DNS, associez les groupes de règles à votre VPC, puis contrôlez l'activité dans les journaux et les métriques du pare-feu DNS. En fonction de l'activité, vous pouvez ajuster le comportement du pare-feu DNS en conséquence.

Le pare-feu DNS protège les requêtes DNS sortantes provenant de votre VPCs. Ces demandes sont acheminées via Resolver pour la résolution des noms de domaine. Une utilisation principale des protections de pare-feu DNS consiste à empêcher l'exfiltration DNS de vos données. L'exfiltration DNS peut se produire lorsqu'un acteur malveillant compromet une instance d'application dans votre VPC, puis utilise la recherche DNS pour extraire des données du VPC et les envoyer vers un domaine qu'il contrôle. Avec le pare-feu DNS, vous pouvez surveiller et contrôler les domaines que vos applications peuvent interroger. Vous pouvez refuser l'accès aux domaines malveillants et autoriser le passage de toutes les autres requêtes. Vous pouvez également refuser l'accès à tous les domaines, sauf ceux que vous approuvez explicitement.

Vous pouvez également utiliser le pare-feu DNS pour bloquer les demandes de résolution aux ressources dans des zones hébergées privées (partagées ou locales), y compris les noms de points de terminaison de VPC. Il peut également bloquer les demandes de noms d' EC2 instances Amazon publics ou privés.

Le pare-feu DNS est une fonction de Route 53 Resolver et ne nécessite aucune configuration supplémentaire de Resolver.

AWS Firewall Manager prend en charge le pare-feu DNS

Vous pouvez utiliser Firewall Manager pour configurer et gérer de manière centralisée vos associations de groupes de règles de pare-feu DNS pour VPCs l'ensemble de vos comptes dans AWS Organizations. Firewall Manager ajoute automatiquement les associations VPCs qui entrent dans le champ d'application de votre politique de pare-feu DNS Firewall Manager. Pour plus d'informations, consultez AWS Firewall Managerle AWS WAF AWS Firewall Manager, et le Guide AWS Shield Advanced du développeur.

Comment fonctionne le pare-feu DNS avec AWS Network Firewall

Le pare-feu DNS et Network Firewall offrent tous deux le filtrage des noms de domaine, mais pour différents types de trafic. En utilisant à la fois le pare-feu DNS et Network Firewall, vous pouvez

configurer le filtrage basé sur le domaine pour le trafic de la couche d'application sur deux chemins réseau différents.

- Le pare-feu DNS permet de filtrer les requêtes DNS sortantes qui transitent par le résolveur Route 53 à partir d'applications internes à votre compte. VPCs Vous pouvez également configurer le pare-feu DNS pour envoyer des réponses personnalisées pour les requêtes adressées à des noms de domaine bloqués.
- Network Firewall fournit un filtrage pour le trafic de la couche réseau et d'application, mais n'a pas de visibilité sur les requêtes effectuées par Route 53 Resolver.

Pour plus d'informations sur Network Firewall, consultez le Guide du développeur Network Firewall.

Fonctionnement de Route 53 Resolver DNS Firewall

Route 53 Resolver DNS Firewall vous permet de contrôler l'accès aux sites et de bloquer les menaces au niveau DNS pour les requêtes DNS sortant de votre VPC via Route 53 Resolver. Avec le pare-feu DNS, vous définissez les règles de filtrage des noms de domaine dans les groupes de règles que vous associez à votre VPCs. Vous pouvez spécifier des listes de noms de domaine à autoriser ou à bloquer, ou des règles avancées du pare-feu DNS Route 53 Resolver qui offrent une protection contre le tunneling DNS et les menaces basées sur l'algorithme de génération de domaines (DGA). Vous pouvez personnaliser les réponses aux requêtes DNS que vous bloquez. Pour les règles contenant une liste de domaines, vous pouvez également affiner la règle pour autoriser certains types de requêtes, tels que les enregistrements MX, à passer.

Le pare-feu DNS filtre uniquement sur le nom de domaine. Il ne résout pas ce nom en une adresse IP à bloquer. En outre, le pare-feu DNS filtre le trafic DNS, mais il ne filtre pas les autres protocoles de couche application, tels que HTTPS, SSH, TLS, FTP, etc.

Composants et paramètres de Route 53 Resolver DNS Firewall

Vous gérez le pare-feu DNS avec les composants et paramètres centraux suivants.

Groupe de règles de pare-feu DNS

Définit un ensemble nommé et réutilisable de règles de pare-feu DNS pour filtrer les requêtes DNS. Vous renseignez le groupe de règles avec les règles de filtrage, puis vous associez le groupe de règles à une ou plusieurs VPCs d'entre elles. Lorsque vous associez un groupe de règles à un VPC, vous activez le filtrage du pare-feu DNS pour le VPC. Ensuite,

lorsque le résolveur reçoit une requête DNS pour un VPC auquel un groupe de règles est associé, le résolveur transmet la requête au pare-feu DNS pour filtrage.

Si vous associez plusieurs groupes de règles à un seul VPC, vous indiquez leur ordre de traitement via le paramètre de priorité de chaque association. Le pare-feu DNS traite les groupes de règles pour un VPC en commençant par le paramètre de priorité numérique le plus bas.

Pour de plus amples informations, veuillez consulter Règles et groupes de règles de pare-feu DNS.

Règles de pare-feu DNS

Définit une règle de filtrage pour les requêtes DNS dans un groupe de règles de pare-feu DNS. Chaque règle spécifie une liste de domaines, ou une protection par pare-feu DNS, et une action à effectuer sur les requêtes DNS dont les domaines correspondent aux spécifications de domaine de la règle. Vous pouvez autoriser (règles relatives aux listes de domaines uniquement), bloquer ou signaler les requêtes correspondantes. Dans les règles comportant des listes de domaines, vous pouvez également spécifier des types de requêtes pour les domaines de la liste. Par exemple, vous pouvez bloquer ou autoriser un type de requête MX pour un ou plusieurs domaines spécifiques. Vous pouvez également définir des réponses personnalisées pour les requêtes bloquées.

En ce qui concerne les règles du pare-feu DNS, vous ne pouvez bloquer ou alerter que si les requêtes correspondent.

Chaque règle d'un groupe de règles possède un paramètre de priorité qui est unique au sein du groupe de règles. Le pare-feu DNS traite les règles d'un groupe de règles en commençant par le paramètre de priorité numérique le plus bas.

Les règles de pare-feu DNS existent uniquement dans le contexte du groupe de règles dans lequel elles sont définies. Vous ne pouvez pas réutiliser une règle ou la référencer indépendamment de son groupe de règles.

Pour de plus amples informations, veuillez consulter Règles et groupes de règles de pare-feu DNS.

Domain list (Liste des domaines)

Définit un ensemble nommé et réutilisable de spécifications de domaine à utiliser dans le filtrage DNS. Chaque règle d'un groupe de règles nécessite une liste de domaines unique. Vous pouvez choisir d'indiquer les domaines auxquels vous souhaitez autoriser l'accès, les domaines

auxquels vous souhaitez refuser l'accès ou une combinaison des deux. Vous pouvez créer vos propres listes de domaines et utiliser des listes de domaines AWS gérées pour vous.

Pour de plus amples informations, veuillez consulter Listes de domaines Route 53 Resolver DNS Firewall.

Paramètre de redirection de domaines (listes de domaines uniquement)

Le paramètre de redirection de domaine vous permet de configurer une règle de pare-feu DNS pour inspecter tous les domaines de la chaîne de redirection DNS (par défaut), tels que CNAME, DNAME, etc., ou simplement le premier domaine et faire confiance au reste. Si vous choisissez d'inspecter l'intégralité de la chaîne de redirection DNS, vous devez ajouter les domaines suivants à une liste de domaines définie sur AUTORISER dans la règle. Si vous choisissez d'inspecter l'ensemble de la chaîne de redirection DNS, vous devez ajouter les domaines suivants à une liste de domaines et définir l'action que vous souhaitez que la règle exécute, soit ALLOW, BLOCK ou ALERT.

Pour de plus amples informations, veuillez consulter Paramètres de règles dans le pare-feu DNS.

Type de requête (listes de domaines uniquement)

Le paramètre du type de requête vous permet de configurer une règle de pare-feu DNS pour filtrer un type de requête DNS particulier. Si vous ne sélectionnez aucun type de requête, la règle s'applique à tous les types de requêtes DNS. Par exemple, vous souhaiterez peut-être bloquer tous les types de requêtes pour un domaine particulier, mais autoriser les enregistrements MX.

Pour de plus amples informations, veuillez consulter Paramètres de règles dans le pare-feu DNS.

Protection avancée du pare-feu DNS

Détecte les requêtes DNS suspectes en fonction des signatures de menaces connues dans les requêtes DNS. Chaque règle d'un groupe de règles nécessite un seul paramètre de protection avancée du pare-feu DNS. Vous pouvez choisir une protection parmi :

- Algorithmes de génération de domaines (DGAs)

  DGAs sont utilisés par les attaquants pour générer un grand nombre de domaines afin de lancer des attaques de malwares.

- Tunneling DNS

  Le tunneling DNS est utilisé par les attaquants pour exfiltrer les données du client en utilisant le tunnel DNS sans établir de connexion réseau avec le client.

Dans une règle avancée de pare-feu DNS, vous pouvez choisir de bloquer ou d'alerter sur une requête correspondant à la menace. Les algorithmes de protection contre les menaces sont gérés et mis à jour par AWS.

Pour de plus amples informations, veuillez consulter Route 53 Resolver DNS Firewall Advanced.

Seuil de confiance (protection avancée du pare-feu DNS uniquement)

Le seuil de confiance pour la protection contre les menaces DNS. Vous devez fournir cette valeur lorsque vous créez une règle avancée de pare-feu DNS. Les valeurs du niveau de confiance signifient :

- Élevé : détecte uniquement les menaces les mieux corroborées avec un faible taux de faux positifs.
- Moyen : fournit un équilibre entre la détection des menaces et celle des faux positifs.
- Faible : fournit le taux de détection des menaces le plus élevé, mais augmente également le nombre de faux positifs.

Pour de plus amples informations, veuillez consulter Paramètres de règles dans le pare-feu DNS.

Association entre un groupe de règles de pare-feu DNS et un VPC

Définit une protection pour un VPC à l'aide d'un groupe de règles de pare-feu DNS et active la configuration du pare-feu DNS de Resolver pour le VPC.

Si vous associez plusieurs groupes de règles à un seul VPC, vous indiquez leur ordre de traitement via le paramètre de priorité des associations. Le pare-feu DNS traite les groupes de règles pour un VPC en commençant par le paramètre de priorité numérique le plus bas.

Pour de plus amples informations, veuillez consulter Activation des protections Route 53 Resolver DNS Firewall pour votre VPC.

Configuration du pare-feu DNS de Resolver pour un VPC

Spécifie comment Resolver doit gérer les protections de pare-feu DNS au niveau du VPC. Cette configuration est en vigueur chaque fois qu'au moins un groupe de règles de pare-feu DNS est associé au VPC.

Cette configuration spécifie comment Route 53 Resolver traite les requêtes lorsque le pare-feu DNS ne parvient pas à les filtrer. Par défaut, si Resolver ne reçoit pas de réponse du pare-feu DNS pour une requête, il échoue et bloque la requête.

Pour de plus amples informations, veuillez consulter Configuration de VPC du pare-feu DNS.

Surveillance des actions du pare-feu DNS

Vous pouvez utiliser Amazon CloudWatch pour surveiller le nombre de requêtes DNS filtrées par les groupes de règles du pare-feu DNS. CloudWatch collecte et traite les données brutes pour en faire des indicateurs lisibles en temps quasi réel.

Pour de plus amples informations, veuillez consulter Surveillance des groupes de règles du pare-feu DNS Route 53 Resolver avec Amazon CloudWatch.

Vous pouvez utiliser Amazon EventBridge, un service sans serveur qui utilise des événements pour connecter les composants de l'application entre eux, afin de créer des applications évolutives pilotées par des événements.

Pour de plus amples informations, veuillez consulter Gestion des événements du pare-feu DNS Route 53 Resolver à l'aide de Amazon EventBridge.

Comment Route 53 Resolver DNS Firewall filtre les requêtes DNS

Lorsqu'un groupe de règles de pare-feu DNS est associé à Route 53 Resolver de votre VPC, le trafic suivant est filtré par le pare-feu :

- Requêtes DNS provenant de ce VPC et passant par le DNS du VPC.
- Requêtes DNS qui passent par les points de terminaison de Resolver à partir de ressources sur site jusqu'au VPC dont le pare-feu DNS est associé à son résolveur.

Lorsque le pare-feu DNS reçoit une requête DNS, il filtre la requête à l'aide des groupes de règles, des règles et d'autres paramètres que vous avez configurés et renvoie les résultats à Resolver :

- Le pare-feu DNS évalue la requête DNS à l'aide des groupes de règles associés au VPC jusqu'à ce qu'il trouve une correspondance ou qu'il épuise tous les groupes de règles. Le pare-feu DNS évalue les groupes de règles dans l'ordre de priorité que vous définissez dans l'association, en commençant par le paramètre numérique le plus bas. Pour plus d’informations, consultez Règles et groupes de règles de pare-feu DNS et Activation des protections Route 53 Resolver DNS Firewall pour votre VPC.
- Au sein de chaque groupe de règles, le pare-feu DNS évalue la requête DNS par rapport à la liste de domaines de chaque règle ou aux protections avancées du pare-feu DNS jusqu'à ce qu'il trouve une correspondance ou qu'il épuise toutes les règles. Le pare-feu DNS évalue les règles dans

l'ordre de priorité, en commençant par le paramètre numérique le plus bas. Pour de plus amples informations, veuillez consulter Règles et groupes de règles de pare-feu DNS.

- Lorsque le pare-feu DNS trouve une correspondance avec la liste de domaines d'une règle ou des anomalies identifiées par les règles de protection avancées du pare-feu DNS, il met fin à l'évaluation de la requête et répond au Resolver avec le résultat. Si l'action est `alert`, le pare-feu DNS envoie également une alerte aux journaux configurés de Resolver. Pour plus d'informations, consultez Actions de règle dans le pare-feu DNS, Listes de domaines Route 53 Resolver DNS Firewall et Route 53 Resolver DNS Firewall Advanced.
- Si le pare-feu DNS évalue tous les groupes de règles sans trouver de correspondance, il répond à la requête comme d'habitude.

Resolver achemine la requête en fonction de la réponse du pare-feu DNS. Dans le cas peu probable où le pare-feu DNS ne répond pas, Resolver applique le mode d'échec configuré du pare-feu DNS du VPC. Pour de plus amples informations, veuillez consulter Configuration de VPC du pare-feu DNS.

Étapes de haut niveau pour utiliser Route 53 Resolver DNS Firewall

Pour implémenter le filtrage Route 53 Resolver DNS Firewall dans votre Amazon Virtual Private Cloud (VPC), effectuez les étapes de haut niveau suivantes.

- Définissez votre approche de filtrage, vos listes de domaines ou les protections du pare-feu DNS : décidez de la manière dont vous souhaitez filtrer les requêtes, identifiez les spécifications de domaine dont vous aurez besoin et définissez la logique que vous utiliserez pour évaluer les requêtes. Par exemple, vous voudrez peut-être autoriser toutes les requêtes, excepté celles qui se trouvent dans une liste de domaines malveillants connus. Ou vous voudrez peut-être faire le contraire et bloquer tous les domaines, sauf ceux qui se trouvent dans une liste approuvée, une approche appelée « walled garden » (jardin fermé). Vous pouvez créer et gérer vos propres listes de spécifications de domaines approuvés ou bloqués et vous pouvez utiliser des listes de domaines AWS gérées pour vous. Pour les protections du pare-feu DNS, vous pouvez filtrer les requêtes en les bloquant toutes, ou vous pouvez émettre une alerte en cas de trafic de requêtes suspect vers des domaines susceptibles de contenir des anomalies associées à des menaces (DGA, tunneling DNS) afin de tester les paramètres de votre pare-feu DNS. Pour plus d'informations, consultez Listes de domaines Route 53 Resolver DNS Firewall et Route 53 Resolver DNS Firewall Advanced.
- Créez un groupe de règles de pare-feu : dans le pare-feu DNS, créez un groupe de règles pour filtrer les requêtes DNS pour votre VPC. Vous devez créer un groupe de règles dans chaque région

où vous souhaitez l'utiliser. Vous pouvez également séparer votre comportement de filtrage en plusieurs groupes de règles afin de pouvoir le réutiliser dans plusieurs scénarios de filtrage adaptés à vos différents VPCs. Pour de plus amples informations sur les groupes de règles, reportez-vous à la section Règles et groupes de règles de pare-feu DNS.

- Ajoutez et configurez vos règles : ajoutez une règle à votre groupe de règles pour chaque liste de domaines et comportement de filtrage que vous souhaitez que le groupe de règles fournisse. Définissez les paramètres de priorité de vos règles afin qu'elles soient traitées dans le bon ordre au sein du groupe de règles, en accordant la priorité la plus faible à la règle que vous souhaitez évaluer en premier. Pour de plus amples informations sur les règles, veuillez consulter Règles et groupes de règles de pare-feu DNS.
- Associez le groupe de règles à votre VPC : pour commencer à utiliser votre groupe de règles de pare-feu DNS, associez-le à votre VPC. Si vous utilisez plusieurs groupes de règles pour votre VPC, définissez la priorité de chaque association afin que les groupes de règles soient traités dans le bon ordre, en donnant la priorité la plus faible au groupe de règles que vous souhaitez évaluer en premier. Pour de plus amples informations, veuillez consulter Gestion des associations entre votre VPC et le groupe de règles Route 53 Resolver DNS Firewall.
- (Facultatif) Modifiez la configuration du pare-feu pour le VPC : si vous voulez que Route 53 Resolver bloque les requêtes pour lesquelles le pare-feu DNS ne parvient pas à renvoyer une réponse, modifiez la configuration du pare-feu DNS du VPC dans Resolver. Pour de plus amples informations, veuillez consulter Configuration de VPC du pare-feu DNS.

Utilisation de groupes de règles Route 53 Resolver DNS Firewall dans plusieurs régions

Le pare-feu DNS Route 53 Resolver étant un service régional, les objets que vous créez dans une AWS région ne sont disponibles que dans cette région. Pour utiliser la même règle dans plusieurs régions, vous devez la créer dans chaque région.

Le AWS compte qui a créé un groupe de règles peut le partager avec d'autres AWS comptes. Pour de plus amples informations, veuillez consulter Partage des groupes de règles du pare-feu DNS Route 53 Resolver entre les comptes AWS.

Disponibilité régionale pour le pare-feu DNS Route 53 Resolver

Le pare-feu DNS est disponible dans les versions suivantes Régions AWS :

- Afrique (Le Cap)
- Asie-Pacifique (Hong Kong)
- Asie-Pacifique (Hyderabad)
- Asie-Pacifique (Jakarta)
- Asie-Pacifique (Malaisie)
- Asie-Pacifique (Melbourne)
- Asie-Pacifique (Mumbai)
- Région Asie-Pacifique (Osaka)
- Asie-Pacifique (Séoul)
- Asie-Pacifique (Singapour)
- Asie-Pacifique (Sydney)
- Asie-Pacifique (Thaïlande)
- Asie-Pacifique (Tokyo)
- Région Canada (Centre)
- Canada-Ouest (Calgary)
- Région Europe (Frankfurt)
- Région Europe (Irlande)
- Région Europe (London)
- Europe (Milan)
- Région Europe (Paris)
- Europe (Espagne)
- Europe (Stockholm)
- Europe (Zurich)
- Israël (Tel Aviv)
- Mexique (centre)
- Moyen-Orient (Bahreïn)
- Moyen-Orient (EAU)
- Amérique du Sud (São Paulo)
- USA Est (Virginie du Nord)
- USA Est (Ohio)

- USA Ouest (Californie du Nord)
- US West (Oregon)
- Chine (Beijing)
- Chine (Ningxia)
- AWS GovCloud (US)

Mise en route avec Route 53 Resolver DNS Firewall

La console du pare-feu DNS inclut un assistant qui vous guide tout au long des étapes suivantes pour démarrer avec le pare-feu DNS :

- Créez des groupes de règles pour chaque ensemble de règles que vous souhaitez utiliser.
- Pour chaque règle, renseignez la liste de domaines que vous souhaitez inspecter. Vous pouvez créer vos propres listes de domaines et utiliser des listes de domaines AWS gérées.
- Associez vos groupes de règles à l' VPCs endroit où vous souhaitez les utiliser.

Exemple de Route 53 Resolver DNS Firewall « walled garden » (jardin fermé)

Dans ce didacticiel, vous allez créer un groupe de règles qui bloque tous les domaines, sauf un groupe de domaines approuvés. C'est ce qu'on appelle une plateforme fermée, ou approche « walled garden » (jardin fermé).

Pour configurer un groupe de règles de pare-feu DNS à l'aide de l'assistant de la console

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.

   Choisissez Pare-feu DNS dans le volet de navigation pour ouvrir la page des groupes de règles de pare-feu DNS sur la console Amazon VPC. Passez à l'étape 3.

   - OU -

   Connectez-vous au AWS Management Console et ouvrez-le

   la console Amazon VPC située sous. https://console.aws.amazon.com/vpc/
2. Dans le volet de navigation, sous Pare-feu DNS, choisissez Groupes de règles.

3. Dans la barre de navigation, choisissez la région pour le groupe de règles.
4. Sur la page Rule groups (Groupes de règles), choisissez Add rule group (Ajouter un groupe de règles).
5. Saisissez **`WalledGardenExample`** comme nom pour le groupe de règles.

   Dans la section Tags, vous pouvez éventuellement saisir une paire clé-valeur pour une balise. Les balises vous aident à organiser et à gérer vos ressources AWS . Pour de plus amples informations, veuillez consulter Balisage des ressources Amazon Route 53.
6. Choisissez Ajouter un groupe de règles.
7. Sur la page de WalledGardenExampledétails, choisissez l'onglet Règles, puis Ajouter une règle.
8. Dans le panneau Rule details (Détails de la règle), saisissez le nom de la règle **`BlockAll`**.
9. Dans le panneau Domain list (Liste des domaines), sélectionnez Add my own domain list (Ajouter ma propre liste de domaines).
10. Sous Choose or create a new domain list (Choisir ou créer une nouvelle liste de domaines), sélectionnez Create new domain list (Créer une nouvelle liste de domaines).
11. Entrez un nom de liste de domaines**`AllDomains`**, puis dans la zone de texte Entrez un domaine par ligne, entrez un astérisque :**`*`**.
12. Pour le paramètre de redirection de domaine, acceptez la valeur par défaut et laissez le champ Type de requête (facultatif) vide.
13. Pour l'action, sélectionnez BLOQUER, puis laissez la réponse à envoyer avec le paramètre par défaut NODATA.
14. Choisissez Ajouter une règle. Votre règle BlockAlls'affiche dans l'onglet Règles de la WalledGardenExamplepage.
15. Sur la WalledGardenExamplepage, choisissez Ajouter une règle pour ajouter une deuxième règle à votre groupe de règles.
16. Dans le volet Détails de la règle, entrez le nom de la règle**`AllowSelectDomains`**.
17. Dans le panneau Domain list (Liste des domaines), sélectionnez Add my own domain list (Ajouter ma propre liste de domaines).
18. Sous Choose or create a new domain list (Choisir ou créer une nouvelle liste de domaines), sélectionnez Create new domain list (Créer une nouvelle liste de domaines).
19. Saisissez un nom de liste de domaines **`ExampleDomains`**.
20. Dans la zone de texte Entrez un domaine par ligne, sur la première ligne, entrez **`example.com`** et sur la deuxième ligne, entrez**`example.org`**.

> **Note**
>
> Si vous souhaitez que la règle s'applique également aux sous-domaines, vous devez également ajouter ces domaines à la liste. Par exemple, pour ajouter tous les sous-domaines de example.com, ajoutez **`*.example.com`** à la liste.

21. Pour le paramètre de redirection de domaine, acceptez la valeur par défaut et laissez le champ Type de requête (facultatif) vide.
22. Pour l'action, sélectionnez AUTORISER.
23. Choisissez Ajouter une règle. Vos règles sont toutes deux affichées dans l'onglet Règles de la WalledGardenExamplepage.
24. Dans l'onglet Règles de la WalledGardenExamplepage, vous pouvez ajuster l'ordre d'évaluation des règles de votre groupe de règles en sélectionnant le numéro indiqué dans la colonne Priorité et en saisissant un nouveau numéro. Le pare-feu DNS évalue les règles en commençant par le paramètre de priorité le plus bas, de sorte que la règle ayant la priorité la plus faible est la première évaluée. Dans cet exemple, nous voulons que le pare-feu DNS identifie et autorise d'abord les requêtes DNS pour la liste de domaines sélectionnée, puis bloque les requêtes restantes.

    Ajustez la priorité de la règle afin qu'AllowSelectDomainselle ait une priorité inférieure.

Vous disposez désormais d'un groupe de règles qui autorise uniquement les requêtes de domaines spécifiques. Pour commencer à l'utiliser, associez-le à l' VPCs endroit où vous souhaitez utiliser le comportement de filtrage. Pour de plus amples informations, veuillez consulter Gestion des associations entre votre VPC et le groupe de règles Route 53 Resolver DNS Firewall.

Exemple de liste rouge Route 53 Resolver DNS Firewall

Dans ce didacticiel, vous allez créer un groupe de règles qui bloque les domaines que vous considérez comme malveillants. Vous allez également ajouter un type de requête DNS autorisé pour les domaines de la liste bloquée. Le groupe de règles autorise toutes les autres requêtes DNS sortantes via Route 53 Resolver.

Pour configurer une liste rouge de pare-feu DNS à l'aide de l'assistant de la console

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.

Choisissez Pare-feu DNS dans le volet de navigation pour ouvrir la page des groupes de règles de pare-feu DNS sur la console Amazon VPC. Passez à l'étape 3.

- OU -

Connectez-vous à la console Amazon VPC AWS Management Console et ouvrez-la à l'adresse. https://console.aws.amazon.com/vpc/

2. Dans le volet de navigation, sous Pare-feu DNS, choisissez Groupes de règles.
3. Dans la barre de navigation, choisissez la région pour le groupe de règles.
4. Sur la page Rule groups (Groupes de règles), choisissez Add rule group (Ajouter un groupe de règles).
5. Saisissez **`BlockListExample`** comme nom pour le groupe de règles.

   Dans la section Tags, vous pouvez éventuellement saisir une paire clé-valeur pour une balise. Les balises vous aident à organiser et à gérer vos ressources AWS . Pour de plus amples informations, veuillez consulter Balisage des ressources Amazon Route 53.
6. Sur la page de BlockListExampledétails, choisissez l'onglet Règles, puis Ajouter une règle.
7. Dans le panneau Rule details (Détails de la règle), saisissez le nom de la règle **`BlockList`**.
8. Dans le panneau Domain list (Liste des domaines), sélectionnez Add my own domain list (Ajouter ma propre liste de domaines).
9. Sous Choose or create a new domain list (Choisir ou créer une nouvelle liste de domaines), sélectionnez Create new domain list (Créer une nouvelle liste de domaines).
10. Saisissez un nom de liste de domaines **`MaliciousDomains`**, puis dans la zone de texte, saisissez les domaines que vous souhaitez bloquer. Par exemple, **`example.org`**. Saisissez un domaine par ligne.

    > **Note**
    >
    > Si vous souhaitez que la règle s'applique également aux sous-domaines, vous devez également ajouter ces domaines à la liste. Par exemple, pour ajouter tous les sous-domaines de example.org, ajoutez **`*.example.org`** à la liste.
11. Pour le paramètre de redirection de domaine, acceptez la valeur par défaut et laissez le champ Type de requête (facultatif) vide.

12. Pour l'action, sélectionnez BLOCK, puis laissez la réponse à envoyer au paramètre par défaut de NODATA.
13. Choisissez Ajouter une règle. Votre règle est affichée dans l'onglet Règles de la BlockListExamplepage
14. dans l'onglet Règles de la BlockedListExamplepage, vous pouvez ajuster l'ordre d'évaluation des règles de votre groupe de règles en sélectionnant le numéro indiqué dans la colonne Priorité et en saisissant un nouveau numéro. Le pare-feu DNS évalue les règles en commençant par le paramètre de priorité le plus bas, de sorte que la règle ayant la priorité la plus faible est la première évaluée.

    Sélectionnez et ajustez la priorité de la règle afin qu'elle BlockListsoit évaluée avant ou après toute autre règle que vous pourriez avoir. La plupart du temps, les domaines malveillants connus devraient être bloqués en premier. Autrement dit, les règles qui leur sont associées devraient avoir le numéro de priorité le plus bas.
15. Pour ajouter une règle autorisant les enregistrements MX pour les BlockList domaines, sur la page de BlockedListExampledétails de l'onglet Règles, sélectionnez Ajouter une règle.
16. Dans le panneau Rule details (Détails de la règle), saisissez le nom de la règle **`BlockList-allowMX`**.
17. Dans le panneau Domain list (Liste des domaines), sélectionnez Add my own domain list (Ajouter ma propre liste de domaines).
18. Sous Choisir ou créer une nouvelle liste de domaines, sélectionnez**`MaliciousDomains`**.
19. Pour le paramètre de redirection de domaine, acceptez la valeur par défaut.
20. Dans la liste des types de requêtes DNS, sélectionnez MX : Spécifie les serveurs de messagerie.
21. Pour l'action, sélectionnez ALLOW.
22. Choisissez Ajouter une règle.
23. dans l'onglet Règles de la BlockedListExamplepage, vous pouvez ajuster l'ordre d'évaluation des règles de votre groupe de règles en sélectionnant le numéro indiqué dans la colonne Priorité et en saisissant un nouveau numéro. Le pare-feu DNS évalue les règles en commençant par le paramètre de priorité le plus bas, de sorte que la règle ayant la priorité la plus faible est la première évaluée.

    Sélectionnez et ajustez la priorité de la règle afin que BlockList-AllowMX soit évalué avant ou après toute autre règle que vous pourriez avoir. Comme vous souhaitez autoriser les requêtes MX, assurez-vous que la règle BlockList-AllowMX a une priorité inférieure à. BlockList

Vous disposez désormais d'un groupe de règles qui bloque les requêtes de domaine malveillantes spécifiques, mais autorise un type de requête DNS spécifique. Pour commencer à l'utiliser, associez-le à l' VPCs endroit où vous souhaitez utiliser le comportement de filtrage. Pour de plus amples informations, veuillez consulter Gestion des associations entre votre VPC et le groupe de règles Route 53 Resolver DNS Firewall.

Règles et groupes de règles de pare-feu DNS

Cette section décrit les paramètres que vous pouvez configurer pour les groupes de règles et les règles de votre pare-feu DNS, afin de définir le comportement de votre pare-feu DNS VPCs. Elle décrit également comment gérer les paramètres de vos règles et groupes de règles.

Une fois vos groupes de règles configurés comme vous le souhaitez, vous les utilisez directement et vous pouvez les partager et les gérer entre les comptes et dans l'ensemble de votre organisation dans AWS Organizations.

- Vous pouvez associer un groupe de règles à plusieurs VPCs afin de garantir un comportement cohérent au sein de votre organisation. Pour plus d'informations, consultez Gestion des associations entre votre VPC et le groupe de règles Route 53 Resolver DNS Firewall.
- Vous pouvez partager des groupes de règles entre les comptes pour bénéficier d'une gestion cohérente des requêtes DNS dans l'ensemble de votre organisation. Pour plus d'informations, consultez Partage des groupes de règles du pare-feu DNS Route 53 Resolver entre les comptes AWS.
- Vous pouvez utiliser les groupes de règles au sein de votre organisation AWS Organizations en les gérant dans AWS Firewall Manager des politiques. Pour plus d'informations sur Firewall Manager, consultez AWS Firewall Managerle AWS WAF AWS Firewall Manager, et le Guide AWS Shield Advanced du développeur.

Paramètres de groupe de règles dans le pare-feu DNS

Lorsque vous créez ou modifiez un groupe de règles de pare-feu DNS, spécifiez les valeurs suivantes :

Nom

Un nom unique qui vous permet de retrouver facilement un groupe de règles sur le tableau de bord.

(Facultatif) Description

Une brève description qui fournit plus de contexte pour le groupe de règles.

Région

La AWS région que vous choisissez lorsque vous créez le groupe de règles. Les groupes de règles que vous créez dans une région ne sont disponibles que dans cette région. Pour utiliser la même règle dans plusieurs régions, vous devez la créer dans chaque région.

Règles

Le comportement de filtrage du groupe de règles est contenu dans ses règles. Pour plus d'informations, consultez la section suivante.

Balises

Spécifiez une ou plusieurs clés et les valeurs correspondantes. Par exemple, vous pouvez indiquer Cost center (Centre de coûts) pour Key (Clé) et 456 pour Value (Valeur).

Ce sont les tags qui AWS Billing and Cost Management permettent d'organiser votre AWS facture. Pour en savoir plus sur l'utilisation des identifications pour la répartition des coûts, consultez Utilisation des identifications de répartition des coûts dans le Guide de l'utilisateur AWS Billing .

Paramètres de règles dans le pare-feu DNS

Lorsque vous créez ou modifiez une règle dans un groupe de règles de pare-feu DNS, spécifiez les valeurs suivantes :

Nom

Un identifiant unique pour la règle dans le groupe de règles.

(Facultatif) Description

Une brève description qui fournit plus d'informations sur la règle.

Domain list (Liste des domaines)

La liste des domaines que la règle inspecte. Vous pouvez créer et gérer vos propres listes de domaines ou vous abonner à une liste de domaines qu' AWS gère pour vous. Pour de plus amples informations, veuillez consulter Listes de domaines Route 53 Resolver DNS Firewall.

Une règle peut contenir une liste de domaines ou une protection avancée par pare-feu DNS, mais pas les deux.

Paramètre de redirection de domaines (listes de domaines uniquement)

Vous pouvez choisir que la règle du pare-feu DNS n'inspecte que le premier domaine ou tous les domaines (par défaut) de la chaîne de redirection DNS, tels que CNAME, DNAME, etc. Si vous choisissez d'inspecter tous les domaines, vous devez ajouter les domaines suivants de la chaîne de redirection DNS à la liste des domaines et définir l'action que vous souhaitez que la règle exécute, soit ALLOW, BLOCK ou ALERT. Pour de plus amples informations, veuillez consulter Composants et paramètres de Route 53 Resolver DNS Firewall.

Type de requête (listes de domaines uniquement)

Liste des types de requêtes DNS inspectés par la règle. Les valeurs valides sont les suivantes :

- R : Renvoie une IPv4 adresse.
- AAAA : renvoie une adresse IPv6.
- CAA : restrictions CAs qui peuvent créer des SSL/TLS certifications pour le domaine.
- CNAME : renvoie un autre nom de domaine.
- DS : enregistrement identifiant la clé de signature DNSSEC d'une zone déléguée.
- MX : Spécifie les serveurs de messagerie.
- NAPTR : Regular-expression-based réécriture de noms de domaine.
- NS : serveurs de noms faisant autorité.
- PTR : associe une adresse IP à un nom de domaine.
- SOA : Début de l'enregistrement d'autorité pour la zone.
- SPF : répertorie les serveurs autorisés à envoyer des e-mails depuis un domaine.
- SRV : valeurs spécifiques à l'application qui identifient les serveurs.
- TXT : vérifie les expéditeurs d'e-mails et les valeurs spécifiques à l'application.
- Type de requête que vous définissez à l'aide de l'ID de type DNS, par exemple 28 pour AAAA. Les valeurs doivent être définies comme TYPE*NUMBER*, où elles *NUMBER* peuvent être comprises entre 1 et 65334, par exemple. TYPE28 Pour plus d'informations, consultez la section Liste des types d'enregistrements DNS.

  Vous pouvez créer un type de requête par règle.

> **Note**
>
> Si vous configurez une règle BLOCK de pare-feu dont l'action NXDOMAIN sur le type de requête est égale à AAAA, cette action ne sera pas appliquée aux IPv6 adresses synthétiques générées lorsqu'elle DNS64 est activée.

Protection avancée du pare-feu DNS

Détecte les requêtes DNS suspectes en fonction des signatures de menaces connues dans les requêtes DNS. Vous pouvez choisir une protection parmi :

- Algorithmes de génération de domaines (DGAs)

  DGAs sont utilisés par les attaquants pour générer un grand nombre de domaines afin de lancer des attaques de malwares.

- Tunneling DNS

  Le tunneling DNS est utilisé par les attaquants pour exfiltrer les données du client en utilisant le tunnel DNS sans établir de connexion réseau avec le client.

Dans une règle avancée de pare-feu DNS, vous pouvez choisir de bloquer ou d'alerter sur une requête correspondant à la menace.

Pour de plus amples informations, veuillez consulter Route 53 Resolver DNS Firewall Advanced.

Une règle peut contenir une protection avancée du pare-feu DNS ou une liste de domaines, mais pas les deux.

Seuil de confiance (DNS Firewall Advanced uniquement)

Le seuil de confiance pour DNS Firewall Advanced. Vous devez fournir cette valeur lorsque vous créez une règle avancée de pare-feu DNS. Les valeurs du niveau de confiance signifient :

- Élevé : détecte uniquement les menaces les mieux corroborées avec un faible taux de faux positifs.
- Moyen : fournit un équilibre entre la détection des menaces et celle des faux positifs.
- Faible : fournit le taux de détection des menaces le plus élevé, mais augmente également le nombre de faux positifs.

Pour de plus amples informations, veuillez consulter Paramètres de règles dans le pare-feu DNS.

Action

La manière dont le pare-feu DNS doit gérer une requête DNS dont le nom de domaine correspond aux spécifications de la liste de domaines de la règle. Pour de plus amples informations, veuillez consulter Actions de règle dans le pare-feu DNS.

Priorité

Paramètre d'entier positif unique pour la règle au sein du groupe de règles qui détermine l'ordre de traitement. Le pare-feu DNS inspecte les requêtes DNS par rapport aux règles d'un groupe de règles en commençant par le paramètre de priorité numérique le plus bas. Vous pouvez modifier la priorité d'une règle à tout moment, par exemple pour modifier l'ordre de traitement ou créer de l'espace pour d'autres règles.

Actions de règle dans le pare-feu DNS

Lorsque le pare-feu DNS trouve une correspondance entre une requête DNS et une spécification de domaine dans une règle, il applique à la requête l'action indiquée dans la règle.

Vous devez indiquer l'une des options suivantes dans chaque règle que vous créez :

- Allow – Arrêter l'inspection de la requête et l'autoriser à passer. Non disponible pour DNS Firewall Advanced.
- Alert – Arrêter l'inspection de la requête, l'autorisez à passer et journaliser une alerte pour la requête dans les journaux de Route 53 Resolver.
- Block – Interrompre l'inspection de la requête, l'empêcher d'accéder à sa destination prévue et journaliser l'action de blocage de la requête dans les journaux de Route 53 Resolver.

  Répondez avec la réponse de blocage configurée, à partir de la liste suivante :

  - NODATA : répondez en indiquant que la requête a réussi, mais qu'aucune réponse n'est disponible.
  - NXDOMAIN – Répondre en indiquant que le nom de domaine de la requête n'existe pas.
  - OVERRIDE : fournissez un remplacement personnalisé dans la réponse. Cette option nécessite les paramètres supplémentaires suivants :
    - Record value – Enregistrement DNS personnalisé à renvoyer en réponse à la requête.
    - Record type – Type de l'enregistrement DNS. Il détermine le format de la valeur d'enregistrement. Il doit être `CNAME`.

- Time to live in seconds – Durée recommandée pour la mise en cache de l'enregistrement de remplacement par le résolveur DNS ou le navigateur web et son utilisation en réponse à cette requête, s'il est de nouveau reçu. Par défaut, ce paramètre est défini sur zéro et l'enregistrement n'est pas mis en cache.

Pour en savoir plus sur la configuration et le contenu des journaux de requête, consultez Journalisation des requêtes Resolver et Valeurs qui apparaissent dans les journaux de requête Resolver.

Utiliser Alert pour tester les règles de blocage

Lorsque vous créez une règle de blocage pour la première fois, vous pouvez la tester en la configurant avec l'action définie sur Alert. Vous pouvez ensuite examiner le nombre de requêtes pour lesquelles la règle crée une alerte afin de voir combien de requêtes seraient bloquées si vous définissez l'action sur Block.

Gestion des règles et groupes de règles dans le pare-feu DNS

Pour gérer les groupes de règles et les règles dans la console, suivez les instructions de cette section.

Lorsque vous apportez des modifications aux entités du pare-feu DNS, telles que les règles et les listes de domaines, le pare-feu DNS propage les modifications partout où les entités sont stockées et utilisées. Vos modifications sont appliquées en quelques secondes, mais il peut y avoir une brève période d'incohérence lorsque les modifications arrivent à certains endroits et non à d'autres. Par exemple, si vous ajoutez un domaine à une liste de domaines référencée par une règle de blocage, le nouveau domaine peut être brièvement bloqué dans une zone de votre VPC et être toujours autorisé dans une autre. Cette incohérence temporaire peut se produire lorsque vous configurez vos associations de groupes de règles et de VPC pour la première fois et lorsque vous modifiez des paramètres existants. En règle générale, les incohérences de ce type ne durent que quelques secondes.

Création d'un groupe de règles et de règles

Pour créer un groupe de règles et y ajouter des règles, suivez les étapes de cette procédure.

Pour créer un groupe de règles et ses règles

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.

   Choisissez Pare-feu DNS dans le volet de navigation pour ouvrir la page des groupes de règles de pare-feu DNS sur la console Amazon VPC. Passez à l'étape 3.

   - OU -

   Connectez-vous au AWS Management Console et ouvrez-le

   la console Amazon VPC située sous. https://console.aws.amazon.com/vpc/
2. Dans le volet de navigation, sous Pare-feu DNS, choisissez Groupes de règles.
3. Dans la barre de navigation, choisissez la région pour le groupe de règles.
4. Choisissez Add rule group (Ajouter un groupe de règles), puis suivez les instructions de l'assistant pour indiquer les paramètres du groupe de règles et des règles.

   Pour plus d'informations sur les valeurs des groupes de règles, consultez Paramètres de groupe de règles dans le pare-feu DNS.

   Pour plus d'informations sur les valeurs des règles, consultez Paramètres de règles dans le pare-feu DNS.

Affichage et mise à jour d'un groupe de règles et des règles

Utilisez la procédure suivante pour afficher les groupes de règles et les règles qui leur sont assignées. Vous pouvez également mettre à jour le groupe de règles et les paramètres des règles.

Pour afficher et mettre à jour un groupe de règles

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.

   Choisissez Pare-feu DNS dans le volet de navigation pour ouvrir la page des groupes de règles de pare-feu DNS sur la console Amazon VPC. Passez à l'étape 3.

   - OU -

   Connectez-vous au AWS Management Console et ouvrez-le

la console Amazon VPC située sous. https://console.aws.amazon.com/vpc/

2. Dans le volet de navigation, sous Pare-feu DNS, choisissez Groupes de règles.
3. Dans la barre de navigation, choisissez la région pour le groupe de règles.
4. Sélectionnez le groupe de règles que vous souhaitez afficher ou modifier, puis choisissez View details (Afficher les détails).
5. Dans la page du groupe de règles, vous pouvez afficher et modifier les paramètres.

   Pour plus d'informations sur les valeurs des groupes de règles, consultez Paramètres de groupe de règles dans le pare-feu DNS.

   Pour plus d'informations sur les valeurs des règles, consultez Paramètres de règles dans le pare-feu DNS.

Suppression d'un groupe de règles

Pour supprimer un groupe de règles, suivez la procédure suivante.

> **Important**
>
> Si vous supprimez un groupe de règles associé à un VPC, le pare-feu DNS supprime l'association et arrête les protections que le groupe de règles fournissait au VPC.

Suppression des entités du pare-feu DNS

Lorsque vous supprimez une entité que vous pouvez utiliser dans le pare-feu DNS, comme une liste de domaines qui peut être utilisée dans un groupe de règles ou un groupe de règles qui peut être associé à un VPC, le pare-feu DNS vérifie si l'entité est actuellement utilisée. S'il constate qu'elle est en cours d'utilisation, le pare-feu DNS vous en avertit. Le pare-feu DNS est presque toujours capable de déterminer si une entité est en cours d'utilisation. Cependant, dans de rares cas, il peut ne pas être en mesure de le faire. Si vous devez vous assurer que rien n'utilise actuellement l'entité, vérifiez si elle se trouve dans vos configurations de pare-feu DNS avant de la supprimer. Si l'entité est une liste de domaines référencée, vérifiez qu'aucun groupe de règles ne l'utilise. Si l'entité est un groupe de règles, vérifiez qu'elle n'est associée à aucun groupe de règles VPCs.

Pour supprimer un groupe de règles

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.

   Choisissez Pare-feu DNS dans le volet de navigation pour ouvrir la page des groupes de règles de pare-feu DNS sur la console Amazon VPC. Passez à l'étape 3.

   - OU -

   Connectez-vous au AWS Management Console et ouvrez-le

   la console Amazon VPC située sous. https://console.aws.amazon.com/vpc/
2. Dans le volet de navigation, sous Pare-feu DNS, choisissez Groupes de règles.
3. Dans la barre de navigation, choisissez la région pour le groupe de règles.
4. Sélectionnez le groupe de règles que vous voulez supprimer, puis choisissez Delete (Supprimer) et confirmez la suppression.

Listes de domaines Route 53 Resolver DNS Firewall

Une liste de domaines est un ensemble réutilisable de spécifications de domaine que vous utilisez dans une règle de pare-feu DNS, à l'intérieur d'un groupe de règles. Lorsque vous associez un groupe de règles à un VPC, le pare-feu DNS compare vos requêtes DNS aux listes de domaines qui sont utilisées dans les règles. S'il trouve une correspondance, il gère la requête DNS en fonction de l'action de la règle correspondante. Pour de plus amples informations sur les règles et les groupes de règles, veuillez consulter Règles et groupes de règles de pare-feu DNS.

Les listes de domaines vous permettent de séparer vos spécifications de domaines explicites des actions que vous souhaitez entreprendre sur elles. Vous pouvez utiliser une seule liste de domaines dans plusieurs règles et toutes les mises à jour que vous apportez à la liste de domaines affectent automatiquement toutes les règles qui l'utilisent.

Les listes de domaines se répartissent en deux catégories principales :

- Des listes de domaines gérées, qui AWS créent et gèrent pour vous.
- Vos propres listes de domaines, que vous créez et gérez vous-même.

Cette section décrit les types de groupes de listes de domaines gérées disponibles et fournit des conseils pour la création et la gestion de vos propres listes de domaines, si vous le souhaitez.

Listes de domaines gérées

Les listes de domaines gérés contiennent des noms de domaine associés à des activités malveillantes ou à d'autres menaces potentielles. AWS tient à jour ces listes pour permettre aux clients de Route 53 Resolver de vérifier gratuitement les requêtes DNS sortantes par rapport à eux lorsqu'ils utilisent le pare-feu DNS.

La mise à jour dans le contexte d'un paysage de menaces en constante évolution peut prendre du temps et coûter cher. Les listes de domaines gérés peuvent vous faire gagner du temps lorsque vous implémentez et utilisez un pare-feu DNS. AWS met automatiquement à jour les listes lorsque de nouvelles vulnérabilités et menaces apparaissent. AWS est souvent informé des nouvelles vulnérabilités avant leur divulgation publique. DNS Firewall peut donc déployer des mesures d'atténuation pour vous avant qu'une nouvelle menace ne soit largement connue.

Les listes de domaines gérées sont conçues pour vous aider à vous protéger contre les menaces Web courantes et elles ajoutent une couche de sécurité supplémentaire à vos applications. Les listes de domaines AWS gérés fournissent leurs données à la fois à partir de AWS sources internes et sont continuellement mises à jour. RecordedFuture Toutefois, les listes de domaines AWS gérés ne sont pas destinées à remplacer d'autres contrôles de sécurité Amazon GuardDuty, tels que ceux qui sont déterminés par les AWS ressources que vous sélectionnez.

À titre de bonne pratique, avant d'utiliser une liste de domaines gérée en production, testez-la dans un environnement autre que de production, avec l'action de règle définie sur `Alert`. Évaluez la règle à l'aide CloudWatch des métriques Amazon associées aux requêtes échantillonnées du pare-feu DNS Route 53 Resolver ou aux journaux du pare-feu DNS. Une fois que le comportement de la règle vous convient, modifiez le paramètre d'action selon vos besoins.

Listes de domaines AWS gérés disponibles

Cette section décrit les listes de domaines gérées par qui sont actuellement disponibles. Si vous êtes dans une région où ces listes de domaines sont prises en charge, vous pouvez les voir sur la console lorsque vous gérez des listes de domaines et lorsque vous spécifiez la liste de domaines pour une règle. Dans les journaux, la liste de domaines est journalisée dans le fichier `firewall_domain_list_id field`.

AWS fournit les listes de domaines gérés suivantes, dans les régions où elles sont disponibles, à tous les utilisateurs du pare-feu DNS Route 53 Resolver.

- `AWSManagedDomainsMalwareDomainList` : domaines associés à l'envoi, à l'hébergement ou à la distribution de logiciels malveillants.
- `AWSManagedDomainsBotnetCommandandControl` : domaines associés au contrôle des réseaux d'ordinateurs infectés par des logiciels malveillants de courrier indésirable.
- `AWSManagedDomainsAggregateThreatList`— Domaines associés à plusieurs catégories de menaces DNS, notamment les malwares, les ransomwares, les botnets, les logiciels espions et le tunneling DNS pour aider à bloquer plusieurs types de menaces. `AWSManagedDomainsAggregateThreatList`inclut tous les domaines figurant dans les autres listes de domaines AWS gérés répertoriées ici.
- `AWSManagedDomainsAmazonGuardDutyThreatList`— Domaines associés aux résultats de sécurité GuardDuty du DNS d'Amazon. Les domaines proviennent uniquement des systèmes de GuardDuty renseignement sur les menaces des États-Unis et ne contiennent pas de domaines provenant de sources tierces externes. Plus précisément, cette liste ne bloque actuellement que les domaines générés en interne et utilisés pour les détections suivantes dans GuardDuty : Impact :/.Reputation, Impact :EC2/AbusedDomainRequest.Reputation, Impact :EC2/BitcoinDomainRequest.Reputation, Impact : EC2 MaliciousDomainRequest .Reputation. Runtime/AbusedDomainRequest.Reputation, Impact:Runtime/BitcoinDomainRequest.Reputation, and Impact:Runtime/MaliciousDomainRequest

  Pour plus d'informations, consultez la section Trouver des types dans le guide de GuardDuty l'utilisateur Amazon.

AWS Les listes de domaines gérés ne peuvent pas être téléchargées ni consultées. Pour protéger la propriété intellectuelle, vous ne pouvez pas consulter ou modifier les spécifications de domaines individuels dans une liste de domaines AWS gérés. Cette restriction aide également à empêcher les utilisateurs malveillants de concevoir des menaces qui contournent les listes publiées.

Pour tester les listes de domaines gérés

Nous fournissons l'ensemble de domaines suivant pour tester les listes de domaines gérées :

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 et AWSManaged DomainsAmazonGuardDutyThreatList

- 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

Ces domaines se résoudront en 1.2.3.4 s'ils ne sont pas bloqués. Si vous utilisez les listes de domaines gérées dans un VPC, les requêtes pour ces domaines renverront la réponse indiquant qu'une action de blocage dans la règle est définie sur (par exemple, NODATA).

Pour plus d'informations sur les listes de domaines gérées, contactez le Centre AWS Support.

Le tableau suivant répertorie la disponibilité des régions pour les listes de domaines AWS gérés.

Disponibilité régionale des listes de domaines gérées

Région	Les listes de domaines gérées sont-elles disponibles ?
Afrique (Le Cap)	Oui
Asie-Pacifique (Hong Kong)	Oui
Asie-Pacifique (Hyderabad)	Oui
Asie-Pacifique (Jakarta)	Oui
Asie-Pacifique (Malaisie)	Oui
Asie-Pacifique (Melbourne)	Oui
Asie-Pacifique (Mumbai)	Oui

Région	Les listes de domaines gérées sont-elles disponibles ?
Région Asie-Pacifique (Osaka)	Oui
Asie-Pacifique (Séoul)	Oui
Asie-Pacifique (Singapour)	Oui
Asie-Pacifique (Sydney)	Oui
Asie-Pacifique (Thaïlande)	Oui
Asie-Pacifique (Tokyo)	Oui
Région Canada (Centre)	Oui
Canada-Ouest (Calgary)	Oui
Région Europe (Francfort)	Oui
Région Europe (Irlande)	Oui
Région Europe (Londres)	Oui
Europe (Milan)	Oui
Région Europe (Paris)	Oui
Europe (Espagne)	Oui

Région	Les listes de domaines gérées sont-elles disponibles ?
Europe (Stockholm)	Oui
Europe (Zurich)	Oui
Israël (Tel Aviv)	Oui
Moyen-Orient (Bahreïn)	Oui
Moyen-Orient (EAU)	Oui
Amérique du Sud (São Paulo)	Oui
USA Est (Virginie du Nord)	Oui
USA Est (Ohio)	Oui
USA Ouest (Californie du Nord)	Oui
USA Ouest (Oregon)	Oui
Chine (Pékin)	Oui
Chine (Ningxia)	Oui
AWS GovCloud (US)	Oui

Considérations supplémentaires en matière de sécurité

AWS Les listes de domaines gérés sont conçues pour vous aider à vous protéger contre les menaces Web les plus courantes. Utilisées conformément à la documentation, ces listes ajoutent une autre couche de sécurité à vos applications. Toutefois, les listes de domaines gérées ne sont pas conçues pour remplacer d'autres contrôles de sécurité qui sont déterminés par les ressources AWS que vous sélectionnez. Pour vous assurer que vos ressources AWS sont correctement protégées, consultez les instructions du Shared Responsibility Model.

Atténuation des risques de scénarios de faux positifs

Si vous rencontrez des scénarios de faux positifs dans les règles qui utilisent les listes de domaines gérées par pour bloquer les requêtes, effectuez les étapes suivantes :

1. Dans les journaux de Resolver, identifiez le groupe de règles et la liste de domaines gérée qui provoquent le faux positif. Pour ce faire, recherchez le journal de la requête que le pare-feu DNS bloque, mais que vous souhaitez autoriser. L'enregistrement du journal répertorie le groupe de règles, l'action de la règle et la liste de domaines gérée. Pour de plus amples informations sur les journaux, veuillez consulter Valeurs qui apparaissent dans les journaux de requête Resolver.
2. Créez une nouvelle règle dans le groupe de règles qui autorise explicitement la requête bloquée. Lorsque vous créez la règle, vous pouvez définir votre propre liste de domaines avec uniquement la spécification de domaine que vous souhaitez autoriser. Suivez les instructions relatives à la gestion des règles et groupes de règles dans Création d'un groupe de règles et de règles.
3. Définissez la priorité de la nouvelle règle au sein du groupe de règles afin qu'elle s'exécute avant la règle qui utilise la liste de domaines gérée. Pour ce faire, donnez à la nouvelle règle un paramètre de priorité numérique inférieur.

Une fois que vous avez mis à jour votre groupe de règles, la nouvelle règle autorise explicitement le nom de domaine que vous souhaitez autoriser avant l'exécution de la règle de blocage.

Gestion de vos propres listes de domaines

Vous pouvez créer vos propres listes de domaines pour indiquer des catégories de domaines que vous ne trouvez pas dans les offres de listes de domaines gérées ou que vous préférez gérer vous-même.

Outre les procédures décrites dans cette section, dans la console, vous pouvez créer une liste de domaines dans le contexte de la gestion des règles Route 53 Resolver DNS Firewall lorsque vous créez ou mettez à jour une règle.

Chaque spécification de domaine dans votre liste de domaines doit satisfaire aux exigences suivantes :

- Elle peut éventuellement commencer par `*` (astérisque).
- À l'exception de l'astérisque initial facultatif et d'un point, comme délimiteur entre les étiquettes, elle ne doit contenir que les caractères suivants : `A-Z`, `a-z`, `0-9`, `-` (trait d'union).
- Sa longueur doit être comprise entre 1 et 255 caractères.

Lorsque vous apportez des modifications aux entités du pare-feu DNS, telles que les règles et les listes de domaines, le pare-feu DNS propage les modifications partout où les entités sont stockées et utilisées. Vos modifications sont appliquées en quelques secondes, mais il peut y avoir une brève période d'incohérence lorsque les modifications arrivent à certains endroits et non à d'autres. Par exemple, si vous ajoutez un domaine à une liste de domaines référencée par une règle de blocage, le nouveau domaine peut être brièvement bloqué dans une zone de votre VPC et être toujours autorisé dans une autre. Cette incohérence temporaire peut se produire lorsque vous configurez vos associations de groupes de règles et de VPC pour la première fois et lorsque vous modifiez des paramètres existants. En règle générale, les incohérences de ce type ne durent que quelques secondes.

Testez votre liste de domaines avant de l'utiliser en production

À titre de bonne pratique, avant d'utiliser une liste de domaines en production, testez-la dans un environnement autre que de production, avec l'action de règle définie sur `Alert`. Évaluez la règle à l'aide CloudWatch des métriques Amazon et des journaux Resolver. Les journaux fournissent le nom de la liste de domaines pour toutes les alertes et actions de blocage. Une fois que la liste de domaines correspond à vos requêtes DNS comme vous le souhaitez, modifiez le paramètre d'action de règle selon vos besoins. Pour plus d'informations sur CloudWatch les métriques et les journaux de requêtesSurveillance des groupes de règles du pare-feu DNS Route 53 Resolver avec Amazon CloudWatch, reportez-vous aux Valeurs qui apparaissent dans les journaux de requête Resolver sections, etGestion des configurations de journalisation des requêtes Resolver.

Pour ajouter une liste de domaines

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.

   Choisissez Pare-feu DNS dans le volet de navigation pour ouvrir la page des groupes de règles de pare-feu DNS sur la console Amazon VPC. Passez à l'étape 2.

- OU -

Connectez-vous au AWS Management Console et ouvrez-le

la console Amazon VPC située sous. https://console.aws.amazon.com/vpc/

2. Dans le volet de navigation, sous Pare-feu DNS, choisissez Listes de domaine. Sur la page Domain lists (Listes de domaines), vous pouvez sélectionner et modifier des listes de domaines existantes et ajouter vos propres listes.
3. Pour ajouter une liste de domaines, choisissez Add domain list (Ajouter une liste de domaines).
4. Indiquez un nom pour votre liste de domaines, puis saisissez vos spécifications de domaine dans la zone de texte (une spécification par ligne).

   Si vous définissez Switch to bulk upload (Passer au téléchargement groupé) sur on (activé), saisissez l'URI du compartiment Amazon S3 dans lequel vous avez créé une liste de domaines. Cette liste de domaines devrait avoir un nom de domaine par ligne.

   > **Note**
   >
   > Les noms de domaine dupliqués entraîneront l'échec de l'importation en bloc.

5. Choisissez Add domain list (Ajouter une liste de domaines). La page Domain lists (Listes de domaines) répertorie votre nouvelle liste de domaines.

Après avoir créé la liste de domaines, vous pouvez la référencer par son nom à partir de vos règles de pare-feu DNS.

Suppression des entités du pare-feu DNS

Lorsque vous supprimez une entité que vous pouvez utiliser dans le pare-feu DNS, comme une liste de domaines qui peut être utilisée dans un groupe de règles ou un groupe de règles qui peut être associé à un VPC, le pare-feu DNS vérifie si l'entité est actuellement utilisée. S'il constate qu'elle est en cours d'utilisation, le pare-feu DNS vous en avertit. Le pare-feu DNS est presque toujours capable de déterminer si une entité est en cours d'utilisation. Cependant, dans de rares cas, il peut ne pas être en mesure de le faire. Si vous devez vous assurer que rien n'utilise actuellement l'entité, vérifiez si elle se trouve dans vos configurations de pare-feu DNS avant de la supprimer. Si l'entité est une liste de domaines référencée, vérifiez qu'aucun groupe de règles ne l'utilise. Si l'entité est un groupe de règles, vérifiez qu'elle n'est associée à aucun groupe de règles VPCs.

Pour supprimer une liste de domaines

1. Dans le panneau de navigation, choisissez Domain lists (Listes de domaines).
2. Dans la barre de navigation, choisissez la région pour la liste de domaines.
3. Sélectionnez la liste de domaines que vous voulez supprimer, puis choisissez Delete (Supprimer) et confirmez la suppression.

Route 53 Resolver DNS Firewall Advanced

DNS Firewall Advanced détecte les requêtes DNS suspectes en fonction des signatures de menaces connues présentes dans les requêtes DNS. Vous pouvez spécifier un type de menace dans une règle que vous utilisez dans une règle de pare-feu DNS, au sein d'un groupe de règles. Lorsque vous associez un groupe de règles à un VPC, DNS Firewall compare vos requêtes DNS aux domaines marqués dans les règles. S'il trouve une correspondance, il gère la requête DNS en fonction de l'action de la règle correspondante.

DNS Firewall Advanced identifie les signatures de menaces DNS suspectes en inspectant une série d'identifiants clés dans la charge utile du DNS, notamment l'horodatage des demandes, la fréquence des demandes et des réponses, les chaînes de requêtes DNS et la longueur, le type ou la taille des requêtes DNS sortantes et entrantes. En fonction du type de signature de menace, vous pouvez configurer des politiques pour bloquer ou simplement enregistrer et envoyer une alerte sur la requête. En utilisant un ensemble étendu d'identificateurs de menaces, vous pouvez vous protéger contre les menaces DNS provenant de sources de domaine qui ne sont peut-être pas encore classifiées par les flux de renseignements sur les menaces gérés par l'ensemble de la communauté de sécurité.

Actuellement, DNS Firewall Advanced offre des protections contre :

- Algorithmes de génération de domaines (DGAs)

  DGAs sont utilisés par les attaquants pour générer un grand nombre de domaines afin de lancer des attaques de malwares.

- Tunneling DNS

  Le tunneling DNS est utilisé par les attaquants pour exfiltrer les données du client en utilisant le tunnel DNS sans établir de connexion réseau avec le client.

Pour savoir comment créer des règles, reportez-vous aux sections Création d'un groupe de règles et de règles etParamètres de règles dans le pare-feu DNS.

Atténuation des risques de scénarios de faux positifs

Si vous rencontrez des scénarios faussement positifs dans les règles qui utilisent les protections avancées du pare-feu DNS pour bloquer les requêtes, effectuez les opérations suivantes :

1. Dans les journaux du résolveur, identifiez le groupe de règles et les protections avancées du pare-feu DNS à l'origine du faux positif. Pour ce faire, recherchez le journal de la requête que le pare-feu DNS bloque, mais que vous souhaitez autoriser. L'enregistrement du journal répertorie le groupe de règles, l'action des règles et la protection avancée du pare-feu DNS. Pour de plus amples informations sur les journaux, veuillez consulter Valeurs qui apparaissent dans les journaux de requête Resolver.
2. Créez une nouvelle règle dans le groupe de règles qui autorise explicitement la requête bloquée. Lorsque vous créez la règle, vous pouvez définir votre propre liste de domaines avec uniquement la spécification de domaine que vous souhaitez autoriser. Suivez les instructions relatives à la gestion des règles et groupes de règles dans Création d'un groupe de règles et de règles.
3. Définissez la priorité de la nouvelle règle au sein du groupe de règles afin qu'elle s'exécute avant la règle qui utilise la liste de domaines gérée. Pour ce faire, donnez à la nouvelle règle un paramètre de priorité numérique inférieur.

Une fois que vous avez mis à jour votre groupe de règles, la nouvelle règle autorise explicitement le nom de domaine que vous souhaitez autoriser avant l'exécution de la règle de blocage.

Configuration de la journalisation du pare-feu DNS

Vous pouvez évaluer les règles de votre pare-feu DNS à l'aide CloudWatch des métriques Amazon et des journaux de requêtes du Resolver. Les journaux fournissent le nom de la liste de domaines pour toutes les alertes et actions de blocage. Pour plus d'informations sur Amazon CloudWatch, consultezSurveillance des groupes de règles du pare-feu DNS Route 53 Resolver avec Amazon CloudWatch.

Lorsque vous activez le pare-feu DNS, que vous l'associez à un VPC et que la journalisation est activée, `firewall_rule_group_id`, `firewall_rule_action` et `firewall_domain_list_id` sont les champs spécifiques au pare-feu DNS fournis dans vos journaux.

> **Note**
>
> Les journaux de requêtes afficheront les champs supplémentaires du pare-feu DNS pour uniquement les requêtes bloquées par les règles du pare-feu DNS.

Pour commencer à enregistrer les requêtes DNS filtrées par les règles de pare-feu DNS qui proviennent de votre VPCs, vous devez effectuer les tâches suivantes dans la console Amazon Route 53 :

Pour configurer la journalisation des requêtes Resolver pour le pare-feu DNS

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Développez le menu de la console Route 53. Dans le coin supérieur gauche de la console, sélectionnez l'icone des trois barres horizontales

   (≡
3. Dans le menu Resolver, choisissez Query logging (Journalisation des requêtes).
4. Dans le sélecteur de région, choisissez la AWS région dans laquelle vous souhaitez créer la configuration de journalisation des requêtes.

   Il doit s'agir de la même région dans laquelle vous avez créé la VPCs région associée au pare-feu DNS pour laquelle vous souhaitez enregistrer les requêtes. Si vous avez plusieurs VPCs régions, vous devez créer au moins une configuration de journalisation des requêtes pour chaque région.
5. Choisissez Configure query logging (Configurer la journalisation des requêtes).
6. Indiquez l'une des valeurs suivantes :

   Nom de la configuration de journalisation des requêtes

   Saisissez un nom pour votre configuration de journalisation des requêtes. Le nom s'affiche dans la console, dans la liste des configurations de journalisation des requêtes. Saisissez un nom qui vous aidera à retrouver la configuration plus tard.

   Destination des journaux de requête

   Choisissez le type de AWS ressource à laquelle Resolver doit envoyer les journaux de requêtes. Pour plus d'informations sur le choix entre les options (groupe de CloudWatch

journaux, compartiment S3 et flux de diffusion Firehose), consultez. AWS ressources auxquelles vous pouvez envoyer les journaux de requêtes du résolveur

Après avoir choisi le type de ressource, vous pouvez créer une autre ressource de ce type ou choisir une ressource existante créée par le AWS compte courant.

> **Note**
>
> Vous pouvez uniquement choisir uniquement les ressources qui ont été créées dans la région AWS que vous avez choisie à l'étape 4, c'est-à-dire la région dans laquelle vous créez la configuration de journalisation des requêtes. Si vous choisissez de créer une nouvelle ressource, celle-ci sera créée dans la même région.

VPCs pour enregistrer les requêtes pour

Cette configuration d'enregistrement des requêtes enregistrera les requêtes DNS qui proviennent du fichier VPCs que vous avez choisi. Cochez la case correspondant à chaque VPC de la région actuelle pour laquelle vous souhaitez que Resolver journalise les requêtes, puis sélectionnez Choose (Choisir).

> **Note**
>
> La diffusion des journaux VPC ne peut être activée qu'une seule fois pour un type de destination spécifique. Les journaux ne peuvent pas être diffusés vers plusieurs destinations du même type. Par exemple, les journaux VPC ne peuvent pas être diffusés vers deux destinations Amazon S3.

7. Choisissez Configure query logging (Configurer la journalisation des requêtes).

> **Note**
>
> Vous devriez commencer à voir ces requêtes DNS exécutées par les ressources de votre VPC dans les journaux quelques minutes après avoir créé avec succès la configuration de journalisation.

Partage des groupes de règles du pare-feu DNS Route 53 Resolver entre les comptes AWS

Vous pouvez partager des groupes de règles de pare-feu DNS entre AWS des comptes. Pour partager des groupes de règles, vous utilisez AWS Resource Access Manager (AWS RAM). La console DNS Firewall s'intègre à la AWS RAM console. Pour plus d'informations AWS RAM, consultez le guide de l'utilisateur de Resource Access Manager.

Remarques :

Associer des groupes de règles partagés à VPCs

Si un autre AWS compte partage un groupe de règles avec le vôtre, vous pouvez l'associer au vôtre de VPCs la même manière que vous associez les groupes de règles que vous avez créés. Pour de plus amples informations, veuillez consulter Gestion des associations entre votre VPC et le groupe de règles Route 53 Resolver DNS Firewall.

Suppression ou annulation du partage d'un groupe de règles

Si vous partagez un groupe de règles avec d'autres comptes, puis que vous supprimez le groupe de règles ou arrêtez de le partager, le pare-feu DNS supprime toutes les associations créées par les autres comptes entre le groupe de règles et le leur VPCs.

Paramètres maximaux pour les groupes de règles et les associations

Les groupes de règles partagés et leurs associations avec eux VPCs sont inclus dans le décompte des comptes avec lesquels les groupes de règles sont partagés.

Pour obtenir les quotas de pare-feu DNS actuels, consultez Quotas sur le pare-feu DNS Route 53 Resolver.

Autorisations

Pour partager un groupe de règles avec un autre AWS compte, vous devez être autorisé à utiliser l'PutFirewallRuleGroupPolicyaction.

Restrictions relatives au AWS compte avec lequel un groupe de règles est partagé

Le compte avec lequel un groupe de règles est partagé ne peut pas modifier ou supprimer le groupe de règles.

Identification

Seul le compte qui a créé un groupe de règles peut ajouter, supprimer ou consulter les identifications du groupe de règles.

Pour consulter le statut de partage actuel d'un groupe de règles (y compris le compte qui a partagé le groupe de règles ou le compte avec lequel un groupe de règles est partagé) et partager des groupes de règles avec un autre compte, suivez la procédure suivante.

Pour consulter l'état du partage et partager des groupes de règles avec un autre AWS compte

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation, sélectionnez Groupes de règles.
3. Dans la barre de navigation, choisissez la région dans laquelle vous avez créé le groupe de règles.

   La colonne Sharing status (Statut de partage) affiche le statut de partage actuel des groupes de règles qui ont été créés par le compte actuel ou qui sont partagés avec le compte actuel :

   - Non partagé : le AWS compte actuel a créé le groupe de règles, qui n'est partagé avec aucun autre compte.
   - Shared by me (Partagé par moi) : le compte actuel a créé le groupe de règles et l'a partagé avec un ou plusieurs comptes.
   - Shared with me (Partagé avec moi) : un autre compte a créé le groupe de règles et l'a partagé avec le compte actuel.
4. Choisissez le nom du groupe de règles dont vous souhaitez afficher les informations de partage ou que vous souhaitez partager avec un autre compte.

   Sur la `rule group name` page Groupe de règles :, la valeur sous Propriétaire affiche l'ID du compte qui a créé le groupe de règles. Il s'agit du compte actuel, à moins que la valeur Sharing status (Statut de partage) soit Shared with me (Partagée avec moi). Dans ce cas, Owner (Propriétaire) désigne le compte qui a créé le groupe de règles et l'a partagé avec le compte actuel.
5. Choisissez Share (Partager) pour afficher des informations supplémentaires ou pour partager le groupe de règles avec un autre compte. Une page s'affiche dans la AWS RAM console, en fonction de la valeur de l'état du partage :

- Not shared (Non partagé) : la page Create resource share (Créer partage de ressource) s'affiche. Pour plus d'informations sur le partage du groupe de règles avec un autre compte, une unité d'organisation (UO) ou une organisation, passez à l'étape suivante.
- Shared by me (Partagé par moi) : la page Shared resources (Ressources partagées) affiche les groupes de règles et autres ressources qui sont détenus par le compte actuel et partagés avec d'autres comptes.
- Shared with me (Partagé avec moi) : la page Shared resources (Ressources partagées) affiche les groupes de règles et autres ressources qui sont détenus par d'autres comptes et partagés avec le compte actuel.

6. Pour partager un groupe de règles avec un autre AWS compte, unité d'organisation ou organisation, spécifiez les valeurs suivantes.

> **Note**
>
> Vous ne pouvez pas mettre à jour les paramètres de partage. Pour modifier les paramètres suivants, vous devez repartager un groupe de règles avec les nouveaux paramètres, puis supprimer les anciens paramètres de partage.

Description

Saisissez une courte description qui vous aide à vous rappeler les raisons pour lesquelles vous avez partagé le groupe de règles.

Ressources

Cochez la case correspondant au groupe de règles à partager.

Principaux

Entrez le numéro de AWS compte, le nom de l'unité d'organisation ou le nom de l'organisation.

Balises

Spécifiez une ou plusieurs clés et les valeurs correspondantes. Par exemple, vous pouvez indiquer Cost center (Centre de coûts) pour Key (Clé) et 456 pour Value (Valeur).

Ce sont les étiquettes qui AWS Billing and Cost Management permettent d'organiser votre AWS facture ; vous pouvez également les utiliser à d'autres fins. Pour en savoir plus

sur l'utilisation des identifications pour la répartition des coûts, consultez Utilisation des identifications de répartition des coûts dans le Guide de l'utilisateur AWS Billing .

Activation des protections Route 53 Resolver DNS Firewall pour votre VPC

Vous activez les protections de pare-feu DNS pour votre VPC en associant un ou plusieurs groupes de règles au VPC. Chaque fois qu'un VPC est associé à un groupe de règles de pare-feu DNS, Route 53 Resolver fournit les protections de pare-feu DNS suivantes :

- Resolver achemine les requêtes DNS sortantes du VPC via le pare-feu DNS, et ce dernier filtre les requêtes à l'aide des groupes de règles associés.
- Resolver applique les paramètres dans la configuration du pare-feu DNS du VPC.

Pour fournir des protections de pare-feu DNS à votre VPC, procédez comme suit :

- Créez et gérez des associations entre vos groupes de règles de pare-feu DNS et votre VPC. Pour de plus amples informations sur les groupes de règles, reportez-vous à la section Règles et groupes de règles de pare-feu DNS.
- Configurez la manière dont vous souhaitez que Resolver gère les requêtes DNS pour le VPC en cas d'échec, par exemple si le pare-feu DNS ne fournit pas de réponse pour une requête DNS.

Gestion des associations entre votre VPC et le groupe de règles Route 53 Resolver DNS Firewall

Pour afficher les associations VPC d'un groupe de règles

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.

   Choisissez Pare-feu DNS dans le volet de navigation pour ouvrir la page des groupes de règles de pare-feu DNS sur la console Amazon VPC.

   - OU -

   Connectez-vous au AWS Management Console et ouvrez-le

la console Amazon VPC située sous. https://console.aws.amazon.com/vpc/

2. Dans le volet de navigation, sous Pare-feu DNS, choisissez Groupes de règles.
3. Dans la barre de navigation, choisissez la région pour le groupe de règles.
4. Sélectionnez le groupe de règles que vous souhaitez associer.
5. Sélectionnez Afficher les détails. La page du groupe de règles s'affiche.
6. Vers le bas, vous pouvez voir une zone de détails à onglets qui inclut les règles et les informations associées VPCs. Choisissez l'onglet Associé VPCs.

Pour associer un groupe de règles à un VPC

1. Recherchez les associations VPC du groupe de règles en suivant les instructions de la procédure précédente Pour afficher les associations VPC d'un groupe de règles.
2. Dans l' VPCsonglet Associé, choisissez Associate VPC.
3. Recherchez le VPC que vous souhaitez associer au groupe de règles dans la liste déroulante. Sélectionnez-le, puis choisissez Associate (Associer).

Sur la page du groupe de règles, votre VPC est répertorié dans l'onglet VPCsAssocié. Dans un premier temps, le Status (Statut) de l'association indique Updating (Mise à jour en cours). Une fois l'association terminée, le statut passe à Complete (Terminée).

Pour supprimer une association entre un groupe de règles et un VPC

1. Recherchez les associations VPC du groupe de règles en suivant les instructions de la procédure précédente Pour afficher les associations VPC d'un groupe de règles.
2. Sélectionnez le VPC que vous souhaitez supprimer de la liste, puis choisissez Disassociate (Dissocier). Vérifiez, puis confirmez l'action.

Sur la page du groupe de règles, votre VPC est répertorié dans l' VPCsonglet Associé avec le statut Dissociation. Une fois l'opération terminée, le pare-feu DNS met à jour la liste pour supprimer le VPC.

Configuration de VPC du pare-feu DNS

La configuration du pare-feu DNS pour votre VPC détermine si Route 53 Resolver autorise ou bloque les requêtes lors d'échecs, par exemple lorsque le pare-feu DNS est altéré, ne répond pas, ou est

indisponible dans la zone. Resolver applique la configuration du pare-feu d'un VPC chaque fois que vous avez un ou plusieurs groupes de règles de pare-feu DNS associés au VPC.

Vous pouvez configurer un VPC pour qu'il échoue et reste ouvert ou qu'il échoue et se ferme.

- Par défaut, le mode d'échec est fermé, ce qui signifie que Resolver bloque toutes les requêtes pour lesquelles il ne reçoit pas de réponse du pare-feu DNS et envoie une `SERVFAIL` réponse DNS. Cette approche favorise la sécurité au détriment de la disponibilité.
- Si vous activez l'ouverture en cas d'échec, Resolver autorise les requêtes à passer s'il ne reçoit pas de réponse du pare-feu DNS. Cette approche favorise la disponibilité au détriment de la sécurité.

Pour modifier la configuration du pare-feu DNS pour un VPC (console)

1. Connectez-vous à la console Resolver AWS Management Console et ouvrez-la à https://console.aws.amazon.com/route53resolver/l'adresse.
2. Dans le volet de navigation, sous Résolveurs, choisissez VPCs.
3. Dans la VPCspage, localisez et modifiez le VPC. Modifiez la configuration du pare-feu DNS pour qu'il échoue et reste ouvert ou qu'il échoue et se ferme, selon vos besoins.

Pour modifier le comportement du pare-feu DNS pour un VPC (API)

- Mettez à jour la configuration de votre pare-feu VPC en appelant UpdateFirewallConfiget en activant ou en désactivant. `FirewallFailOpen`

Vous pouvez récupérer une liste de vos configurations de pare-feu VPC via l'API en appelant. ListFirewallConfigs

Que sont les profils Amazon Route 53 ?

Avec les profils Route 53, vous pouvez appliquer et gérer des configurations Route 53 liées au DNS dans de nombreuses VPCs configurations différentes. Comptes AWS Les profils permettent de gérer les paramètres DNS pour de nombreuses personnes VPCs aussi facilement que de les gérer pour un seul VPC. Lorsque vous mettez à jour un profil, ses paramètres sont propagés à tous les utilisateurs VPCs associés au profil. Vous pouvez également partager un profil Comptes AWS dans les mêmes régions en utilisant AWS RAM. Les ressources actuellement prises en charge par Route 53 que vous pouvez associer à un profil sont les suivantes :

- Les zones hébergées privées et les paramètres qui y sont spécifiés. Pour plus d'informations sur l'utilisation de zones hébergées privées, consultezUtilisation des zones hébergées privées.
- Règles du résolveur Route 53, à la fois pour le transfert et pour le système. Pour plus d'informations sur les règles du résolveur, consultezGestion des règles de réacheminement.
- Groupes de règles du pare-feu DNS. Pour plus d'informations sur les groupes de règles du pare-feu DNS, consultezRègles et groupes de règles de pare-feu DNS.
- Points de terminaison VPC d'interface. Pour plus d'informations sur les points de terminaison VPC d'interface, consultez la section Points de terminaison VPC d'interface dans le guide de l'utilisateur Amazon VPC.

Certaines configurations VPC sont directement gérées sur le profil. Les configurations sont les suivantes :

- Configuration de recherche DNS inversée pour les règles du résolveur.
- Configuration du mode de défaillance du pare-feu DNS.
- Configuration de validation DNSSEC.

Par exemple, vous pouvez activer la configuration du mode de défaillance du pare-feu DNS pour tous les éléments auxquels VPCs le profil est associé, tout en conservant la configuration de validation DNSSEC existante du VPC.

> **Important**
>
> Une fois que vous avez activé les paramètres de profil pour les configurations précédentes et que vous associez le profil à un VPC, les paramètres de profil prennent effet immédiatement.

Vous pouvez également l'utiliser AWS CloudFormation pour configurer des paramètres DNS cohérents pour les nouveaux approvisionnements. VPCs

Vous pouvez associer un profil par VPC et le nombre de ressources que vous pouvez associer par profil varie. Pour de plus amples informations, veuillez consulter Quotas sur les profils de la Route 53 .

Comment les paramètres du profil Route 53 sont hiérarchisés

Vous pouvez définir les paramètres DNS locaux et les associations pour les profils à des fins de migration ou à d'autres fins de test. Lorsqu'une requête DNS correspond à la fois à la règle du résolveur pour une zone hébergée privée directement associée au VPC et à une règle du résolveur pour une zone hébergée privée associée au profil, les paramètres DNS locaux ont priorité. Lorsqu'une requête DNS est effectuée pour un nom de domaine en conflit, le nom le plus spécifique gagne. Le tableau suivant contient des exemples de l'ordre d'évaluation :

requête DNS	Règle de profil	Règle VPC	Règle évaluée
example.com	example.com	example.com	VPC local
test.exemple.com	test.exemple.com	example.com	Profil
marketing.exemple.com	Aucun	marketing.exemple.com	VPC local

Route 53 Profils | Disponibilité des régions

Pour connaître la disponibilité de la région et les points de terminaison, consultez la section Points de terminaison de service pour Route 53 dans le guide de référence AWS général.

Étapes de haut niveau pour l'utilisation des profils Route 53

Pour implémenter les profils Amazon Route 53 dans votre Amazon Virtual Private Cloud VPCs, vous devez suivre les étapes de haut niveau suivantes.

1. Créer un profil vide — La première étape consiste à créer un profil vide auquel vous pouvez associer des ressources DNS. Pour de plus amples informations, veuillez consulter Création de profils Route 53.
2. Associer des ressources DNS au profil — Les ressources que vous pouvez actuellement associer à un profil sont les zones hébergées privées, les règles du résolveur Route 53, à la fois le transfert et le système, les groupes de règles du pare-feu DNS et les points de terminaison VPC d'interface. Pour plus d'informations, consultez Associer des groupes de règles de pare-feu DNS à un profil Route 53, Associer des zones hébergées privées à un profil Route 53, Associer les règles du résolveur à un profil Route 53 et Associer les points de terminaison VPC de l'interface à un profil Route 53.
3. Configurer certains paramètres VPC pour le profil — Certains paramètres DNS, tels que les zones hébergées associées au profil, sont appliqués immédiatement au VPCs . Pour les configurations de validation DNSSEC, de recherche DNS inversée par le résolveur et de mode de défaillance du pare-feu DNS, vous pouvez choisir l'une des options suivantes :
   - Pour la validation DNSSEC, vous pouvez choisir d'utiliser la configuration VPC locale (par défaut), d'activer la validation ou de désactiver la validation pour tous les éléments VPCs associés au profil.
   - Pour la configuration de la recherche DNS inversée par Resolver, vous pouvez l'activer, la désactiver ou utiliser les règles définies automatiquement pour le VPC localement (par défaut).
   - Pour la configuration du mode de défaillance du pare-feu DNS, vous pouvez l'activer, le désactiver ou utiliser la configuration du mode de défaillance définie pour le VPC localement (par défaut).

   Pour de plus amples informations, veuillez consulter Modifier les configurations du profil Route 53.
4. Associer le profil à un ou plusieurs VPCs : pour commencer à utiliser votre profil, associez-le à un ou plusieurs VPCs. Pour de plus amples informations, veuillez consulter Associer un profil Route 53 à VPCs.

Création de profils Route 53

Pour créer des profils Route 53, suivez les instructions de cette rubrique. Choisissez un onglet pour créer un profil Route 53 à l'aide de la console Route 53, ou AWS CLI.

- Console
- INTERFACE DE LIGNE DE COMMANDE (CLI)

Console

Pour créer un profil Route 53

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation, sélectionnez Profiles.
3. Dans la barre de navigation, choisissez la région dans laquelle vous souhaitez créer le profil.
4. Entrez un nom pour le profil, ajoutez éventuellement des balises, puis choisissez Create Profile.

   Cela crée un profil vide avec des configurations par défaut auxquelles vous pouvez associer des ressources. Après avoir associé des ressources au profil, vous pouvez l'associer à un certain nombre de VPCs et modifier la façon dont certaines configurations du résolveur s'appliquent au VPCs.

CLI

Vous pouvez créer un profil en exécutant une AWS CLI commande comme celle-ci et en utilisant votre propre valeur pourname.

```
aws route53profiles create-profile --name test
```

Voici un exemple de sortie après l'exécution de la commande :

```
{
    "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"
    }
}
```

Pour associer vos profils à différentes ressources et modifier les configurations VPC du profil, consultez les procédures suivantes :

Rubriques

- Associer des groupes de règles de pare-feu DNS à un profil Route 53
- Associer des zones hébergées privées à un profil Route 53
- Associer les règles du résolveur à un profil Route 53
- Associer les points de terminaison VPC de l'interface à un profil Route 53
- Modifier les configurations du profil Route 53
- Associer un profil Route 53 à VPCs

Associer des groupes de règles de pare-feu DNS à un profil Route 53

Pour obtenir des instructions sur la création d'un groupe de règlesCréation d'un groupe de règles et de règles, consultez, puis choisissez un onglet pour associer des groupes de règles de pare-feu DNS à un profil Route 53 à l'aide de la console Route 53, ou AWS CLI.

- Console
- INTERFACE DE LIGNE DE COMMANDE (CLI)

Console

Pour associer des groupes de règles de pare-feu DNS

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans la barre de navigation, choisissez la région dans laquelle vous avez créé le profil.
3. Dans le volet de navigation, sélectionnez Profils, puis dans le tableau Profils, choisissez le nom lié du profil avec lequel vous souhaitez travailler.
4. Sur la <Profile name>page, choisissez l'onglet Groupes de règles du pare-feu DNS, puis Associer.
5. Dans la section Groupes de règles du pare-feu DNS, vous pouvez sélectionner jusqu'à 10 groupes de règles que vous avez créés précédemment. Si vous souhaitez associer plus de 10 groupes de règles, utilisez le APIs. Pour de plus amples informations, veuillez consulter AssociateResourceToProfile.

Pour créer de nouveaux groupes de règles, voirCréation d'un groupe de règles et de règles.

6. Choisissez Suivant.
7. Sur la page Définir la priorité, vous pouvez définir l'ordre dans lequel les groupes de règles sont traités en cliquant sur le numéro de priorité préattribué et en saisissant un nouveau. Les valeurs autorisées pour la priorité sont comprises entre 100 et 9 900.

   Les groupes de règles sont évalués en commençant par le paramètre de priorité numérique le plus bas et en augmentant progressivement. Vous pouvez modifier la priorité d'un groupe de règles à tout moment, par exemple pour modifier l'ordre de traitement ou libérer de la place pour d'autres groupes de règles.

   Sélectionnez Envoyer.
8. La progression de l'association est affichée dans la colonne État de la boîte de dialogue des groupes de règles du pare-feu DNS.

CLI

Vous pouvez associer un groupe de règles à un profil en exécutant une AWS CLI commande comme celle-ci et en utilisant vos propres valeurs pour `name` `profile-id``resource-arn`, et `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}"
```

Voici un exemple de sortie après l'exécution de la commande :

```
{
    "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"
    }
}
```

Associer des zones hébergées privées à un profil Route 53

Pour obtenir des instructions sur la création d'une zone hébergée privée, consultezCréation d'une zone hébergée privée, puis suivez les étapes de cette procédure pour associer une zone hébergée privée à un profil.

Pour associer des zones hébergées privées

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans la barre de navigation, choisissez la région dans laquelle vous avez créé le profil.
3. Dans le volet de navigation, sélectionnez Profils, puis dans le tableau Profils, choisissez le nom lié du profil avec lequel vous souhaitez travailler.
4. Sur la <Profile name>page, choisissez l'onglet Zones hébergées privées, puis Associer.
5. Sur la page Associer des zones hébergées privées, vous pouvez sélectionner jusqu'à 10 zones hébergées privées que vous avez créées précédemment. Si vous souhaitez associer plus de 10 zones hébergées privées, utilisez le APIs. Pour de plus amples informations, veuillez consulter AssociateResourceToProfile.

   Pour créer des zones hébergées privées, voirCréation d'une zone hébergée privée.
6. Choisissez Associer
7. La progression de l'association est affichée dans la colonne État de l'onglet Zones hébergées privées.

Associer les règles du résolveur à un profil Route 53

Pour savoir comment créer une règle de résolution, consultezCréer des règles de réacheminement, puis suivez les étapes de cette procédure pour associer des règles de résolution à un profil.

Pour associer les règles du résolveur

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans la barre de navigation, choisissez la région dans laquelle vous avez créé le profil.
3. Sur la <Profile name>page, choisissez l'onglet Règles du résolveur, puis Associer.
4. Sur la page Règles du résolveur associé, dans le tableau des règles du résolveur, vous pouvez sélectionner jusqu'à 10 règles du résolveur que vous avez créées précédemment. Si vous souhaitez associer plus de 10 règles de résolution, utilisez le APIs. Pour de plus amples informations, veuillez consulter AssociateResourceToProfile.

   Pour créer des règles de résolution, voirCréer des règles de réacheminement.
5. Choisissez Associer
6. La progression de l'association est affichée dans la colonne État de l'onglet Règles du résolveur.

Associer les points de terminaison VPC de l'interface à un profil Route 53

Pour obtenir des instructions sur la création d'un point de terminaison VPC d'interface, consultez la section Créer un point de terminaison VPC dans le guide de l'utilisateur VPC. puis suivez les étapes de cette procédure pour associer un point de terminaison VPC à un profil.

Pour associer des points de terminaison VPC

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans la barre de navigation, choisissez la région dans laquelle vous avez créé le profil.
3. Sur la page, choisissez l'onglet Points de terminaison VPC, puis Associer. <Profile name>
4. Sur la page Associer les points de terminaison VPC, dans le tableau des points de terminaison VPC, vous pouvez sélectionner jusqu'à 10 points de terminaison que vous avez créés précédemment. Si vous souhaitez associer plus de 10 points de terminaison, utilisez le APIs. Pour de plus amples informations, veuillez consulter AssociateResourceToProfile.

   Pour créer des règles de résolution, voirCréer des règles de réacheminement.
5. Choisissez Associer
6. La progression de l'association est affichée dans la colonne État de l'onglet Points de terminaison du VPC.

Modifier les configurations du profil Route 53

Après avoir associé des ressources à un profil, vous pouvez modifier les configurations VPC par défaut pour décider de la manière dont elles sont appliquées au. VPCs

Pour modifier les configurations de profil

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans la barre de navigation, choisissez la région dans laquelle vous avez créé le profil.
3. Dans le volet de navigation, sélectionnez Profils, puis dans le tableau Profils, choisissez le nom lié du profil avec lequel vous souhaitez travailler.
4. Sur la <Profile name>page, choisissez l'onglet Configuration, puis Modifier.
5. Sur la page Modifier la configuration, choisissez l'une des valeurs pour la configuration DNSSEC VPC, la configuration de recherche DNS inversée du résolveur et la configuration du mode de défaillance du pare-feu DNS.

   Pour plus d'informations sur les valeurs, consultezParamètres de configuration pour le profil Route 53.
6. Choisissez Mettre à jour.

Paramètres de configuration pour le profil Route 53

Lorsque vous modifiez une configuration de profil Route 53, vous spécifiez les valeurs suivantes :

Configuration du DNSSEC

Choisissez l’une des valeurs suivantes :

- Utiliser la configuration DNSSEC VPC locale (par défaut)

  Choisissez cette option pour que toutes les entités VPCs associées à ce profil conservent leur configuration de validation DNSSEC locale.
- Activer la validation DNSSEC

  Choisissez cette option pour activer la validation DNSSEC dans tous les éléments VPCs associés à ce profil.
- Désactiver la validation DNSSEC

Choisissez cette option pour désactiver la validation DNSSEC dans tous les VPCs éléments associés à ce profil.

Configuration de la recherche DNS inversée par le résolveur

Choisissez l'une des valeurs suivantes :

- Activer

  Choisissez cette option pour créer des règles définies automatiquement pour la recherche DNS inversée dans tous les fichiers associés VPCs.

- Non activé

  Choisissez cette option pour ne pas créer de règles définies automatiquement pour la recherche DNS inversée dans tous les fichiers associés VPCs.

- Utiliser les règles autodéfinies locales (valeur par défaut)

  Choisissez cette option pour utiliser les paramètres VPC locaux pour la recherche DNS inversée pour le DNS associé. VPCs

Configuration du mode de défaillance du pare-feu DNS

Choisissez l'une des valeurs suivantes :

- Désactiver

  Choisissez cette option pour fermer le mode d'échec du pare-feu DNS pour le système associé VPCs. Avec cette option, le pare-feu DNS bloquera toutes les requêtes qu'il ne peut pas évaluer correctement.

- Enabled

  Choisissez cette option pour que le mode de défaillance du pare-feu DNS reste ouvert pour tous les éléments associés VPCs. Avec cette option, le pare-feu DNS autorise le traitement des requêtes s'il n'est pas en mesure de les évaluer correctement.

- Utiliser les paramètres du mode de défaillance local (par défaut)

  Choisissez cette option pour utiliser les paramètres du mode de défaillance du pare-feu DNS VPC local.

Pour plus d'informations sur les configurations, voir

- Activation de la validation DNSSEC dans Amazon Route 53
- Règles de transfert pour les requêtes DNS inverses dans Resolver
- Configuration de VPC du pare-feu DNS

Associer un profil Route 53 à VPCs

Pour associer un profil Route 53 à un VPC, suivez les instructions de cette rubrique. Choisissez un onglet pour associer un profil Route 53 à un VPC à l'aide de la console Route 53, ou. AWS CLI

- Console
- INTERFACE DE LIGNE DE COMMANDE (CLI)

Console

Pour associer VPCs

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans la barre de navigation, choisissez la région dans laquelle vous avez créé le profil.
3. Sur la <Profile name>page, choisissez l'VPCsonglet, puis Associer.
4. Sur la VPCs page Associer, vous pouvez sélectionner jusqu'à 10 VPCs que vous avez déjà créés. Si vous souhaitez en associer plus de 10 VPCs, utilisez le APIs. Pour de plus amples informations, veuillez consulter AssociateProfile.
5. Choisissez Associer
6. La progression de l'association est affichée dans la colonne État de la VPCspage.

CLI

Vous pouvez répertorier les profils en exécutant une AWS CLI commande comme celle-ci et en utilisant vos propres valeurs pour `nameprofile-id`, et `resource-id` :

```
aws route53profiles associate-profile --name test-association --profile-id rp-4987774726example --resource-id vpc-0af3b96b3example
```

Voici un exemple de sortie après l'exécution de la commande :

```
{
    "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"
    }
}
```

Afficher et mettre à jour les profils Amazon Route 53

Choisissez l'onglet console pour afficher et modifier le profil Route 53. Choisissez l'onglet CLI à utiliser AWS CLI pour répertorier les profils que vous possédez, que vous partagez ou que vous partagez avec vous.

- Console
- INTERFACE DE LIGNE DE COMMANDE (CLI)

Console

Affichage et mise à jour des profils Route 53

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation, sélectionnez Profiles.
3. Sélectionnez le bouton à côté du nom du profil que vous souhaitez consulter ou modifier.
4. Sur <Profile name>cette page, vous pouvez afficher les ressources DNS actuellement associées, en associer de nouvelles et modifier les balises et les configurations VPC.

CLI

Vous pouvez répertorier les profils en exécutant une AWS CLI commande comme celle-ci :

```
aws route53profiles list-profiles
```

Voici un exemple de sortie après l'exécution de la commande :

```
{
    "ProfileSummaries": [
        {
            "Arn": "arn:aws:route53profiles:us-east-1:123456789012:profile/
rp-4987774726example",
            "Id": "rp-4987774726example",
            "Name": "test",
            "ShareStatus": "NOT_SHARED"
        }
    ]
}
```

Vous pouvez obtenir des informations sur un VPS particulier auquel le profil est associé en exécutant une AWS CLI commande comme celle-ci et en utilisant votre propre valeur pour `profile-association-id` :

```
aws route53profiles get-profile-association --profile-association-id
rpassoc-489ce212fexample
```

Voici un exemple de sortie après l'exécution de la commande :

```
   "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"
    }   ]
}
```

Supprimer un profil Amazon Route 53

Choisissez un onglet pour supprimer un profil Route 53 à l'aide de la console Route 53, ou AWS CLI.

- Console
- INTERFACE DE LIGNE DE COMMANDE (CLI)

Console

Pour supprimer un profil Route 53

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation, sélectionnez Profiles.
3. Sélectionnez le bouton à côté du nom du profil que vous souhaitez supprimer, puis choisissez Supprimer.

> **Important**
>
> Vous ne pouvez pas supprimer un profil s'il est associé à VPCs. De plus, si le profil est partagé avec une autre Compte AWS personne, toutes VPCs les configurations auxquelles les configurations du profil sont associées perdront ces configurations.

4. Dans la <Profile name>boîte de dialogue Supprimer, tapez**`confirm`**, puis choisissez Supprimer.

CLI

> **Important**
>
> Vous ne pouvez pas supprimer un profil s'il est associé à VPCs. De plus, si le profil est partagé avec une autre Compte AWS personne, toutes VPCs les configurations auxquelles les configurations du profil sont associées perdront ces configurations.

Vous pouvez supprimer un profil en exécutant une AWS CLI commande comme celle-ci et en utilisant votre propre valeur pour `profile-id` :

```
aws route53profiles delete-profile --profile-id rp-6ffe47d5example
```

Voici un exemple de sortie après l'exécution de la commande :

```
{
    "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"
    }
}
```

Afficher et mettre à jour les ressources Route 53 associées à un profil Amazon Route 53

Choisissez l'onglet console pour afficher les associations de ressources du profil Route 53 et modifiez éventuellement la priorité du groupe de règles du pare-feu DNS. Choisissez l'onglet CLI AWS CLI à utiliser pour répertorier les associations de ressources et pour voir un exemple de mise à jour d'une priorité d'un groupe de règles de pare-feu DNS.

- Console
- INTERFACE DE LIGNE DE COMMANDE (CLI)

Console

Pour afficher et mettre à jour les ressources associées à un profil

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation, sélectionnez Profiles.

3. Dans la barre de navigation, choisissez la région dans laquelle vous avez créé le profil.
4. Sélectionnez le bouton à côté du nom du profil pour lequel vous souhaitez afficher ou modifier les associations de ressources.
5. Sur la <Profile name>page, choisissez l'onglet correspondant à la ressource que vous souhaitez afficher ou modifier, qu'il s'agisse de groupes de règles de pare-feu DNS, de zones hébergées privées, de règles de résolution ou de points de terminaison VPC.
6. Sur l'onglet d'une ressource, vous pouvez afficher les noms, l'ARN et le statut des ressources associées. Vous pouvez également choisir l'icône représentant une roue dentée pour ajuster ce qui est affiché dans le tableau des ressources.

   Sur la page de l'onglet Groupes de règles du pare-feu DNS, vous pouvez également choisir l'entrée prioritaire du groupe de règles et la modifier en un nombre plus petit ou plus grand. Les groupes de règles sont évalués dans l'ordre en commençant par le numéro de priorité le plus bas jusqu'au numéro de priorité le plus élevé.

CLI

Vous pouvez répertorier les ressources associées à un profil en exécutant une AWS CLI commande comme celle-ci et en utilisant votre propre valeur pour `profile-id` :

```
aws route53profiles list-profile-resource-associations --profile-id
rp-4987774726example
```

Voici un exemple de sortie après l'exécution de la commande :

```
{
    "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"
        }
    ]
}
```

Vous pouvez mettre à jour la priorité d'un groupe de règles de pare-feu DNS associé à un profil en exécutant une AWS CLI commande comme celle-ci, en utilisant votre propre valeur pour et en utilisant vos propres valeurs pour `profile-resource-association-id` et `--resource-properties` :

```
aws route53profiles update-profile-resource-association --profile-
resource-association-id rpr-001913120a7example --resource-properties
"{\"priority\": 105}"
```

Voici un exemple de sortie après l'exécution de la commande :

```
{
    "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"
    }
}
```

Dissociation d'une ressource d'un profil Amazon Route 53

Avant de supprimer un profil, vous devez dissocier toutes les ressources de celui-ci.

Pour dissocier une ressource associée à un profil Route 53

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation, sélectionnez Profiles.
3. Dans la barre de navigation, choisissez la région dans laquelle le profil à partir duquel vous souhaitez dissocier une ressource a été créé.
4. Sélectionnez le bouton à côté du nom du profil dont vous souhaitez dissocier une ressource.
5. Sur la <Profile name>page, choisissez l'onglet correspondant à la ressource que vous souhaitez supprimer, qu'il s'agisse de groupes de règles de pare-feu DNS, de zones hébergées privées, de règles de résolution ou de points de terminaison VPC.
6. Sur l'onglet de la ressource, choisissez la ressource que vous souhaitez dissocier, puis Dissocier.
7. Dans la boîte de dialogue Dissocier les ressources, tapez**`confirm`**, puis choisissez Dissocier.

Affichage VPCs associé à un profil Amazon Route 53

Choisissez l'onglet console pour afficher et modifier le profil Route 53 vers les associations VPC. Choisissez l'onglet CLI à utiliser pour AWS CLI répertorier les associations entre le profil et le VPC, ou pour obtenir des informations sur une association spécifique

- Console
- INTERFACE DE LIGNE DE COMMANDE (CLI)

Console

Pour afficher les VPCs informations associées à un profil

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation, sélectionnez Profiles.
3. Dans la barre de navigation, choisissez la région dans laquelle vous avez créé le profil.
4. Sélectionnez le bouton à côté du nom du profil dont vous souhaitez afficher le profil associé VPCs.

5. Sur la <Profile name>page, choisissez l'VPCsonglet.
6. Sur la page de l'onglet, VPCs vous pouvez afficher les noms, l'ARN et le statut des entités associées VPCs.

CLI

Vous pouvez répertorier VPCs les profils auxquels le profil est associé en exécutant une AWS CLI commande comme celle-ci :

```
aws route53profiles list-profile-associations
```

Voici un exemple de sortie après l'exécution de la commande :

```
{
    "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"
        }
    ]
}
```

Vous pouvez obtenir des informations sur un VPS particulier auquel le profil est associé en exécutant une AWS CLI commande comme celle-ci et en utilisant votre propre valeur pour `profile-association-id` :

```
aws route53profiles get-profile-association --profile-association-id
rpassoc-489ce212fexample
```

Voici un exemple de sortie après l'exécution de la commande :

```
   "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"
    }   ]
}
```

Dissociation d'un VPC d'un profil Amazon Route 53

Choisissez un onglet pour dissocier un profil Route 53 d'un VPC à l'aide de la console Route 53, ou. AWS CLI

- Console
- INTERFACE DE LIGNE DE COMMANDE (CLI)

Console

Pour dissocier un VPC associé à un profil Route 53

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation, sélectionnez Profiles.
3. Dans la barre de navigation, choisissez la région dans laquelle le profil à partir duquel vous souhaitez dissocier un VPC a été créé.

4. Sélectionnez le bouton à côté du nom du profil dont vous souhaitez dissocier un VPC.
5. Sur la <Profile name>page, choisissez l'VPCsonglet.
6. Sur l' VPCs onglet de la ressource, choisissez le VPC que vous souhaitez dissocier, puis Dissocier.
7. Dans la boîte de dialogue Dissocier les ressources, tapez**`confirm`**, puis choisissez Dissocier.

CLI

Vous pouvez dissocier un profil d'un VPC en exécutant AWS CLI une commande comme celle-ci et en utilisant votre propre valeur `profile-id` pour et : `--resource-id`

```
aws route53profiles disassociate-profile --profile-id
rp-4987774726example --resource-id vpc-0af3b96b3example
```

Voici un exemple de sortie après l'exécution de la commande :

```
"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"
    }
```

Utilisation de profils Route 53 partagés

Vous pouvez partager un profil avec d'autres comptes en :

- Accorder des autorisations en lecture seule, ce qui signifie que l'autre compte peut associer le profil à son compte. VPCs Dans ce cas, toutes les ressources et configurations DNS seront appliquées sur le serveur associé VPCs.
- Octroi d'autorisations d'administrateur. Dans ce cas, les comptes dotés du profil partagé peuvent modifier le profil puis l'associer au leur VPCs. Un propriétaire peut également créer des

autorisations gérées par le client qui peuvent être utilisées pour spécifier les actions pouvant être effectuées par le compte du client. Pour plus d'informations, consultez la section Autorisations gérées par le client dans le guide de AWS RAM l'utilisateur.

Le profil Amazon Route 53 s'intègre à AWS Resource Access Manager (AWS RAM) pour permettre le partage des ressources. AWS RAM est un service qui vous permet de partager certaines ressources de la Route 53 avec d'autres Comptes AWS ou via AWS Organizations. Avec AWS RAM, vous partagez les ressources que vous possédez en créant un partage de ressources. Un partage de ressources spécifie les ressources à partager, ainsi que les consommateurs avec qui elles seront partagées. Les consommateurs peuvent être :

- Spécifique Comptes AWS
- Une unité organisationnelle au sein de son organisation dans AWS Organizations
- Toute son organisation en AWS Organizations

Pour plus d'informations AWS RAM, consultez le guide de AWS RAM l'utilisateur.

Cette rubrique explique comment partager des ressources dont vous êtes propriétaire et comment utiliser les ressources partagées avec vous.

Table des matières

- Octroi d'autorisations pour le partage de profils Route 53
- Conditions préalables au partage de profils Route 53
- Partage d'un profil Route 53
- Annulation du partage d'un profil Route 53 partagé
- Identifier un profil Route 53 partagé
- Responsabilités et autorisations pour les profils Route 53 partagés
- Facturation et mesures
- Quotas d'instances

Octroi d'autorisations pour le partage de profils Route 53

Un ensemble minimal d'autorisations est requis pour qu'un directeur IAM puisse partager un profil. Nous vous recommandons d'utiliser la politique IAM `AmazonRoute53ProfilesFullAccess` gérée

pour vous assurer que vos principaux IAM disposent des autorisations requises pour partager et utiliser des profils partagés.

Si vous utilisez une politique IAM personnalisée, les actions `route53profiles:GetProfilePolicy` et `route53profiles:PutProfilePolicy` sont requises. Il s'agit d'actions IAM avec autorisation uniquement. Si ces autorisations ne sont pas accordées à un principal IAM, une erreur se produira lors de la tentative de partage du profil à l'aide du AWS RAM service.

Conditions préalables au partage de profils Route 53

- Pour partager un profil Route 53, vous devez le posséder dans votre Compte AWS. Cela signifie que la ressource doit être allouée ou provisionnée dans votre compte. Vous ne pouvez pas partager un profil Route 53 qui a été partagé avec vous.
- Pour partager un profil Route 53 avec votre organisation ou une unité organisationnelle dans AWS Organizations, vous devez activer le partage avec AWS Organizations. Pour plus d'informations, consultez Activation du partage avec AWS Organizations dans le Guide de l'utilisateur AWS RAM .

Partage d'un profil Route 53

Lorsque vous partagez un profil que vous possédez avec un autre Compte AWS utilisateur, vous lui permettez d'appliquer les paramètres DNS du profil à son compte. VPCs Il est ainsi plus facile d'appliquer des configurations DNS uniformes à des milliers de serveurs VPCs avec un minimum de frais de gestion.

Pour partager un profil Route 53, vous devez l'ajouter à un partage de ressources. Un partage de ressources est une ressource AWS RAM qui vous permet de partager vos ressources entre des Comptes AWS. Un partage de ressources spécifie les ressources à partager, ainsi que les consommateurs avec qui elles seront partagées. Lorsque vous partagez un profil Route 53 à l'aide de la console Route 53, vous l'ajoutez à un partage de ressources existant. Pour ajouter le profil Route 53 à un nouveau partage de ressources, vous devez d'abord créer le partage de ressources à l'aide de la AWS RAM console.

Si vous faites partie d'une organisation AWS Organizations et que le partage au sein de votre organisation est activé, les clients de votre organisation ont automatiquement accès au profil Route 53 partagé. Dans le cas contraire, les consommateurs reçoivent une invitation à rejoindre le partage de ressources et ont accès au profil Route 53 partagé après avoir accepté l'invitation.

Vous pouvez commencer à partager un profil Route 53 que vous possédez sur la console Route 53 et continuer sur la AWS RAM console.

Pour partager un profil Route 53 dont vous êtes propriétaire à l'aide de la console Route 53

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation, sélectionnez Profiles.
3. Sélectionnez le profil que vous souhaitez partager, puis sur la page de détails du profil, choisissez Partager le profil.
4. Vous êtes redirigé vers la AWS RAM console où vous pouvez suivre les étapes suivantes : Création d'un partage de ressources dans le guide de AWS RAM l'utilisateur.
5. Si un profil vous est partagé, le tableau Profils inclut le texte « Partagé avec moi ».

   Lorsque vous avez partagé un profil, il est répertorié comme partagé dans le tableau Profils.

Pour partager un profil Route 53 dont vous êtes propriétaire à l'aide de la AWS RAM console

Consultez Création d’un partage de ressources dans le Guide de l’utilisateur AWS RAM .

Pour partager un profil Route 53 dont vous êtes propriétaire à l'aide du AWS CLI

Utilisez la commande create-resource-share.

Annulation du partage d'un profil Route 53 partagé

Lorsque vous annulez le partage d'un profil et VPCs que les configurations de ce profil sont associées, vous le perdez et utilisez par défaut les configurations spécifiques au VPC.

Pour annuler le partage d'un profil Route 53 dont vous êtes le propriétaire, vous devez le supprimer du partage de ressources. Vous pouvez le faire à l'aide de la console Route 53, de la AWS RAM console ou du AWS CLI.

Pour annuler le partage d'un profil Route 53 que vous possédez à l'aide de la console Route 53

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation, sélectionnez Profiles.

3. Sélectionnez le nom associé du profil dont vous souhaitez annuler le partage, puis sur la <Profile name>page, choisissez Gérer le partage.
4. Vous êtes redirigé vers la AWS RAM console où vous pouvez suivre les étapes suivantes : Mettre à jour un partage de ressources dans le guide de AWS RAM l'utilisateur.

Pour annuler le partage d'un profil Route 53 partagé dont vous êtes propriétaire à l'aide de la console AWS RAM

Consultez Mise à jour d'un partage de ressources dans le Guide de l'utilisateur AWS RAM .

Pour annuler le partage d'un profil Route 53 partagé dont vous êtes le propriétaire à l'aide du AWS CLI

Utilisez la commande disassociate-resource-share.

Identifier un profil Route 53 partagé

Les propriétaires et les consommateurs peuvent identifier les profils Route 53 partagés à l'aide de la console Route 53 et AWS CLI.

Pour identifier un profil Route 53 partagé à l'aide de la console Route 53

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation, sélectionnez Profiles.
3. Si un profil vous est partagé, le tableau Profils inclut le texte « Partagé avec moi ».

   Lorsque vous avez partagé un profil, il est répertorié comme partagé dans le tableau Profils.

Pour identifier un profil Route 53 partagé à l'aide du AWS CLI

Utilisez la commande get-profile ou list-profile. Les commandes renvoient des informations sur les profils Route 53 que vous possédez et sur l'état de partage des profils Route 53.

Responsabilités et autorisations pour les profils Route 53 partagés

Autorisations accordées aux propriétaires

Le propriétaire d'un profil peut consulter, gérer et supprimer les associations de ressources du profil, y compris les associations de ressources créées par les comptes de consommateurs. Le propriétaire

peut afficher et supprimer les associations VPC qu'il possède. En outre, seul le propriétaire d'un profil peut supprimer un profil qu'il possède, ce qui supprime automatiquement toutes les associations de ressources du profil.

> **Note**
>
> Vous devez créer une autorisation gérée personnalisée qui inclut l'`route53profiles:AssociateResourceToProfile`action, en plus des autorisations par défaut, d'associer les ressources des comptes avec lesquels le profil est partagé, car la politique par défaut `AWSRAMPermissionRoute53ProfileAllowAssociation` ne les inclut pas.

Autorisations accordées aux consommateurs

L'autorisation par défaut pour les utilisateurs d'un profil partagé est en lecture seule. Avec l'autorisation de lecture seule, ils peuvent voir les ressources associées et les associer VPCs, mais ne peuvent pas gérer les associations de ressources.

Un propriétaire peut également créer des autorisations gérées par le client sur la AWS RAM console. Pour plus d'informations, consultez la section Création et utilisation des autorisations gérées par le client dans le Guide de AWS RAM l'utilisateur.

Facturation et mesures

Les profils Route 53 sont facturés en fonction du nombre d'associations VPC. Le propriétaire du profil est responsable de la facture des associations VPC par le client.

Quotas d'instances

Les propriétaires de profils et les consommateurs partagent le même quota, à l'exception du nombre de profils Route 53 par compte dans une région. Pour de plus amples informations, veuillez consulter Quotas sur les profils de la Route 53 .

Qu'est-ce que Amazon Route 53 sur Outposts ?

AWS Outposts est un service entièrement géré qui étend AWS les infrastructures APIs, les services et les outils aux locaux des clients. Cela permet aux clients d'exécuter AWS des services avec des charges de travail sur site en utilisant les mêmes interfaces de programmation que dans. Régions AWS Pour plus d'informations, voir Qu'est-ce que c'est AWS Outposts ? dans le guide de AWS Outposts l'utilisateur.

Route 53 sur Outposts offre deux fonctionnalités :

- Un résolveur qui met en cache toutes les requêtes DNS provenant de AWS Outposts.
- Connectivité hybride entre un résolveur Outpost et un résolveur DNS sur site lorsque vous déployez des points de terminaison entrants et sortants.

Pour de plus amples informations, veuillez consulter Qu'est-ce que c'est Amazon Route 53 Resolver ?.

De plus, Route 53 sur Outposts réduit la latence du réseau en permettant de résoudre les requêtes au sein d'Outpost au lieu d'effectuer l'aller-retour jusqu'à la Région AWS la plus proche.

> **Note**
>
> Si vous possédez une version de AWS Outposts racks qui n'est pas compatible avec Route 53 sur Outposts, AWS l'équipe chargée du compte en est informée et vous contactera pour vous aider à effectuer la mise à niveau. AWS Outposts

Fonctionnalités d'Amazon Route 53 sur Outposts

Le tableau suivant décrit les différences entre les fonctionnalités de Route 53 sur Outposts et celles d'Amazon Route 53.

Route 53 sur Outposts par rapport à Route 53

Fonctionnalité	Disponibilité dans Route 53 sur Outposts
Route 53 Resolver	Oui. Resolver gère un cache local d'enregistrements pour les applications hébergées sur le rack Outpost, le VPC

Fonctionnalité	Disponibilité dans Route 53 sur Outposts
	apparenté qui s'y trouve et tout nom d'hôte accessible Région AWS au public.
Surveillance de l'état	Non. Les surveillances de l'état sont calculées et signalées à partir de la Région AWS. Si Outpost se déconnecte du cloud, les points de terminaison ne s'ouvrent pas et ne peuvent pas basculer vers une sauvegarde.
Points de terminaison du résolveur	Oui. Les points de terminaison du résolveur situés sur le rack Outpost permettent de transférer et de recevoir des requêtes DNS depuis les serveurs DNS sur site. Seul le type de IPv4 point de terminaison est disponible pour les points de terminaison.
Route 53 Resolver DNS Firewall	Indisponible.
Flux de trafic	Indisponible.

Comportement du résolveur Route 53 lorsqu'il AWS Outposts est déconnecté du VPC

S'il AWS Outposts est déconnecté du Région AWS, le résolveur d'Outpost se comporte comme suit :

- Les modifications du plan de contrôle ne sont pas disponibles.
- Les surveillances de l'état et la fonctionnalité de basculement DNS ne sont pas disponibles.
- Les requêtes DNS pour les ressources hébergées localement sur Outposts sont résolues, mais dans certains cas, la réponse peut être périmée si l'adresse IP de la ressource a été mise à jour alors que Outpost était déconnecté.
- Les requêtes DNS pour les ressources hébergées sur le VPC de la région peuvent être résolues. Toutefois, les ressources ne seront pas accessibles tant que la connexion à Outpost ne sera pas rétablie. Région AWS
- Les requêtes DNS pour les ressources DNS publiques peuvent être résolues si elles sont disponibles dans le cache du résolveur Route 53 sur Outpost.

Mise en route avec le résolveur de Route 53 sur AWS Outposts

Une fois que vous avez commandé vos AWS Outposts racks et qu'ils ont été livrés, comme décrit ici : Créez un AWS Outposts dans le AWS Outposts guide, vous pouvez configurer Resolver sur Outpost.

Vous pouvez également l'utiliser APIs pour gérer la Route 53 sur les Outposts. Pour plus d'informations, consultez la section Résolveur sur les actions Outpost.

> **Important**
>
> La création d'un cache de résolveur sur AWS Outposts peut prendre de 30 à 150 minutes.

Une fois vos AWS Outposts racks livrés, vous pouvez opter pour la Route 53 sur Outposts.

Pour configurer le résolveur sur Outpost

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation de gauche, développez Résolveur, puis accédez à Outposts.
3. Dans la barre de navigation, choisissez la région dans laquelle vous vous AWS Outposts trouvez.
4. Sur la page Résolveur sur Outpost, choisissez Créer un résolveur.
5. Sur la page Créer un résolveur :

   - Sous AWS Outpostssélectionnez celui sur lequel AWS Outposts vous souhaitez créer le résolveur.
   - Entrez le nom du résolveur dans la zone de texte Nom du résolveur.
   - Une fois que les types d'instances recommandés pour Resolver sont renseignés avec les EC2 instances Amazon, choisissez-en une.

     Pour plus d'informations sur les types d'instance, consultez Quotas sur le résolveur sur Outpost.
   - Pour le Nombre d'instances, choisissez le nombre d'instances d'interface Elastic pour le résolveur VPC. La valeur par défaut est 4.

     Si aucun type d'instance AWS Outposts ne prend en charge le résolveur, vous ne pourrez pas créer de résolveur.

6. Choisissez Create Resolver (Créer un résolveur).

   Vous pouvez suivre la création du résolveur sur la page Résolveur sur Outpost.

Création de points de terminaison entrants

Après avoir créé un résolveur sur Outpost, vous pouvez ajouter des points de terminaison entrants et sortants pour résoudre les requêtes DNS à destination et en provenance de votre réseau sur site.

Pour configurer les points de terminaison entrants pour le résolveur sur Outpost

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation de gauche, développez Résolveur, puis accédez à Outposts.
3. Dans la barre de navigation, choisissez la région dans laquelle vous vous AWS Outposts trouvez.
4. Cochez la case correspondant au résolveur qui est en état de fonctionnement et choisissez Afficher les détails.
5. Dans le tableau des points de terminaison entrants, choisissez Créer un point de terminaison entrant.
6. Sur la page Créer un point de terminaison entrant, entrez les valeurs applicables. Pour de plus amples informations, veuillez consulter Valeurs à spécifier lors de la création ou de la modification de points de terminaison entrants sur un Outpost.
7. Choisissez Créer un point de terminaison.

Valeurs à spécifier lors de la création ou de la modification de points de terminaison entrants sur un Outpost

Lorsque vous créez ou modifiez un point de terminaison entrant, spécifiez les valeurs suivantes :

ID Outpost

Si vous créez le point de terminaison d'un résolveur sur un AWS Outposts VPC, il s'agit AWS Outposts de l'ID.

Nom du point de terminaison

Un nom convivial vous permettant de retrouver facilement le point de terminaison entrant sur le tableau de bord.

VPC dans la région region-name

Toutes les requêtes DNS entrantes à partir de votre réseau transitent via ce VPC lors de leur transfert vers Resolver.

Groupe de sécurité de ce point de terminaison

L'ID d'un ou de plusieurs groupes de sécurité que vous souhaitez utiliser pour contrôler l'accès à ce point de terminaison sortant. Le groupe de sécurité que vous spécifiez doit inclure une ou plusieurs règles entrantes. Les règles entrantes doivent autoriser l'accès TCP et UDP sur le port 53. Vous ne pouvez pas modifier cette valeur après avoir créé un point de terminaison.

Pour plus d'informations, consultez Groupes de sécurité pour votre VPC dans le Guide de l'utilisateur Amazon VPC.

Adresses IP

Les adresses IP vers lesquelles vous souhaitez que les résolveurs DNS de votre réseau réacheminent les requêtes DNS. Nous vous demandons de spécifier au moins deux adresses IP pour la redondance. Remarques :

Adresses IP et interfaces réseau Elastic Amazon VPC

Pour chaque combinaison de zone de disponibilité, sous-réseau, et adresse IP que vous spécifiez, Resolver crée une interface réseau Elastic Amazon VPC. Pour le nombre maximum actuel de requêtes DNS par seconde et par adresse IP dans un point de terminaison, consultez Quotas sur Route 53 Resolver. Pour plus d'informations sur la tarification de chaque interface réseau Elastic, veuillez consulter la section Amazon Route 53 sur la page de tarification d'Amazon Route 53.

> **Note**
>
> Le point de terminaison Resolver possède une adresse IP privée. Ces adresses IP ne changeront pas au cours de la durée de vie d'un point de terminaison.

Pour chaque adresse IP, spécifiez les valeurs suivantes. Chaque adresse IP doit se trouver dans une zone de disponibilité du VPC que vous avez indiquée dans VPC dans la région region-name.

Zone de disponibilité

La zone de disponibilité par laquelle vous voulez que les requêtes DNS transitent lors de leur transfert vers votre VPC. La zone de disponibilité que vous spécifiez doit être configurée avec un sous-réseau.

Sous-réseau

Le sous-réseau qui contient l'adresse IP vers laquelle vous souhaitez acheminer les requêtes DNS. Le sous-réseau doit avoir une adresse IP disponible.

Spécifiez le sous-réseau pour une IPv4 adresse. IPv6 n'est pas pris en charge.

Adresse IP

Adresse IP unique vers laquelle les requêtes DNS doivent être transférées.

Choisissez si vous souhaitez que Resolver choisisse une adresse IP pour vous parmi les adresses IP disponibles dans le sous-réseau indiqué, ou si vous voulez indiquer l'adresse IP vous-même.

Si vous choisissez de spécifier vous-même l'adresse IP, saisissez-en une IPv4 . IPv6 n'est pas pris en charge.

Balises

Spécifiez une ou plusieurs clés et les valeurs correspondantes. Par exemple, vous pouvez indiquer Cost center (Centre de coûts) pour Key (Clé) et 456 pour Value (Valeur).

Ce sont les étiquettes qui AWS Billing and Cost Management permettent d'organiser votre AWS facture ; vous pouvez également les utiliser à d'autres fins. Pour plus d'informations sur l'utilisation de balises pour l'allocation de coûts, consultez Utilisation des balises d'allocation de coûts dans le Guide de l'utilisateur AWS Billing .

Création de points de terminaison sortants

Après avoir choisi et configuré un résolveur de Route 53, vous pouvez ajouter des points de terminaison entrants et sortants pour résoudre les requêtes DNS à destination et en provenance de votre réseau sur site.

Pour configurer les points de terminaison sortants pour le résolveur sur Outpost

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation de gauche, développez Résolveur, puis accédez à Outposts.
3. Dans la barre de navigation, choisissez la région dans laquelle vous vous AWS Outposts trouvez.
4. Cochez la case correspondant au résolveur qui est en état de fonctionnement et choisissez Afficher les détails.
5. Dans le tableau des points de terminaison sortants, choisissez Créer un point de terminaison sortant.
6. Sur la page Créer un point de terminaison sortant, entrez les valeurs applicables. Pour de plus amples informations, veuillez consulter Valeurs à spécifier lors de la création ou de la modification de points de terminaison entrants sur un Outpost.
7. Choisissez Créer un point de terminaison.

Valeurs à spécifier lors de la création ou de la modification de points de terminaison sortants dans un AWS Outposts

Lorsque vous créez ou modifiez un point de terminaison entrant, spécifiez les valeurs suivantes :

ID Outpost

Si vous créez le point de terminaison d'un résolveur sur un AWS Outposts VPC, il s'agit AWS Outposts de l'ID.

Nom du point de terminaison

Un nom convivial vous permettant de retrouver facilement le point de terminaison entrant sur le tableau de bord.

VPC dans la région region-name

Toutes les requêtes DNS entrantes à partir de votre réseau transitent via ce VPC lors de leur transfert vers Resolver.

Groupe de sécurité de ce point de terminaison

L'ID d'un ou de plusieurs groupes de sécurité que vous souhaitez utiliser pour contrôler l'accès à ce VPC. Le groupe de sécurité que vous spécifiez doit inclure une ou plusieurs règles entrantes.

Les règles entrantes doivent autoriser l'accès TCP et UDP sur le port 53. Vous ne pouvez pas modifier cette valeur après avoir créé un point de terminaison.

Pour plus d'informations, consultez Groupes de sécurité pour votre VPC dans le Guide de l'utilisateur Amazon VPC.

Adresses IP

Les adresses IP vers lesquelles vous souhaitez que les résolveurs DNS de votre réseau réacheminent les requêtes DNS. Nous vous demandons de spécifier au moins deux adresses IP pour la redondance. Remarques :

Adresses IP et interfaces réseau Elastic Amazon VPC

Pour chaque combinaison de zone de disponibilité, sous-réseau, et adresse IP que vous spécifiez, Resolver crée une interface réseau Elastic Amazon VPC. Pour le nombre maximum actuel de requêtes DNS par seconde et par adresse IP dans un point de terminaison, consultez Quotas sur Route 53 Resolver. Pour plus d'informations sur la tarification pour chaque interface réseau Elastic, veuillez consulter la section « Amazon Route 53 » sur la page de tarification d'Amazon Route 53.

> **Note**
>
> Le point de terminaison Resolver possède une adresse IP privée. Ces adresses IP ne changeront pas au cours de la durée de vie d'un point de terminaison.

Pour chaque adresse IP, spécifiez les valeurs suivantes. Chaque adresse IP doit se trouver dans une zone de disponibilité du VPC que vous avez indiquée dans VPC dans la région region-name.

Zone de disponibilité

La zone de disponibilité par laquelle vous voulez que les requêtes DNS transitent lors de leur transfert vers votre VPC. La zone de disponibilité que vous spécifiez doit être configurée avec un sous-réseau.

Sous-réseau

Le sous-réseau qui contient l'adresse IP vers laquelle vous souhaitez acheminer les requêtes DNS. Le sous-réseau doit avoir une adresse IP disponible.

Spécifiez le sous-réseau pour une IPv4 adresse. IPv6 n'est pas pris en charge.

Adresse IP

Adresse IP unique vers laquelle les requêtes DNS doivent être transférées.

Choisissez si vous souhaitez que Resolver choisisse une adresse IP pour vous parmi les adresses IP disponibles dans le sous-réseau indiqué, ou si vous voulez indiquer l'adresse IP vous-même.

Si vous choisissez de spécifier vous-même l'adresse IP, saisissez-en une IPv4 . IPv6 n'est pas pris en charge.

Balises

Spécifiez une ou plusieurs clés et les valeurs correspondantes. Par exemple, vous pouvez indiquer Cost center (Centre de coûts) pour Key (Clé) et 456 pour Value (Valeur).

Ce sont les étiquettes qui AWS Billing and Cost Management permettent d'organiser votre AWS facture ; vous pouvez également les utiliser à d'autres fins. Pour plus d'informations sur l'utilisation de balises pour l'allocation de coûts, consultez Utilisation des balises d'allocation de coûts dans le Guide de l'utilisateur AWS Billing .

Création de règles de réacheminement pour les points de terminaison sortants

Vous pouvez également créer des règles de réacheminement pour les points de terminaison sortants. Pour plus d’informations, consultez Pour créer des règles de transfert et les associer à une ou plusieurs VPCs.

Gestion du résolveur sur Outpost

Pour gérer le résolveur sur Outpost, exécutez la procédure applicable.

Rubriques

- Modification du résolveur sur Outpost
- Affichage de l'état du résolveur sur Outpost
- Suppression du résolveur sur Outpost

Modification du résolveur sur Outpost

Pour modifier un résolveur sur Outpost, procédez comme suit.

Pour modifier un résolveur sur Outpost

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation de gauche, développez Résolveur, puis accédez à Outposts.
3. Dans la barre de navigation, choisissez la région dans laquelle vous vous AWS Outposts trouvez.
4. Cochez la case à côté du résolveur qui est en état de fonctionnement et choisissez Modifier.
5. Vous pouvez modifier les informations suivantes :
   - Le nom du résolveur
   - Le type d'instance
   - Le nombre d'instances
6. Une fois les modifications terminées, choisissez Enregistrer les modifications.

Affichage de l'état du résolveur sur Outpost

Pour afficher l'état du résolveur sur Outpost, procédez comme suit.

Pour afficher le statut d'un point de terminaison entrant

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation de gauche, développez Résolveur, puis accédez à Outposts.
3. Dans la barre de navigation, choisissez la région dans laquelle vous vous AWS Outposts trouvez.
4. Cochez la case correspondant au résolveur qui est en état de fonctionnement et choisissez Afficher les détails.
5. La colonne État de la page Résolveur sur Outpost contient l'une des valeurs suivantes :

   Création

   Le résolveur sur Outpost est en cours de création.

Fonctionnement

Le résolveur sur Outpost est correctement configuré.

Mise à jour

Le résolveur sur Outpost met à jour les types d'instances.

Action requise

Le résolveur est défectueux et ne peut pas être récupéré automatiquement. Pour résoudre le problème, nous vous recommandons de vous assurer que l'instance est compatible AWS Outposts avec Resolver on Outpost.

Suppression

Le résolveur sur Outpost est en cours de suppression.

Échec de la création

La création du résolveur sur Outpost a échoué.

Échec de la suppression

La suppression du résolveur sur Outpost a échoué. Pour résoudre ce problème, réessayez dans quelques minutes.

Suppression du résolveur sur Outpost

> **Note**
>
> Avant de supprimer un résolveur sur Outpost, vous devez commencer par supprimer tous les points de terminaison associés.

Pour supprimer un résolveur sur Outpost, procédez comme suit.

Pour supprimer un résolveur sur Outpost

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation de gauche, développez Résolveur, puis accédez à Outposts.

3. Dans la barre de navigation, choisissez la région dans laquelle vous vous AWS Outposts trouvez.
4. Cochez la case correspondant au résolveur qui est en état de fonctionnement et choisissez Supprimer.
5. Dans la boîte de dialogue Supprimer le résolveur, saisissez **`delete`**, puis choisissez Supprimer.

Gestion des points de terminaison entrants sur le résolveur sur Outpost

Pour gérer les points de terminaison entrants sur le résolveur sur Outpost, exécutez la procédure applicable.

Rubriques

- Affichage et modification des points de terminaison entrants
- Affichage du statut des points de terminaison entrants
- Suppression des points de terminaison entrants

Affichage et modification des points de terminaison entrants

Pour afficher et modifier les paramètres d'un point de terminaison entrant, exécutez la procédure suivante.

Afficher ou modifier les paramètres d'un point de terminaison entrant

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation de gauche, développez Résolveur, puis accédez à Outposts.
3. Dans la barre de navigation, choisissez la région dans laquelle vous vous AWS Outposts trouvez.
4. Cochez la case correspondant au résolveur qui est en état de fonctionnement et choisissez Afficher les détails.
5. Dans la liste des points de terminaison entrants, choisissez l'option correspondant au point de terminaison que vous souhaitez consulter ou modifier.
6. Choisissez View details (Consulter les détails) ou Edit (Modifier).

Pour plus d'informations sur les valeurs des points de terminaison entrants, consultez Valeurs à spécifier lors de la création ou de la modification de points de terminaison entrants sur un Outpost.

7. Si vous avez choisi Edit (Modifier), entrez les valeurs applicables puis sélectionnez Save (Enregistrer).

Affichage du statut des points de terminaison entrants

Pour afficher le statut d'un point de terminaison entrant, procédez comme suit.

Pour afficher le statut d'un point de terminaison entrant

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation de gauche, développez Résolveur, puis accédez à Outposts.
3. Dans la barre de navigation, choisissez la région dans laquelle vous vous AWS Outposts trouvez.
4. Cochez la case correspondant au résolveur en état de fonctionnement et choisissez Afficher les détails.
5. La colonne État des points de terminaison entrants contient l'une des valeurs suivantes :

   Création

   Resolver crée et configure une ou plusieurs interfaces réseau Amazon VPC pour ce point de terminaison.

   Fonctionnement

   Les interfaces réseau Amazon VPC pour ce point de terminaison sont correctement configurées et en mesure de transmettre les requêtes DNS entrantes ou sortantes entre votre réseau et Resolver.

   Mise à jour

   Le résolveur associe ou dissocie une ou plusieurs interfaces réseau à l'aide de ce point de terminaison.

Récupération automatique

Resolver tente de récupérer une ou plusieurs des interfaces réseau qui sont associées à ce point de terminaison. Pendant le processus de récupération, le point de terminaison fonctionne avec une capacité limitée, en raison de la limite du nombre de requêtes DNS par adresse IP (par interface réseau). Pour connaître la limite actuelle, veuillez consulter Quotas sur Route 53 Resolver.

Action requise

Ce point de terminaison est non sain, et Resolver ne peut pas le récupérer automatiquement. Pour résoudre le problème, nous vous recommandons de vérifier chaque adresse IP que vous avez associé au point de terminaison. Pour chaque adresse IP qui n'est pas disponible, ajouter une autre adresse IP, puis supprimer l'adresse IP qui n'est pas disponible. Un point de terminaison doit toujours inclure au moins deux adresses IP. Un état Action needed (Action nécessaire) peut avoir plusieurs causes. Voici les deux plus courantes :

- Une ou plusieurs des interfaces réseau qui sont associées au point de terminaison ont été supprimées en utilisant Amazon VPC.
- L'interface réseau n'a pas pu être créée pour une certaine raison que Resolver ne peut pas contrôler.

Suppression

Le résolveur supprime ce point de terminaison et les interfaces réseau associées.

Suppression des points de terminaison entrants

Pour supprimer un point de terminaison entrant, utilisez la procédure suivante.

> **Important**
>
> Si vous supprimez un point de terminaison entrant, les requêtes DNS de votre réseau ne seront plus réacheminées vers Resolver dans le VPC que vous avez indiqué dans le point de terminaison.

Supprimer un point de terminaison entrant

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation de gauche, développez Résolveur, puis accédez à Outposts.
3. Dans la barre de navigation, choisissez la région dans laquelle vous vous AWS Outposts trouvez.
4. Cochez la case correspondant au résolveur en état de fonctionnement et choisissez Afficher les détails.
5. Cochez la case en regard du point de terminaison que vous souhaitez supprimer.
6. Sélectionnez Delete (Supprimer).
7. Pour confirmer que vous voulez supprimer le point de terminaison, saisissez le nom du point de terminaison et sélectionnez Submit (Envoyer).

Gestion des points de terminaison sortants sur le résolveur sur Outpost

Pour gérer les points de terminaison sortants sur le résolveur sur Outpost, exécutez la procédure applicable.

Rubriques

- Affichage et modification des points de terminaison sortants
- Affichage du statut des points de terminaison sortants
- Suppression des points de terminaison sortants

Affichage et modification des points de terminaison sortants

Pour afficher et modifier les paramètres d'un point de terminaison sortant, exécutez la procédure suivante.

Afficher ou modifier les paramètres d'un point de terminaison sortant

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.

2. Dans le volet de navigation de gauche, développez Résolveur, puis accédez à Outposts.
3. Dans la barre de navigation, choisissez la région dans laquelle vous vous AWS Outposts trouvez.
4. Cochez la case correspondant au résolveur en état de fonctionnement et choisissez Afficher les détails.
5. Dans la liste des points de terminaison sortants, cochez la case correspondant au point de terminaison pour lequel vous souhaitez afficher ou modifier les paramètres.
6. Choisissez View details (Consulter les détails) ou Edit (Modifier).

   Pour plus d'informations sur les valeurs des points de terminaison sortants, veuillez consulter Valeurs à spécifier lors de la création ou de la modification de points de terminaison sortants dans un AWS Outposts.
7. Si vous avez choisi Edit (Modifier), entrez les valeurs applicables puis sélectionnez Save (Enregistrer).

Affichage du statut des points de terminaison sortants

Pour afficher le statut d'un point de terminaison sortant, procédez comme suit.

Pour afficher le statut d'un point de terminaison sortant

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation de gauche, développez Résolveur, puis accédez à Outposts.
3. Dans la barre de navigation, choisissez la région dans laquelle vous vous AWS Outposts trouvez.
4. Cochez la case correspondant au résolveur en état de fonctionnement et choisissez Afficher les détails.
5. Dans la liste des points de terminaison sortants, la colonne État contient l'une des valeurs suivantes :

   Création

   Resolver crée et configure une ou plusieurs interfaces réseau Amazon VPC pour ce point de terminaison.

Fonctionnement

Les interfaces réseau Amazon VPC pour ce point de terminaison sont correctement configurées et en mesure de transmettre les requêtes DNS entrantes ou sortantes entre votre réseau et Resolver.

Mise à jour

Le résolveur associe ou dissocie une ou plusieurs interfaces réseau à l'aide de ce point de terminaison.

Récupération automatique

Resolver tente de récupérer une ou plusieurs des interfaces réseau qui sont associées à ce point de terminaison. Pendant le processus de récupération, le point de terminaison fonctionne avec une capacité limitée, en raison de la limite du nombre de requêtes DNS par adresse IP (par interface réseau). Pour connaître la limite actuelle, veuillez consulter Quotas sur Route 53 Resolver.

Action requise

Ce point de terminaison est non sain, et Resolver ne peut pas le récupérer automatiquement. Pour résoudre le problème, nous vous recommandons de vérifier chaque adresse IP que vous avez associé au point de terminaison. Pour chaque adresse IP qui n'est pas disponible, ajouter une autre adresse IP, puis supprimer l'adresse IP qui n'est pas disponible. (Un point de terminaison doivent toujours inclure au moins deux adresses IP.) Un état Action needed (Action nécessaire) peut avoir plusieurs causes. Voici les deux plus courantes :

- Une ou plusieurs des interfaces réseau qui sont associées au point de terminaison ont été supprimées en utilisant Amazon VPC.
- L'interface réseau n'a pas pu être créée pour une certaine raison que Resolver ne peut pas contrôler.

Suppression

Le résolveur supprime ce point de terminaison et les interfaces réseau associées.

Suppression des points de terminaison sortants

Avant de pouvoir supprimer un point de terminaison, vous devez d'abord supprimer toutes les règles associées à un VPC.

Pour supprimer un point de terminaison sortant, utilisez la procédure suivante.

> **Important**
>
> Si vous supprimez un point de terminaison sortant, Resolver cessera de réacheminer les requêtes DNS à partir de votre VPC vers votre réseau pour les règles qui spécifient le point de terminaison sortant supprimé.

Supprimer un point de terminaison sortant

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation de gauche, développez Résolveur, puis accédez à Outposts.
3. Cochez la case correspondant au résolveur en état de fonctionnement et choisissez Afficher les détails.
4. Dans la liste des points de terminaison sortants, choisissez l'option correspondant au point de terminaison que vous souhaitez supprimer.
5. Sélectionnez Delete (Supprimer).
6. Pour confirmer que vous voulez supprimer le point de terminaison, saisissez le nom du point de terminaison puis sélectionnez Submit (Envoyer).

Création d'Amazon Route 53 et de Amazon Route 53 Resolver ressources avec AWS CloudFormation

Amazon Route 53 est intégré à un service qui vous aide à modéliser et à configurer vos AWS ressources afin que vous puissiez passer moins de temps à créer et à gérer vos ressources et votre infrastructure. Amazon Route 53 Resolver AWS CloudFormation Vous créez un modèle qui décrit toutes les AWS ressources que vous souhaitez, et qui AWS CloudFormation fournit et configure ces ressources pour vous.

Lorsque vous l'utilisez AWS CloudFormation, vous pouvez réutiliser votre modèle pour configurer vos ressources Route 53 et Route 53 Resolver de manière cohérente et répétée. Décrivez vos ressources une seule fois, puis fournissez les mêmes ressources encore et encore dans plusieurs Comptes AWS régions.

Route 53, Route 53 Resolver et modèles AWS CloudFormation

Pour mettre en service et configurer des ressources pour Route 53, Route 53 Resolver et des services associés, vous devez maîtriser les modèles AWS CloudFormation. Les modèles sont des fichiers texte formatés en JSON ou YAML. Ces modèles décrivent les ressources que vous souhaitez mettre à disposition dans vos AWS CloudFormation piles. Si vous n'êtes pas familiarisé avec JSON ou YAML, vous pouvez utiliser AWS CloudFormation Designer pour vous aider à démarrer avec les AWS CloudFormation modèles. Pour plus d’informations, consultez Qu’est-ce que AWS CloudFormation Designer ? dans le AWS CloudFormation Guide de l’utilisateur.

Route 53 prend en charge la création des types de ressources suivants dans AWS CloudFormation :

- `AWS::Route53::DNSSEC`
- `AWS::Route53::HealthCheck`
- `AWS::Route53::HostedZone`
- `AWS::Route53::KeySigningKey`
- `AWS::Route53::RecordSet`
- `AWS::Route53::RecordSetGroup`

Pour plus d'informations, y compris des exemples de modèles JSON et YAML pour des ressources Route 53, consultez la Référence de type de ressource Amazon Route 53 dans le Guide de l'utilisateur AWS CloudFormation .

Route 53 Resolver prend en charge la création des types de ressources suivants dans AWS 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`

Pour plus d'informations, y compris des exemples de modèles JSON et YAML pour des ressources Route 53 Resolver, consultez la Amazon Route 53 Resolver Référence de type de ressource dans le Guide de l'utilisateur AWS CloudFormation .

En savoir plus sur AWS CloudFormation

Pour en savoir plus AWS CloudFormation, consultez les ressources suivantes :

- AWS CloudFormation
- AWS CloudFormation Guide de l'utilisateur
- AWS CloudFormation API Reference
- AWS CloudFormation Guide de l'utilisateur de l'interface de ligne de commande

Exemples de code pour Route 53 utilisant AWS SDKs

Les exemples de code suivants montrent comment utiliser Route 53 avec un kit de développement AWS logiciel (SDK).

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation de Route 53 avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit de développement logiciel (SDK).

Exemples de code

- Exemples de code pour Route 53 utilisant AWS SDKs
  - Exemples de base pour l'utilisation de Route 53 AWS SDKs
    - Actions pour utiliser Route 53 AWS SDKs
      - Utilisation de ChangeResourceRecordSets avec une CLI
      - Utilisation de CreateHostedZone avec une CLI
      - Utilisation de DeleteHostedZone avec une CLI
      - Utilisation de GetHostedZone avec une CLI
      - Utilisation ListHostedZones avec un AWS SDK ou une CLI
      - Utilisation de ListHostedZonesByName avec une CLI
      - Utilisation de ListQueryLoggingConfigs avec une CLI
- Exemples de code pour l'enregistrement de domaines Route 53 à l'aide de AWS SDKs
  - Exemples de base pour l'enregistrement de domaines Route 53 à l'aide de AWS SDKs
    - Bonjour Enregistrement de domaine Route 53
    - Découvrez les bases de l'enregistrement de domaines Route 53 à l'aide d'un AWS SDK
    - Actions pour l'enregistrement de domaines Route 53 à l'aide de AWS SDKs
      - Utilisation CheckDomainAvailability avec un AWS SDK ou une CLI
      - Utilisation CheckDomainTransferability avec un AWS SDK ou une CLI
      - Utilisation GetDomainDetail avec un AWS SDK ou une CLI
      - Utilisation GetDomainSuggestions avec un AWS SDK ou une CLI
      - Utilisation GetOperationDetail avec un AWS SDK ou une CLI
      - Utilisation ListDomains avec un AWS SDK ou une CLI

- Utilisation ListOperations avec un AWS SDK ou une CLI
- Utilisation ListPrices avec un AWS SDK
- Utilisation RegisterDomain avec un AWS SDK ou une CLI
- Utilisation ViewBilling avec un AWS SDK ou une CLI

Exemples de code pour Route 53 utilisant AWS SDKs

Les exemples de code suivants montrent comment utiliser Route 53 avec un kit de développement AWS logiciel (SDK).

Les actions sont des extraits de code de programmes plus larges et doivent être exécutées dans leur contexte. Alors que les actions vous indiquent comment appeler des fonctions de service individuelles, vous pouvez les voir en contexte dans leurs scénarios associés.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation de Route 53 avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit de développement logiciel (SDK).

Exemples de code

- Exemples de base pour l'utilisation de Route 53 AWS SDKs
  - Actions pour utiliser Route 53 AWS SDKs
    - Utilisation de ChangeResourceRecordSets avec une CLI
    - Utilisation de CreateHostedZone avec une CLI
    - Utilisation de DeleteHostedZone avec une CLI
    - Utilisation de GetHostedZone avec une CLI
    - Utilisation ListHostedZones avec un AWS SDK ou une CLI
    - Utilisation de ListHostedZonesByName avec une CLI
    - Utilisation de ListQueryLoggingConfigs avec une CLI

Exemples de base pour l'utilisation de Route 53 AWS SDKs

Les exemples de code suivants montrent comment utiliser les bases d'Amazon Route 53 avec AWS SDKs.

Exemples

- Actions pour utiliser Route 53 AWS SDKs
  - Utilisation de ChangeResourceRecordSets avec une CLI
  - Utilisation de CreateHostedZone avec une CLI
  - Utilisation de DeleteHostedZone avec une CLI
  - Utilisation de GetHostedZone avec une CLI
  - Utilisation ListHostedZones avec un AWS SDK ou une CLI
  - Utilisation de ListHostedZonesByName avec une CLI
  - Utilisation de ListQueryLoggingConfigs avec une CLI

Actions pour utiliser Route 53 AWS SDKs

Les exemples de code suivants montrent comment effectuer des actions Route 53 individuelles avec AWS SDKs. Chaque exemple inclut un lien vers GitHub, où vous pouvez trouver des instructions pour configurer et exécuter le code.

Les exemples suivants incluent uniquement les actions les plus couramment utilisées. Pour obtenir la liste complète, veuillez consulter la référence de l'API Amazon Route 53.

Exemples

- Utilisation de ChangeResourceRecordSets avec une CLI
- Utilisation de CreateHostedZone avec une CLI
- Utilisation de DeleteHostedZone avec une CLI
- Utilisation de GetHostedZone avec une CLI
- Utilisation ListHostedZones avec un AWS SDK ou une CLI
- Utilisation de ListHostedZonesByName avec une CLI
- Utilisation de ListQueryLoggingConfigs avec une CLI

Utilisation de **`ChangeResourceRecordSets`** avec une CLI

Les exemples de code suivants illustrent comment utiliser `ChangeResourceRecordSets`.

CLI

AWS CLI

Pour créer, mettre à jour ou supprimer un jeu d'enregistrements de ressources

La `change-resource-record-sets` commande suivante crée un ensemble d'enregistrements de ressources à l'aide de `hosted-zone-id` `Z1R8UBAEXAMPLE` la configuration au format JSON figurant dans le fichier : `C:\awscli\route53\change-resource-record-sets.json`

```
aws route53 change-resource-record-sets --hosted-zone-id Z1R8UBAEXAMPLE --change-batch file://C:\awscli\route53\change-resource-record-sets.json
```

Pour plus d'informations, consultez POST ChangeResourceRecordSets dans le manuel Amazon Route 53 API Reference.

La configuration du fichier JSON dépend du type d'ensemble d'enregistrements de ressources que vous souhaitez créer :

BasicWeightedAliasWeighted AliasLatencyLatency AliasFailoverFailover Alias

Syntaxe de base :

```
{
  "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"
          },
          {...}
        ]
      }
    },
    {...}
```

```
  ]
}
```

Syntaxe pondérée :

```
{
  "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"
      }
    },
    {...}
  ]
}
```

Syntaxe des alias :

```
{
  "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"
      }
    },
    {...}
  ]
}
```

Syntaxe d'alias pondérée :

```
{
  "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"
      }
    },
    {...}
  ]
}
```

Syntaxe de latence :

```
{
```

```
  "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"
      }
    },
    {...}
  ]
}
```

Syntaxe de l'alias de latence :

```
{
  "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"
      }
    },
    {...}
  ]
}
```

Syntaxe de basculement :

```
{
  "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"
      }
    },
    {...}
  ]
}
```

Syntaxe de l'alias Failover :

```
{
  "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"
      }
    },
    {...}
  ]
}
```

- Pour plus de détails sur l'API, reportez-vous ChangeResourceRecordSetsà la section Référence des AWS CLI commandes.

PowerShell

Outils pour PowerShell V4

Exemple 1 : Cet exemple crée un enregistrement A pour www.exemple.com et modifie l'enregistrement A pour test.exemple.com de 192.0.2.3 à 192.0.2.1. Notez que les valeurs des modifications des enregistrements de type TXT doivent être entre guillemets. Consultez la documentation Amazon Route 53 pour plus de détails. Vous pouvez utiliser l'Get-R53Changeapplet de commande pour effectuer un sondage afin de déterminer quand les modifications sont terminées.

```
$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
```

Exemple 2 : Cet exemple montre comment créer des ensembles d'enregistrements de ressources d'alias. « Z222222222 » est l'ID de la zone hébergée Amazon Route 53 dans laquelle vous créez le jeu d'enregistrements de ressources d'alias. « exemple.com » est l'apex de zone pour lequel vous souhaitez créer un alias et « www.exemple.com » est un sous-domaine pour lequel vous souhaitez également créer un alias. « Z1111111111111 » est un exemple d'ID de zone hébergée pour l'équilibreur de charge et « example-load-balancer -1111111111.us-east-1.elb.amazonaws.com » est un exemple de nom de domaine d'équilibreur de charge avec lequel Amazon Route 53 répond aux requêtes pour exemple.com et www.example.com. Consultez la documentation Amazon Route 53 pour plus de détails. Vous pouvez utiliser l'Get-R53Changeapplet de commande pour effectuer un sondage afin de déterminer quand les modifications sont terminées.

```
$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
```

Exemple 3 : Cet exemple crée deux enregistrements A pour www.example.com. Un quart du temps (1/ (1+3)), Amazon Route 53 répond aux requêtes relatives à www.example.com avec les deux valeurs du premier ensemble d'enregistrements de ressources (192.0.2.9 et 192.0.2.10). Dans les trois quarts des cas (3/ (1+3)), Amazon Route 53 répond aux requêtes relatives à www.example.com avec les deux valeurs du deuxième ensemble d'enregistrements de ressources (192.0.2.11 et 192.0.2.12). Consultez la documentation Amazon Route 53 pour plus de détails. Vous pouvez utiliser l'Get-R53Changeapplet de commande pour effectuer un sondage afin de déterminer quand les modifications sont terminées.

```
$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
```

Exemple 4 : Cet exemple montre comment créer des ensembles d'enregistrements de ressources d'alias pondérés en supposant que exemple.com est le domaine pour lequel vous souhaitez créer des ensembles d'enregistrements de ressources d'alias pondérés. SetIdentifier différencie les deux ensembles d'enregistrements de ressources alias pondérés l'un de l'autre. Cet élément est obligatoire car les éléments Nom et Type ont les mêmes valeurs pour les deux ensembles d'enregistrements de ressources. Z1111111111111 et Z3333333333333 sont des exemples de zone hébergée pour l'équilibreur de charge ELB spécifié par la valeur de. IDs DNSName example-load-balancer-2222222222.us-east-1.elb.amazonaws.com et example-load-balancer -4444444444.us-east-1.elb.amazonaws.com sont des exemples de domaines Elastic Load Balancing à partir desquels Amazon Route 53 répond aux requêtes pour exemple.com. Consultez la documentation Amazon Route 53 pour plus de détails. Vous pouvez utiliser l'Get-R53Changeapplet de commande pour effectuer un sondage afin de déterminer quand les modifications sont terminées.

```
$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
```

Exemple 5 : Cet exemple crée deux ensembles d'enregistrements de ressources d'alias de latence, l'un pour un équilibreur de charge ELB dans la région USA Ouest (Oregon) (us-west-2) et l'autre pour un équilibreur de charge dans la région Asie-Pacifique (Singapour) (ap-southeast-1). Consultez la documentation Amazon Route 53 pour plus de détails. Vous pouvez

utiliser l'Get-R53Changeapplet de commande pour effectuer un sondage afin de déterminer quand les modifications sont terminées.

```
$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
```

- Pour plus de détails sur l'API, reportez-vous ChangeResourceRecordSetsà la section Référence des Outils AWS pour PowerShell applets de commande (V4).

Outils pour PowerShell V5

Exemple 1 : Cet exemple crée un enregistrement A pour www.exemple.com et modifie l'enregistrement A pour test.exemple.com de 192.0.2.3 à 192.0.2.1. Notez que les valeurs des modifications des enregistrements de type TXT doivent être entre guillemets. Consultez la documentation Amazon Route 53 pour plus de détails. Vous pouvez utiliser l'Get-R53Changeapplet de commande pour effectuer un sondage afin de déterminer quand les modifications sont terminées.

```
$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
```

Exemple 2 : Cet exemple montre comment créer des ensembles d'enregistrements de ressources d'alias. « Z222222222 » est l'ID de la zone hébergée Amazon Route 53 dans laquelle vous créez le jeu d'enregistrements de ressources d'alias. « exemple.com » est l'apex de zone pour lequel vous souhaitez créer un alias et « www.exemple.com » est un sous-domaine pour lequel vous souhaitez également créer un alias. « Z1111111111111 » est un exemple d'ID de zone hébergée pour l'équilibreur de charge et « example-load-balancer -1111111111.us-east-1.elb.amazonaws.com » est un exemple de nom de domaine d'équilibreur de charge avec lequel Amazon Route 53 répond aux requêtes pour exemple.com et www.example.com. Consultez la documentation Amazon Route 53 pour plus de détails. Vous pouvez utiliser l'Get-R53Changeapplet de commande pour effectuer un sondage afin de déterminer quand les modifications sont terminées.

```
$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
```

Exemple 3 : Cet exemple crée deux enregistrements A pour www.example.com. Un quart du temps (1/ (1+3)), Amazon Route 53 répond aux requêtes relatives à www.example.com avec les deux valeurs du premier ensemble d'enregistrements de ressources (192.0.2.9 et 192.0.2.10). Dans les trois quarts des cas (3/ (1+3)), Amazon Route 53 répond aux requêtes relatives à www.example.com avec les deux valeurs du deuxième ensemble d'enregistrements de ressources (192.0.2.11 et 192.0.2.12). Consultez la documentation Amazon Route 53 pour plus de détails. Vous pouvez utiliser l'Get-R53Changeapplet de commande pour effectuer un sondage afin de déterminer quand les modifications sont terminées.

```
$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
```

Exemple 4 : Cet exemple montre comment créer des ensembles d'enregistrements de ressources d'alias pondérés en supposant que exemple.com est le domaine pour lequel vous souhaitez créer des ensembles d'enregistrements de ressources d'alias pondérés. SetIdentifier différencie les deux ensembles d'enregistrements de ressources alias pondérés l'un de l'autre. Cet élément est obligatoire car les éléments Nom et Type ont les mêmes valeurs pour les deux ensembles d'enregistrements de ressources. Z1111111111111 et Z3333333333333 sont des exemples de zone hébergée pour l'équilibreur de charge ELB spécifié par la valeur de. IDs DNSName example-load-balancer-2222222222.us-east-1.elb.amazonaws.com et example-load-balancer -4444444444.us-east-1.elb.amazonaws.com sont des exemples de domaines Elastic Load Balancing à partir desquels Amazon Route 53 répond aux requêtes pour exemple.com. Consultez la documentation Amazon Route 53 pour plus de détails. Vous pouvez utiliser l'Get-R53Changeapplet de commande pour effectuer un sondage afin de déterminer quand les modifications sont terminées.

```
$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
```

Exemple 5 : Cet exemple crée deux ensembles d'enregistrements de ressources d'alias de latence, l'un pour un équilibreur de charge ELB dans la région USA Ouest (Oregon) (us-west-2) et l'autre pour un équilibreur de charge dans la région Asie-Pacifique (Singapour) (ap-southeast-1). Consultez la documentation Amazon Route 53 pour plus de détails. Vous pouvez utiliser l'Get-R53Changeapplet de commande pour effectuer un sondage afin de déterminer quand les modifications sont terminées.

```
$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
```

- Pour plus de détails sur l'API, reportez-vous ChangeResourceRecordSetsà la section Référence des Outils AWS pour PowerShell applets de commande (V5).

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation de Route 53 avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation de **`CreateHostedZone`** avec une CLI

Les exemples de code suivants illustrent comment utiliser `CreateHostedZone`.

CLI

AWS CLI

Pour créer une zone hébergée

La `create-hosted-zone` commande suivante ajoute une zone hébergée nommée à `example.com` l'aide de la référence `2014-04-01-18:47` de l'appelant. Le commentaire facultatif inclut un espace, il doit donc être placé entre guillemets :

```
aws route53 create-hosted-zone --name example.com --caller-
reference 2014-04-01-18:47 --hosted-zone-config Comment="command-line version"
```

Pour plus d'informations, consultez la section Travailler avec des zones hébergées dans le guide du développeur Amazon Route 53.

- Pour plus de détails sur l'API, reportez-vous CreateHostedZoneà la section Référence des AWS CLI commandes.

PowerShell

Outils pour PowerShell V4

Exemple 1 : crée une nouvelle zone hébergée nommée « exemple.com », associée à un ensemble de délégations réutilisable. Notez que vous devez fournir une valeur pour le CallerReference paramètre afin que les demandes puissent être réessayées si nécessaire sans risquer d'exécuter l'opération deux fois. Comme la zone hébergée est créée dans un VPC, elle est automatiquement privée et vous ne devez pas définir le paramètre -HostedZoneConfig _PrivateZone .

```
$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
```

- Pour plus de détails sur l'API, reportez-vous CreateHostedZoneà la section Référence des Outils AWS pour PowerShell applets de commande (V4).

Outils pour PowerShell V5

Exemple 1 : crée une nouvelle zone hébergée nommée « exemple.com », associée à un ensemble de délégations réutilisable. Notez que vous devez fournir une valeur pour le CallerReference paramètre afin que les demandes puissent être réessayées si nécessaire sans risquer d'exécuter l'opération deux fois. Comme la zone hébergée est créée dans

un VPC, elle est automatiquement privée et vous ne devez pas définir le paramètre -HostedZoneConfig _PrivateZone .

```
$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
```

- Pour plus de détails sur l'API, reportez-vous CreateHostedZoneà la section Référence des Outils AWS pour PowerShell applets de commande (V5).

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation de Route 53 avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation de **`DeleteHostedZone`** avec une CLI

Les exemples de code suivants illustrent comment utiliser `DeleteHostedZone`.

CLI

AWS CLI

Pour supprimer une zone hébergée

La `delete-hosted-zone` commande suivante supprime la zone hébergée avec un `id` de `Z36KTIQEXAMPLE` :

```
aws route53 delete-hosted-zone --id Z36KTIQEXAMPLE
```

- Pour plus de détails sur l'API, reportez-vous DeleteHostedZoneà la section Référence des AWS CLI commandes.

PowerShell

Outils pour PowerShell V4

Exemple 1 : Supprime la zone hébergée avec l'ID spécifié. Vous serez invité à confirmer avant que la commande ne soit exécutée, sauf si vous ajoutez le paramètre de commutation -Force.

```
Remove-R53HostedZone -Id Z1PA6795UKMFR9
```

- Pour plus de détails sur l'API, reportez-vous DeleteHostedZoneà la section Référence des Outils AWS pour PowerShell applets de commande (V4).

Outils pour PowerShell V5

Exemple 1 : Supprime la zone hébergée avec l'ID spécifié. Vous serez invité à confirmer avant que la commande ne soit exécutée, sauf si vous ajoutez le paramètre de commutation -Force.

```
Remove-R53HostedZone -Id Z1PA6795UKMFR9
```

- Pour plus de détails sur l'API, reportez-vous DeleteHostedZoneà la section Référence des Outils AWS pour PowerShell applets de commande (V5).

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation de Route 53 avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation de **`GetHostedZone`** avec une CLI

Les exemples de code suivants illustrent comment utiliser `GetHostedZone`.

CLI

AWS CLI

Pour obtenir des informations sur une zone hébergée

La `get-hosted-zone` commande suivante permet d'obtenir des informations sur la zone hébergée avec un `id` de `Z1R8UBAEXAMPLE` :

```
aws route53 get-hosted-zone --id Z1R8UBAEXAMPLE
```

- Pour plus de détails sur l'API, reportez-vous GetHostedZoneà la section Référence des AWS CLI commandes.

PowerShell

Outils pour PowerShell V4

Exemple 1 : Renvoie les détails de la zone hébergée avec l'ID PJN98 FT9 Z1D633.

```
Get-R53HostedZone -Id Z1D633PJN98FT9
```

- Pour plus de détails sur l'API, reportez-vous GetHostedZoneà la section Référence des Outils AWS pour PowerShell applets de commande (V4).

Outils pour PowerShell V5

Exemple 1 : Renvoie les détails de la zone hébergée avec l'ID PJN98 FT9 Z1D633.

```
Get-R53HostedZone -Id Z1D633PJN98FT9
```

- Pour plus de détails sur l'API, reportez-vous GetHostedZoneà la section Référence des Outils AWS pour PowerShell applets de commande (V5).

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation de Route 53 avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`ListHostedZones`** avec un AWS SDK ou une CLI

Les exemples de code suivants illustrent comment utiliser `ListHostedZones`.

CLI

AWS CLI

Pour répertorier les zones hébergées associées au AWS compte actuel

La `list-hosted-zones` commande suivante répertorie les informations récapitulatives sur les 100 premières zones hébergées associées au AWS compte actuel. :

```
aws route53 list-hosted-zones
```

Si vous avez plus de 100 zones hébergées ou si vous souhaitez les répertorier dans des groupes inférieurs à 100, incluez le paramètre `--max-items`. Par exemple, pour répertorier les zones hébergées une par une, utilisez la commande suivante :

```
aws route53 list-hosted-zones --max-items 1
```

Pour afficher les informations relatives à la zone hébergée suivante, prenez la valeur `NextToken` de la réponse à la commande précédente et incluez-la dans le paramètre `--starting-token`, par exemple :

```
aws route53 list-hosted-zones --max-items 1 --starting-token Z3M3LMPEXAMPLE
```

- Pour plus de détails sur l'API, reportez-vous ListHostedZonesà la section Référence des AWS CLI commandes.

PowerShell

Outils pour PowerShell V4

Exemple 1 : affiche toutes vos zones hébergées publiques et privées.

```
Get-R53HostedZoneList
```

Exemple 2 : affiche toutes les zones hébergées associées à l'ensemble de délégations réutilisable portant l'ID NZ8 X2CISAMPLE

```
Get-R53HostedZoneList -DelegationSetId NZ8X2CISAMPLE
```

- Pour plus de détails sur l'API, reportez-vous ListHostedZonesà la section Référence des Outils AWS pour PowerShell applets de commande (V4).

Outils pour PowerShell V5

Exemple 1 : affiche toutes vos zones hébergées publiques et privées.

```
Get-R53HostedZoneList
```

Exemple 2 : affiche toutes les zones hébergées associées à l'ensemble de délégations réutilisable portant l'ID NZ8 X2CISAMPLE

```
Get-R53HostedZoneList -DelegationSetId NZ8X2CISAMPLE
```

- Pour plus de détails sur l'API, reportez-vous ListHostedZonesà la section Référence des Outils AWS pour PowerShell applets de commande (V5).

Rust

SDK pour Rust

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
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(())
}
```

- Pour plus de détails sur l'API, voir ListHostedZonesla section de référence de l'API AWS SDK for Rust.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation de Route 53 avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation de **`ListHostedZonesByName`** avec une CLI

Les exemples de code suivants illustrent comment utiliser `ListHostedZonesByName`.

CLI

AWS CLI

La commande suivante répertorie jusqu'à 100 zones hébergées classées par nom de domaine :

```
aws route53 list-hosted-zones-by-name
```

Sortie :

```
{
  "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"
}
```

La commande suivante répertorie les zones hébergées classées par nom, en commençant par `www.example.com` :

```
aws route53 list-hosted-zones-by-name --dns-name www.example.com
```

Sortie :

```
{
    "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"
}
```

- Pour plus de détails sur l'API, reportez-vous ListHostedZonesByNameà la section Référence des AWS CLI commandes.

PowerShell

Outils pour PowerShell V4

Exemple 1 : renvoie toutes vos zones hébergées publiques et privées dans l'ordre ASCII par nom de domaine.

```
Get-R53HostedZonesByName
```

Exemple 2 : renvoie vos zones hébergées publiques et privées, dans l'ordre ASCII par nom de domaine, en commençant par le nom DNS spécifié.

```
Get-R53HostedZonesByName -DnsName example2.com
```

- Pour plus de détails sur l'API, reportez-vous ListHostedZonesByNameà la section Référence des Outils AWS pour PowerShell applets de commande (V4).

Outils pour PowerShell V5

Exemple 1 : renvoie toutes vos zones hébergées publiques et privées dans l'ordre ASCII par nom de domaine.

```
Get-R53HostedZonesByName
```

Exemple 2 : renvoie vos zones hébergées publiques et privées, dans l'ordre ASCII par nom de domaine, en commençant par le nom DNS spécifié.

```
Get-R53HostedZonesByName -DnsName example2.com
```

- Pour plus de détails sur l'API, reportez-vous ListHostedZonesByNameà la section Référence des Outils AWS pour PowerShell applets de commande (V5).

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation de Route 53 avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation de **`ListQueryLoggingConfigs`** avec une CLI

Les exemples de code suivants illustrent comment utiliser `ListQueryLoggingConfigs`.

CLI

AWS CLI

Pour répertorier les configurations de journalisation des requêtes

L'`list-query-logging-configs`exemple suivant répertorie les informations relatives aux 100 premières configurations de journalisation des requêtes de votre AWS compte, pour la zone hébergée`Z1OX3WQEXAMPLE`.

```
aws route53 list-query-logging-configs \
    --hosted-zone-id Z1OX3WQEXAMPLE
```

Sortie :

```
{
    "QueryLoggingConfigs": [
        {
            "Id": "964ff34e-ae03-4f06-80a2-9683cexample",
            "HostedZoneId": "Z1OX3WQEXAMPLE",
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-
east-1:111122223333:log-group:/aws/route53/example.com:*"
        }
    ]
}
```

Pour plus d'informations, consultez la section Journalisation des requêtes DNS dans le manuel Amazon Route 53 Developer Guide.

- Pour plus de détails sur l'API, reportez-vous ListQueryLoggingConfigsà la section Référence des AWS CLI commandes.

PowerShell

Outils pour PowerShell V4

Exemple 1 : Cet exemple renvoie toutes les configurations pour la journalisation des requêtes DNS associées au courant Compte AWS.

```
Get-R53QueryLoggingConfigList
```

Sortie :

```
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:*
```

- Pour plus de détails sur l'API, reportez-vous ListQueryLoggingConfigsà la section Référence des Outils AWS pour PowerShell applets de commande (V4).

Outils pour PowerShell V5

Exemple 1 : Cet exemple renvoie toutes les configurations pour la journalisation des requêtes DNS associées au courant Compte AWS.

```
Get-R53QueryLoggingConfigList
```

Sortie :

```
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:*
```

- Pour plus de détails sur l'API, reportez-vous ListQueryLoggingConfigsà la section Référence des Outils AWS pour PowerShell applets de commande (V5).

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation de Route 53 avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Exemples de code pour l'enregistrement de domaines Route 53 à l'aide de AWS SDKs

Les exemples de code suivants montrent comment utiliser l'enregistrement de domaine Route 53 avec un kit de développement AWS logiciel (SDK).

Les principes de base sont des exemples de code qui vous montrent comment effectuer les opérations essentielles au sein d'un service.

Les actions sont des extraits de code de programmes plus larges et doivent être exécutées dans leur contexte. Alors que les actions vous indiquent comment appeler des fonctions de service individuelles, vous pouvez les voir en contexte dans leurs scénarios associés.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation de Route 53 avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Mise en route

Bonjour Enregistrement de domaine Route 53

Les exemples de code suivants montrent comment démarrer avec l'enregistrement de domaine Route 53.

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
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}");
        }
    }
}
```

- Pour plus de détails sur l'API, reportez-vous ListPricesà la section Référence des AWS SDK pour .NET API.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
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);
        }
    }
}
```

- Pour plus de détails sur l'API, reportez-vous ListPricesà la section Référence des AWS SDK for Java 2.x API.

Kotlin

SDK pour Kotlin

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
/**
 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}")
            }
    }
}
```

- Pour plus de détails sur l'API, consultez ListPricesla section AWS SDK pour la référence de l'API Kotlin.

Exemples de code

- Exemples de base pour l'enregistrement de domaines Route 53 à l'aide de AWS SDKs
  - Bonjour Enregistrement de domaine Route 53
  - Découvrez les bases de l'enregistrement de domaines Route 53 à l'aide d'un AWS SDK
  - Actions pour l'enregistrement de domaines Route 53 à l'aide de AWS SDKs
    - Utilisation CheckDomainAvailability avec un AWS SDK ou une CLI
    - Utilisation CheckDomainTransferability avec un AWS SDK ou une CLI
    - Utilisation GetDomainDetail avec un AWS SDK ou une CLI
    - Utilisation GetDomainSuggestions avec un AWS SDK ou une CLI
    - Utilisation GetOperationDetail avec un AWS SDK ou une CLI
    - Utilisation ListDomains avec un AWS SDK ou une CLI
    - Utilisation ListOperations avec un AWS SDK ou une CLI
    - Utilisation ListPrices avec un AWS SDK

- Utilisation RegisterDomain avec un AWS SDK ou une CLI
- Utilisation ViewBilling avec un AWS SDK ou une CLI

Exemples de base pour l'enregistrement de domaines Route 53 à l'aide de AWS SDKs

Les exemples de code suivants montrent comment utiliser les principes de base de Amazon Route 53 domain registration with AWS SDKs.

Exemples

- Bonjour Enregistrement de domaine Route 53
- Découvrez les bases de l'enregistrement de domaines Route 53 à l'aide d'un AWS SDK
- Actions pour l'enregistrement de domaines Route 53 à l'aide de AWS SDKs
  - Utilisation CheckDomainAvailability avec un AWS SDK ou une CLI
  - Utilisation CheckDomainTransferability avec un AWS SDK ou une CLI
  - Utilisation GetDomainDetail avec un AWS SDK ou une CLI
  - Utilisation GetDomainSuggestions avec un AWS SDK ou une CLI
  - Utilisation GetOperationDetail avec un AWS SDK ou une CLI
  - Utilisation ListDomains avec un AWS SDK ou une CLI
  - Utilisation ListOperations avec un AWS SDK ou une CLI
  - Utilisation ListPrices avec un AWS SDK
  - Utilisation RegisterDomain avec un AWS SDK ou une CLI
  - Utilisation ViewBilling avec un AWS SDK ou une CLI

Bonjour Enregistrement de domaine Route 53

Les exemples de code suivants montrent comment démarrer avec l'enregistrement de domaine Route 53.

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
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}");
        }
    }
```

```
}
```

- Pour plus de détails sur l'API, reportez-vous ListPricesà la section Référence des AWS SDK pour .NET API.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
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);
        }
    }
}
```

- Pour plus de détails sur l'API, reportez-vous ListPricesà la section Référence des AWS SDK for Java 2.x API.

Kotlin

SDK pour Kotlin

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
/**
 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}")
            }
```

```
    }
}
```

- Pour plus de détails sur l'API, consultez ListPricesla section AWS SDK pour la référence de l'API Kotlin.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation de Route 53 avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Découvrez les bases de l'enregistrement de domaines Route 53 à l'aide d'un AWS SDK

Les exemples de code suivants montrent comment :

- Répertorier les domaines actuels et les opérations effectuées au cours de l'année écoulée.
- Afficher la facturation de l'année écoulée et les prix des types de domaines.
- Obtenir des suggestions de domaines.
- Vérifier la disponibilité et la transférabilité du domaine.
- Éventuellement, demander l'enregistrement d'un domaine.
- Obtenir des informations sur une opération.
- Éventuellement, obtenir des informations sur un domaine.

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Exécutez un scénario interactif à une invite de commande.

```
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;
    }
}
```

Méthodes d'encapsulation utilisées par le scénario pour les actions d'enregistrement de domaine Route 53.

```
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.";
        }
    }
}
```

- Pour plus d'informations sur l'API consultez les rubriques suivantes dans la référence de l'API AWS SDK pour .NET .
  - CheckDomainAvailability
  - CheckDomainTransferability
  - GetDomainDetail
  - GetDomainSuggestions
  - GetOperationDetail
  - ListDomains
  - ListOperations
  - ListPrices
  - RegisterDomain
  - ViewBilling

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
/**
 * 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);
        }
    }
}
```

- Pour plus d'informations sur l'API, consultez les rubriques suivantes dans la référence de l'API AWS SDK for Java 2.x .
  - CheckDomainAvailability
  - CheckDomainTransferability
  - GetDomainDetail
  - GetDomainSuggestions
  - GetOperationDetail
  - ListDomains
  - ListOperations
  - ListPrices
  - RegisterDomain
  - ViewBilling

Kotlin

SDK pour Kotlin

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
/**
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}")
            }
    }
}
```

- Pour plus d'informations sur l'API, consultez les rubriques suivantes dans AWS SDK for Kotlin API reference.
  - CheckDomainAvailability
  - CheckDomainTransferability
  - GetDomainDetail
  - GetDomainSuggestions
  - GetOperationDetail
  - ListDomains
  - ListOperations
  - ListPrices
  - RegisterDomain
  - ViewBilling

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation de Route 53 avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Actions pour l'enregistrement de domaines Route 53 à l'aide de AWS SDKs

Les exemples de code suivants montrent comment effectuer des actions d'enregistrement de domaine Route 53 individuelles avec AWS SDKs. Chaque exemple inclut un lien vers GitHub, où vous pouvez trouver des instructions pour configurer et exécuter le code.

Les exemples suivants incluent uniquement les actions les plus couramment utilisées. Pour obtenir la liste complète, veuillez consulter la Amazon Route 53 domain registration Référence d'API.

Exemples

- Utilisation CheckDomainAvailability avec un AWS SDK ou une CLI
- Utilisation CheckDomainTransferability avec un AWS SDK ou une CLI
- Utilisation GetDomainDetail avec un AWS SDK ou une CLI
- Utilisation GetDomainSuggestions avec un AWS SDK ou une CLI
- Utilisation GetOperationDetail avec un AWS SDK ou une CLI
- Utilisation ListDomains avec un AWS SDK ou une CLI
- Utilisation ListOperations avec un AWS SDK ou une CLI
- Utilisation ListPrices avec un AWS SDK
- Utilisation RegisterDomain avec un AWS SDK ou une CLI
- Utilisation ViewBilling avec un AWS SDK ou une CLI

Utilisation **`CheckDomainAvailability`** avec un AWS SDK ou une CLI

Les exemples de code suivants illustrent comment utiliser `CheckDomainAvailability`.

Les exemples d'actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans l'exemple de code suivant :

- Principes de base

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
/// <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;
}
```

- Pour plus de détails sur l'API, reportez-vous CheckDomainAvailabilityà la section Référence des AWS SDK pour .NET API.

CLI

AWS CLI

Pour déterminer si vous pouvez enregistrer un nom de domaine avec Route 53

La `check-domain-availability` commande suivante renvoie des informations indiquant si le nom de domaine `example.com` est disponible pour être enregistré via Route 53.

Cette commande s'exécute uniquement dans la `us-east-1` région. Si votre région par défaut est définie sur`us-east-1`, vous pouvez omettre le `region` paramètre.

```
aws route53domains check-domain-availability \
    --region us-east-1 \
    --domain-name example.com
```

Sortie :

```
{
    "Availability": "UNAVAILABLE"
}
```

Route 53 prend en charge un grand nombre de domaines de premier niveau (TLDs), tels que `.com` et `.jp`, mais nous ne prenons pas en charge tous les domaines disponibles TLDs. Si vous vérifiez la disponibilité d'un domaine et que Route 53 ne prend pas en charge le TLD, `check-domain-availability` renvoie le message suivant.

```
An error occurred (UnsupportedTLD) when calling the CheckDomainAvailability
 operation: <top-level domain> tld is not supported.
```

Pour obtenir la liste des domaines TLDs que vous pouvez utiliser lors de l'enregistrement d'un domaine auprès de Route 53, consultez la section Domaines que vous pouvez enregistrer auprès d'Amazon Route 53 dans le guide du développeur Amazon Route 53. Pour plus d'informations sur l'enregistrement de domaines auprès d'Amazon Route 53, consultez la section Enregistrer un nouveau domaine dans le manuel Amazon Route 53 Developer Guide.

- Pour plus de détails sur l'API, reportez-vous CheckDomainAvailabilityà la section Référence des AWS CLI commandes.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    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);
        }
    }
```

- Pour plus de détails sur l'API, reportez-vous CheckDomainAvailabilityà la section Référence des AWS SDK for Java 2.x API.

Kotlin

SDK pour Kotlin

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
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}")
    }
}
```

- Pour plus de détails sur l'API, consultez CheckDomainAvailabilityla section AWS SDK pour la référence de l'API Kotlin.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation de Route 53 avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`CheckDomainTransferability`** avec un AWS SDK ou une CLI

Les exemples de code suivants illustrent comment utiliser `CheckDomainTransferability`.

Les exemples d'actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans l'exemple de code suivant :

- Principes de base

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    /// <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;
    }
```

- Pour plus de détails sur l'API, reportez-vous CheckDomainTransferabilityà la section Référence des AWS SDK pour .NET API.

CLI

AWS CLI

Pour déterminer si un domaine peut être transféré vers Route 53

La `check-domain-transferability` commande suivante renvoie des informations indiquant si vous pouvez transférer le nom de domaine `example.com` vers Route 53.

Cette commande s'exécute uniquement dans la `us-east-1` région. Si votre région par défaut est définie sur`us-east-1`, vous pouvez omettre le `region` paramètre.

```
aws route53domains check-domain-transferability \
    --region us-east-1 \
    --domain-name example.com
```

Sortie :

```
{
    "Transferability": {
        "Transferable": "UNTRANSFERABLE"
    }
}
```

Pour plus d'informations, consultez la section Transfert de l'enregistrement d'un domaine vers Amazon Route 53 dans le manuel du développeur Amazon Route 53.

- Pour plus de détails sur l'API, reportez-vous CheckDomainTransferabilityà la section Référence des AWS CLI commandes.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
   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);
       }
   }
```

- Pour plus de détails sur l'API, reportez-vous CheckDomainTransferabilityà la section Référence des AWS SDK for Java 2.x API.

Kotlin

SDK pour Kotlin

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
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}")
    }
}
```

- Pour plus de détails sur l'API, consultez CheckDomainTransferabilityla section AWS SDK pour la référence de l'API Kotlin.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation de Route 53 avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`GetDomainDetail`** avec un AWS SDK ou une CLI

Les exemples de code suivants illustrent comment utiliser `GetDomainDetail`.

Les exemples d'actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans l'exemple de code suivant :

- Principes de base

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    /// <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.";
        }
    }
```

- Pour plus de détails sur l'API, reportez-vous GetDomainDetailà la section Référence des AWS SDK pour .NET API.

CLI

AWS CLI

Pour obtenir des informations détaillées sur un domaine spécifique

La `get-domain-detail` commande suivante affiche des informations détaillées sur le domaine spécifié.

Cette commande s'exécute uniquement dans la `us-east-1` région. Si votre région par défaut est définie sur`us-east-1`, vous pouvez omettre le `region` paramètre.

```
aws route53domains get-domain-detail \
    --region us-east-1 \
    --domain-name example.com
```

Sortie :

```
{
    "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"
    ]
}
```

- Pour plus de détails sur l'API, reportez-vous GetDomainDetailà la section Référence des AWS CLI commandes.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
   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);
        }
    }
```

- Pour plus de détails sur l'API, reportez-vous GetDomainDetailà la section Référence des AWS SDK for Java 2.x API.

Kotlin

SDK pour Kotlin

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
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}")
    }
}
```

- Pour plus de détails sur l'API, consultez GetDomainDetailla section AWS SDK pour la référence de l'API Kotlin.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation de Route 53 avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`GetDomainSuggestions`** avec un AWS SDK ou une CLI

Les exemples de code suivants illustrent comment utiliser `GetDomainSuggestions`.

Les exemples d'actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans l'exemple de code suivant :

- Principes de base

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    /// <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;
    }
```

- Pour plus de détails sur l'API, reportez-vous GetDomainSuggestionsà la section Référence des AWS SDK pour .NET API.

CLI

AWS CLI

Pour obtenir une liste des noms de domaine suggérés

La `get-domain-suggestions` commande suivante affiche une liste de noms de domaine suggérés en fonction du nom de domaine`example.com`. La réponse inclut uniquement les noms de domaine disponibles. Cette commande s'exécute uniquement dans la `us-east-1` région. Si votre région par défaut est définie sur`us-east-1`, vous pouvez omettre le `region` paramètre.

```
aws route53domains get-domain-suggestions \
    --region us-east-1 \
    --domain-name example.com \
    --suggestion-count 10 \
    --only-available
```

Sortie :

```
{
    "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"
        }
    ]
}
```

- Pour plus de détails sur l'API, reportez-vous GetDomainSuggestionsà la section Référence des AWS CLI commandes.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
   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);
       }
   }
```

- Pour plus de détails sur l'API, reportez-vous GetDomainSuggestionsà la section Référence des AWS SDK for Java 2.x API.

Kotlin

SDK pour Kotlin

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
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(" ")
        }
    }
}
```

- Pour plus de détails sur l'API, consultez GetDomainSuggestionsla section AWS SDK pour la référence de l'API Kotlin.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation de Route 53 avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`GetOperationDetail`** avec un AWS SDK ou une CLI

Les exemples de code suivants illustrent comment utiliser `GetOperationDetail`.

Les exemples d'actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans l'exemple de code suivant :

- Principes de base

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    /// <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}.";
        }
```

```
    }
```

- Pour plus de détails sur l'API, reportez-vous GetOperationDetailà la section Référence des AWS SDK pour .NET API.

CLI

AWS CLI

Pour obtenir le statut actuel d'une opération

Certaines opérations d'enregistrement de domaine fonctionnent de manière asynchrone et renvoient une réponse avant leur fin. Ces opérations renvoient un identifiant d'opération que vous pouvez utiliser pour obtenir le statut actuel. La `get-operation-detail` commande suivante renvoie le statut de l'opération spécifiée.

Cette commande s'exécute uniquement dans la `us-east-1` région. Si votre région par défaut est définie sur`us-east-1`, vous pouvez omettre le `region` paramètre.

```
aws route53domains get-operation-detail \
    --region us-east-1 \
    --operation-id edbd8d63-7fe7-4343-9bc5-54033example
```

Sortie :

```
{
    "OperationId": "edbd8d63-7fe7-4343-9bc5-54033example",
    "Status": "SUCCESSFUL",
    "DomainName": "example.com",
    "Type": "DOMAIN_LOCK",
    "SubmittedDate": 1573749367.864
}
```

- Pour plus de détails sur l'API, reportez-vous GetOperationDetailà la section Référence des AWS CLI commandes.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
   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);
       }
   }
```

- Pour plus de détails sur l'API, reportez-vous GetOperationDetailà la section Référence des AWS SDK for Java 2.x API.

Kotlin

SDK pour Kotlin

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
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}")
    }
}
```

- Pour plus de détails sur l'API, consultez GetOperationDetailla section AWS SDK pour la référence de l'API Kotlin.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation de Route 53 avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`ListDomains`** avec un AWS SDK ou une CLI

Les exemples de code suivants illustrent comment utiliser `ListDomains`.

Les exemples d'actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans l'exemple de code suivant :

- Principes de base

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
/// <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;
}
```

- Pour plus de détails sur l'API, reportez-vous ListDomainsà la section Référence des AWS SDK pour .NET API.

CLI

AWS CLI

Pour répertorier les domaines enregistrés avec le AWS compte actuel

La `list-domains` commande suivante répertorie les informations récapitulatives sur les domaines enregistrés avec le AWS compte actuel.

Cette commande s'exécute uniquement dans la `us-east-1` région. Si votre région par défaut est définie sur`us-east-1`, vous pouvez omettre le `region` paramètre.

```
aws route53domains list-domains
    --region us-east-1
```

Sortie :

```
{
    "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
        }
    ]
}
```

- Pour plus de détails sur l'API, reportez-vous ListDomainsà la section Référence des AWS CLI commandes.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    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);
        }
    }
```

- Pour plus de détails sur l'API, reportez-vous ListDomainsà la section Référence des AWS SDK for Java 2.x API.

Kotlin

SDK pour Kotlin

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
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}")
            }
    }
}
```

- Pour plus de détails sur l'API, consultez ListDomainsla section AWS SDK pour la référence de l'API Kotlin.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation de Route 53 avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`ListOperations`** avec un AWS SDK ou une CLI

Les exemples de code suivants illustrent comment utiliser `ListOperations`.

Les exemples d'actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans l'exemple de code suivant :

- Principes de base

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    /// <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;
    }
```

- Pour plus de détails sur l'API, reportez-vous ListOperationsà la section Référence des AWS SDK pour .NET API.

CLI

AWS CLI

Pour répertorier le statut des opérations qui renvoient un ID d'opération

Certaines opérations d'enregistrement de domaine s'exécutent de manière asynchrone et renvoient une réponse avant leur fin. Ces opérations renvoient un identifiant d'opération que vous pouvez utiliser pour obtenir le statut actuel. La `list-operations` commande suivante répertorie les informations récapitulatives, y compris le statut, concernant les opérations d'enregistrement de domaine en cours.

Cette commande s'exécute uniquement dans la `us-east-1` région. Si votre région par défaut est définie sur`us-east-1`, vous pouvez omettre le `region` paramètre.

```
aws route53domains list-operations
    --region us-east-1
```

Sortie :

```
{
    "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
        }
    ]
}
```

La sortie inclut toutes les opérations qui renvoient un ID d'opération et que vous avez effectuées sur tous les domaines que vous avez enregistrés à l'aide du AWS compte courant. Si vous souhaitez obtenir uniquement les opérations que vous avez soumises après une date spécifiée, vous pouvez inclure le `submitted-since` paramètre et spécifier une date au format Unix et en temps universel coordonné (UTC). La commande suivante permet d'obtenir le statut de toutes les opérations soumises après 00h00 UTC le 1er janvier 2020.

```
aws route53domains list-operations \
    --submitted-since 1577836800
```

- Pour plus de détails sur l'API, reportez-vous ListOperationsà la section Référence des AWS CLI commandes.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
   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);
        }
    }
```

- Pour plus de détails sur l'API, reportez-vous ListOperationsà la section Référence des AWS SDK for Java 2.x API.

Kotlin

SDK pour Kotlin

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
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}")
```

```
            }
        }
    }
```

- Pour plus de détails sur l'API, consultez ListOperationsla section AWS SDK pour la référence de l'API Kotlin.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation de Route 53 avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`ListPrices`** avec un AWS SDK

Les exemples de code suivants illustrent comment utiliser `ListPrices`.

Les exemples d'actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans l'exemple de code suivant :

- Principes de base

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    /// <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();
    }
```

- Pour plus de détails sur l'API, reportez-vous ListPricesà la section Référence des AWS SDK pour .NET API.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
   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);
        }
    }
```

- Pour plus de détails sur l'API, reportez-vous ListPricesà la section Référence des AWS SDK for Java 2.x API.

Kotlin

SDK pour Kotlin

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
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}")
                }
        }
    }
```

- Pour plus de détails sur l'API, consultez ListPricesla section AWS SDK pour la référence de l'API Kotlin.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation de Route 53 avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`RegisterDomain`** avec un AWS SDK ou une CLI

Les exemples de code suivants illustrent comment utiliser `RegisterDomain`.

Les exemples d'actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans l'exemple de code suivant :

- Principes de base

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    /// <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;
        }
    }
```

- Pour plus de détails sur l'API, reportez-vous RegisterDomainà la section Référence des AWS SDK pour .NET API.

CLI

AWS CLI

Pour enregistrer un domaine

La `register-domain` commande suivante enregistre un domaine et récupère toutes les valeurs de paramètres d'un fichier au format JSON.

Cette commande s'exécute uniquement dans la `us-east-1` région. Si votre région par défaut est définie sur`us-east-1`, vous pouvez omettre le `region` paramètre.

```
aws route53domains register-domain \
    --region us-east-1 \
    --cli-input-json file://register-domain.json
```

Contenu de `register-domain.json` :

```
{
    "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
}
```

Sortie :

```
{
    "OperationId": "b114c44a-9330-47d1-a6e8-a0b11example"
}
```

Pour confirmer que l'opération a réussi, vous pouvez exécuter`get-operation-detail`. Pour plus d'informations, consultez get-operation-detail.

Pour de plus amples informations, veuillez consulter Enregistrement d'un nouveau domaine dans le Manuel du développeur Amazon Route 53.

Pour plus d'informations sur les domaines de premier niveau (TLDs) nécessitant des valeurs `ExtraParams` et sur les valeurs valides, consultez le manuel ExtraParamde référence des API Amazon Route 53.

- Pour plus de détails sur l'API, reportez-vous RegisterDomainà la section Référence des AWS CLI commandes.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
   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 "";
    }
```

- Pour plus de détails sur l'API, reportez-vous RegisterDomainà la section Référence des AWS SDK for Java 2.x API.

Kotlin

SDK pour Kotlin

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
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
    }
}
```

- Pour plus de détails sur l'API, consultez RegisterDomainla section AWS SDK pour la référence de l'API Kotlin.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation de Route 53 avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`ViewBilling`** avec un AWS SDK ou une CLI

Les exemples de code suivants illustrent comment utiliser `ViewBilling`.

Les exemples d'actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans l'exemple de code suivant :

- Principes de base

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    /// <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;
    }
```

- Pour plus de détails sur l'API, reportez-vous ViewBillingà la section Référence des AWS SDK pour .NET API.

CLI

AWS CLI

Pour obtenir les informations de facturation relatives aux frais d'enregistrement de domaine pour le AWS compte courant

La `view-billing` commande suivante renvoie tous les enregistrements de facturation relatifs au domaine pour le compte courant pour la période comprise entre le 1er janvier 2018 (1514764800 en heure Unix) et minuit le 31 décembre 2019 (1577836800 en heure Unix).

Cette commande s'exécute uniquement dans la `us-east-1` région. Si votre région par défaut est définie sur`us-east-1`, vous pouvez omettre le `region` paramètre.

```
aws route53domains view-billing \
    --region us-east-1 \
    --start-time 1514764800 \
    --end-time 1577836800
```

Sortie :

```
{
    "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
        }
```

```
    ]
}
```

Pour plus d'informations, consultez ViewBillingle manuel de référence des API Amazon Route 53.

- Pour plus de détails sur l'API, reportez-vous ViewBillingà la section Référence des AWS CLI commandes.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
   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);
        }
    }
```

- Pour plus de détails sur l'API, reportez-vous ViewBillingà la section Référence des AWS SDK for Java 2.x API.

Kotlin

SDK pour Kotlin

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
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}")
            }
    }
}
```

- Pour plus de détails sur l'API, consultez ViewBillingla section AWS SDK pour la référence de l'API Kotlin.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation de Route 53 avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Sécurité dans Amazon Route 53

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit cette notion par les termes sécurité du cloud et sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de conformitéAWS. Pour en savoir plus sur les programmes de conformité qui s'appliquent à Amazon Route 53, veuillez consulter la section Services AWS concernés par le programme de conformité.
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris la sensibilité de vos données, les exigences de votre entreprise, ainsi que la législation et la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation de Route 53. Les rubriques suivantes vous montrent comment configurer Route 53 pour répondre à vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser vos ressources Route 53.

Rubriques

- Protection des données sur Route 53
- Identity and Access Management dans Amazon Route 53
- Journalisation et surveillance dans Amazon Route 53
- Validation de la conformité pour Amazon Route 53
- La résilience dans Amazon Route 53
- Sécurité de l'infrastructure dans Amazon Route 53

Protection des données sur Route 53

Le modèle de responsabilité AWS partagée de s'applique à la protection des données dans Amazon Route 53. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez Questions fréquentes (FAQ) sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagée AWS et RGPD (Règlement général sur la protection des données) sur le Blog de sécuritéAWS .

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- SSL/TLS À utiliser pour communiquer avec AWS les ressources. Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail. Pour plus d'informations sur l'utilisation des CloudTrail sentiers pour capturer AWS des activités, consultez la section Utilisation des CloudTrail sentiers dans le guide de AWS CloudTrail l'utilisateur.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-3 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d'informations sur les points de terminaison FIPS disponibles, consultez Norme FIPS (Federal Information Processing Standard) 140-3.

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Nom. Cela inclut lorsque vous travaillez avec Route 53 ou autre à Services AWS l'aide de

la console, de l'API ou AWS SDKs. AWS CLI Toutes les données que vous entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

Protection contre les registres de délégation suspendu dans Route 53

Avec Route 53, un client peut créer une zone hébergée, par exemple `example.com` pour héberger ses enregistrements DNS. Chaque zone hébergée est fournie avec un « ensemble de délégations », qui est un ensemble de quatre serveurs de noms qu'un client peut utiliser pour configurer les enregistrements NS dans le domaine parent. Ces enregistrements NS peuvent être appelés « enregistrements NS de délégation » ou « enregistrements de délégation ».

Pour que la zone hébergée `example.com` Route 53 fasse autorité, le propriétaire légitime du `example.com` domaine doit configurer les enregistrements de délégation dans son domaine parent « .com » via le bureau d'enregistrement de domaines. Si un client perd l'accès aux quatre serveurs de noms configurés dans le domaine parent, par exemple parce que la zone hébergée associée est supprimée, cela peut créer un risque qu'un attaquant peut exploiter. C'est ce que l'on appelle le risque de « pendaison des dossiers de délégation ».

Route 53 protège contre le risque lié aux records de délégation en cas de suppression d'une zone hébergée. Après la suppression, si une nouvelle zone hébergée est créée avec le même nom de domaine, Route 53 vérifiera si les enregistrements de délégation pointant vers la zone hébergée supprimée sont toujours présents dans le domaine parent. Si tel est le cas, Route 53 empêchera l'attribution de serveurs de noms qui se chevauchent. Il s'agit du scénario 1 dans les exemples suivants.

Cependant, il existe d'autres risques liés aux dossiers de délégation, contre lesquels Route 53 ne peut pas se protéger, comme le décrivent les scénarios 2 et 3 dans les exemples suivants. Pour vous protéger contre cet ensemble plus large de risques, assurez-vous que les enregistrements NS du parent correspondent à la délégation définie pour la zone hébergée Route 53. Vous pouvez trouver l'ensemble de délégations d'une zone hébergée via la console Route 53 ou AWS CLI. Pour plus d'informations, consultez Liste des enregistrements ou get-hosted-zone.

En outre, l'activation de la signature DNSSEC pour une zone hébergée Route 53 peut constituer une couche de protection supplémentaire au-delà des meilleures pratiques mentionnées ci-dessus. Le protocole DNSSEC certifie que les réponses DNS proviennent d'une source faisant autorité,

protégeant ainsi efficacement contre ce risque. Pour de plus amples informations, veuillez consulter Configuration de la signature DNSSEC dans Amazon Route 53.

Exemples

Dans les exemples suivants, nous supposons que vous avez un domaine `example.com` et son domaine enfant`child.example.com`. Nous expliquerons comment, dans différents scénarios, des enregistrements de délégation suspendus peuvent être créés, comment Route 53 protège votre domaine contre les abus et comment atténuer efficacement les risques associés aux enregistrements de délégation suspendus.

Scénario 1:

Vous créez une zone hébergée `child.example.com` avec quatre serveurs de noms : <ns1><ns2>,<ns3>, et<ns4>. Vous configurez correctement la délégation dans la zone hébergée`example.com`, en créant des enregistrements NS `child.example.com` de délégation pour quatre serveurs de noms <ns1><ns2>,<ns3>, et<ns4>. Lorsque la zone `child.example.com` hébergée est supprimée sans supprimer les enregistrements NS de la délégation dans laquelle se trouvent les enregistrements`example.com`, Route 53 `child.example.com` protège contre le risque lié aux enregistrements de délégation en empêchant <ns1><ns2><ns3>, et <ns4>en empêchant leur attribution à des zones hébergées nouvellement créées avec le même nom de domaine.

Scénario 2:

Similaire au scénario 1, mais cette fois, vous supprimez la zone hébergée pour enfants ET les enregistrements NS de la délégation dans la zone hébergée`example.com`. Toutefois, vous pouvez réajouter des enregistrements NS de délégation <ns1><ns2>,<ns3>, <ns4>sans créer de zone hébergée pour enfants. Ici,<ns1>, <ns2><ns3>, et <ns4>sont en suspens les dossiers de délégation, car Route 53 supprime le blocage, qui empêchait<ns1>, <ns2><ns3>, et d'<ns4>être attribué et autorisera désormais les zones hébergées nouvellement créées à utiliser au-dessus des serveurs de noms. Pour atténuer les risques, supprimez, <ns1><ns2><ns3>, et des <ns4>enregistrements de délégation et ajoutez-les à nouveau uniquement une fois que la zone hébergée par l'enfant a été créée.

Scénario 3 :

Dans ce scénario, vous créez un ensemble de délégations réutilisables Route 53 avec des serveurs de noms <ns1><ns2>,<ns3>, et<ns4>. Vous déléguez ensuite le domaine `example.com` à ces serveurs de noms dans le domaine parent`.com`. Cependant, vous n'avez

pas encore créé la zone `example.com` hébergée pour l'ensemble de délégations réutilisable. Voici,<ns1>, <ns2><ns3>, et <ns4>pendent des dossiers de délégation. Pour atténuer le risque, créez la zone hébergée à l'aide du jeu de délégation réutilisable avec les serveurs de noms <ns1><ns2><ns3>,, et<ns4>.

Identity and Access Management dans Amazon Route 53

Pour effectuer toute opération sur les ressources Amazon Route 53, telle que l'enregistrement d'un domaine ou la mise à jour d'un enregistrement, AWS Identity and Access Management (IAM) vous oblige à authentifier que vous êtes un utilisateur approuvé AWS . Si vous utilisez la console Route 53, vous authentifiez votre identité en fournissant votre nom d'utilisateur AWS et un mot de passe.

Après avoir authentifié votre identité, IAM contrôle votre accès AWS en vérifiant que vous êtes autorisé à effectuer des opérations et à accéder aux ressources. Si vous êtes un administrateur de compte, vous pouvez utiliser IAM pour contrôler l'accès d'autres utilisateurs aux ressources qui sont associées à votre compte.

Ce chapitre explique comment utiliser IAM et Route 53 pour aider à sécuriser vos ressources.

Rubriques

- Authentification par des identités
- Contrôle d’accès
- Présentation de la gestion des autorisations d'accès à vos ressources Amazon Route 53
- Utilisation des stratégies basées sur l'identité (stratégies IAM) pour Amazon Route 53
- Utilisation des rôles liés à un service pour Amazon Route 53 Resolver
- AWS politiques gérées pour Amazon Route 53
- Utilisation de conditions de politique IAM pour un contrôle d’accès précis
- Autorisations d'API Amazon Route 53 : référence des actions, ressources et conditions

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. Vous devez être authentifié (connecté à AWS) en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

Vous pouvez vous connecter en AWS tant qu'identité fédérée en utilisant les informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center Les utilisateurs (IAM Identity Center), l'authentification unique de votre entreprise et vos informations d'identification Google ou Facebook sont des exemples d'identités fédérées. Lorsque vous vous connectez avec une identité fédérée, votre administrateur aura précédemment configuré une fédération d'identités avec des rôles IAM. Lorsque vous accédez à AWS l'aide de la fédération, vous assumez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter au portail AWS Management Console ou au portail AWS d'accès. Pour plus d'informations sur la connexion à AWS, consultez la section Comment vous connecter à votre compte Compte AWS dans le guide de Connexion à AWS l'utilisateur.

Si vous y accédez AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. Si vous n'utilisez pas d' AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer des demandes vous-même, consultez AWS Signature Version 4 pour les demandes d'API dans le Guide de l'utilisateur IAM.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être fournir des informations de sécurité supplémentaires. Par exemple, il vous AWS recommande d'utiliser l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour plus d'informations, consultez Authentification multifactorielle dans le Guide de l'utilisateur AWS IAM Identity Center et Authentification multifactorielle AWS dans IAM dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes Services AWS les ressources du compte. Cette identité est appelée utilisateur Compte AWS root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent de vous connecter en tant qu'utilisateur racine, consultez Tâches nécessitant des informations d'identification d'utilisateur racine dans le Guide de l'utilisateur IAM.

Identité fédérée

La meilleure pratique consiste à obliger les utilisateurs humains, y compris ceux qui ont besoin d'un accès administrateur, à utiliser la fédération avec un fournisseur d'identité pour accéder à l'aide Services AWS d'informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, d'un fournisseur d'identité Web AWS Directory Service, du répertoire Identity Center ou de tout utilisateur qui y accède à l'aide des informations d'identification fournies Services AWS par le biais d'une source d'identité. Lorsque des identités fédérées y accèdent Comptes AWS, elles assument des rôles, qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Vous pouvez créer des utilisateurs et des groupes dans IAM Identity Center, ou vous pouvez vous connecter et synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité afin de les utiliser dans toutes vos applications Comptes AWS et applications. Pour obtenir des informations sur IAM Identity Center, consultez Qu'est-ce que IAM Identity Center ? dans le Guide de l'utilisateur AWS IAM Identity Center .

Utilisateurs et groupes IAM

Un utilisateur IAM est une identité au sein de vous Compte AWS qui possède des autorisations spécifiques pour une seule personne ou application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des utilisateurs IAM ayant des informations d'identification à long terme telles que des mots de passe et des clés d'accès. Toutefois, si certains cas d'utilisation spécifiques nécessitent des informations d'identification à long terme avec les utilisateurs IAM, nous vous recommandons d'effectuer une rotation des clés d'accès. Pour plus d'informations, consultez Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification dans le Guide de l'utilisateur IAM.

Un groupe IAM est une identité qui concerne un ensemble d'utilisateurs IAM. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez nommer un groupe IAMAdminset lui donner les autorisations nécessaires pour administrer les ressources IAM.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin.

Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des informations d'identification temporaires. Pour plus d'informations, consultez Cas d'utilisation pour les utilisateurs IAM dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une identité au sein de vous Compte AWS dotée d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais le rôle IAM n'est pas associé à une personne en particulier. Pour assumer temporairement un rôle IAM dans le AWS Management Console, vous pouvez passer d'un rôle d'utilisateur à un rôle IAM (console). Vous pouvez assumer un rôle en appelant une opération d' AWS API AWS CLI ou en utilisant une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez Méthodes pour endosser un rôle dans le Guide de l'utilisateur IAM.

Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

- Accès utilisateur fédéré : pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour obtenir des informations sur les rôles pour la fédération, consultez Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM. Si vous utilisez IAM Identity Center, vous configurez un jeu d'autorisations. IAM Identity Center met en corrélation le jeu d'autorisations avec un rôle dans IAM afin de contrôler à quoi vos identités peuvent accéder après leur authentification. Pour plus d'informations sur les jeux d'autorisations, consultez Jeux d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .
- Autorisations d'utilisateur IAM temporaires : un rôle ou un utilisateur IAM peut endosser un rôle IAM pour profiter temporairement d'autorisations différentes pour une tâche spécifique.
- Accès intercompte : vous pouvez utiliser un rôle IAM pour permettre à un utilisateur (principal de confiance) d'un compte différent d'accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Toutefois, dans certains Services AWS cas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour en savoir plus sur la différence entre les rôles et les politiques basées sur les ressources pour l'accès intercompte, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.
- Accès multiservices — Certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service

peut le faire en utilisant les autorisations d'appel du principal, un rôle de service ou un rôle lié au service.

- Sessions d'accès direct (FAS) : lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez Transmission des sessions d'accès.
- Rôle de service : il s'agit d'un rôle IAM attribué à un service afin de réaliser des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer un rôle de service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.
- Rôle lié à un service — Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un rôle IAM pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une EC2 instance et qui envoient des demandes AWS CLI d' AWS API. Cela est préférable au stockage des clés d'accès dans l' EC2 instance. Pour attribuer un AWS rôle à une EC2 instance et le rendre disponible pour toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes exécutés sur l' EC2 instance d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez Utiliser un rôle IAM pour accorder des autorisations aux applications exécutées sur des EC2 instances Amazon dans le guide de l'utilisateur IAM.

Contrôle d'accès

Pour créer, mettre à jour, supprimer ou répertorier des ressources Amazon Route 53, vous devez détenir les autorisations nécessaires pour effectuer l'opération et pour accéder aux ressources correspondantes.

Les sections suivantes décrivent comment gérer les autorisations pour Route 53. Nous vous recommandons de lire d'abord la présentation.

Présentation de la gestion des autorisations d'accès à vos ressources Amazon Route 53

Chaque AWS ressource appartient à un AWS compte, et les autorisations de création ou d'accès à une ressource sont régies par des politiques d'autorisation.

> **Note**
>
> Un administrateur de compte (ou utilisateur administrateur) est un utilisateur détenant des privilèges d'administrateur. Pour de plus amples informations sur les administrateurs, veuillez consulter Bonnes pratiques IAM dans le Guide de l'utilisateur IAM.

Lorsque vous accordez des autorisations, vous décidez qui obtient les autorisations, pour quelles ressources, ainsi que les actions autorisées.

Les utilisateurs ont besoin d'un accès programmatique s'ils souhaitent interagir avec AWS l'extérieur du AWS Management Console. La manière d'accorder un accès programmatique dépend du type d'utilisateur qui y accède AWS.

Pour accorder aux utilisateurs un accès programmatique, choisissez l'une des options suivantes.

Quel utilisateur a besoin d'un accès programmatique ?	Pour	Par
Identité de la main-d'œuvre (Utilisateurs gérés dans IAM Identity Center)	Utilisez des informations d'identification temporaires pour signer les demandes programmatiques adressées au AWS CLI AWS SDKs, ou AWS APIs.	Suivez les instructions de l'interface que vous souhaitez utiliser. • Pour le AWS CLI, voir Configuration du AWS CLI à utiliser AWS IAM Identity Center dans le guide de AWS Command Line Interface l'utilisateur.

Quel utilisateur a besoin d'un accès programmatique ?	Pour	Par
		• Pour AWS SDKs, outils, et AWS APIs, voir Authentification IAM Identity Center dans le guide de référence AWS SDKs et Tools.
IAM	Utilisez des informations d'identification temporaires pour signer les demandes programmatiques adressées au AWS CLI AWS SDKs, ou AWS APIs.	Suivez les instructions de la section Utilisation d'informations d'identification temporaires avec AWS les ressources du Guide de l'utilisateur IAM.
IAM	(Non recommandé) Utilisez des informations d'identification à long terme pour signer des demandes programmatiques adressées au AWS CLI AWS SDKs, ou AWS APIs.	Suivez les instructions de l'interface que vous souhaitez utiliser. • Pour le AWS CLI, voir Authentification à l'aide des informations d'identification utilisateur IAM dans le Guide de l'AWS Command Line Interface utilisateur. • Pour les outils AWS SDKs et, voir Authentifier à l'aide d'informations d'identification à long terme dans le guide de référence des outils AWS SDKs et. • Pour AWS APIs, voir Gestion des clés d'accès pour les utilisateurs IAM dans le Guide de l'utilisateur IAM.

Rubriques

- ARNs pour les ressources Amazon Route 53
- Présentation de la propriété des ressources
- Gestion de l'accès aux ressources
- Spécification des éléments d'une stratégie : ressources, actions, effets et mandataires
- Spécification de conditions dans une politique

ARNs pour les ressources Amazon Route 53

Amazon Route 53 prend en charge différents types de ressources pour DNS, la surveillance de l'état et l'enregistrement de domaine. Dans une stratégie, vous pouvez accorder ou refuser l'accès aux ressources suivantes en utilisant * pour l'ARN :

- Surveillance de l'état
- Zones hébergées
- Ensembles de délégations réutilisables
- Statut d'un lot de modifications d'un jeu d'enregistrements de ressources (API uniquement)
- Stratégies de trafic (flux de trafic)
- Instances de stratégies de trafic (flux de trafic)

Certaines ressources Route 53 ne prennent pas en charge les autorisations. Vous ne pouvez pas accorder ni refuser l'accès aux ressources suivantes :

- Domaines
- Enregistrements individuels
- Balises pour les domaines
- Balises pour les surveillances de l'état
- Balises pour les zones hébergées

Route 53 fournit des actions d'API pour utiliser chacun de ces types de ressources. Pour plus d'informations, consultez la référence d'API Amazon Route 53. Pour une liste des actions et l'ARN que vous spécifiez pour accorder ou refuser l'autorisation d'utiliser chaque action, consultez la section Autorisations d'API Amazon Route 53 : référence des actions, ressources et conditions.

Présentation de la propriété des ressources

Un AWS compte possède les ressources qui y sont créées, quelle que soit la personne qui les a créées. Plus précisément, le propriétaire de la ressource est le AWS compte de l'entité principale (c'est-à-dire le compte root ou un rôle IAM) qui authentifie la demande de création de ressource.

Les exemples suivants illustrent comment cela fonctionne :

- Si vous utilisez les informations d'identification du compte root de votre AWS compte pour créer une zone hébergée, votre AWS compte est le propriétaire de la ressource.
- Si vous créez un utilisateur dans votre AWS compte et que vous accordez l'autorisation de créer une zone hébergée à cet utilisateur, celui-ci peut créer une zone hébergée. Toutefois, votre compte AWS , auquel l'utilisateur appartient, détient la ressource des zones hébergées.
- Si vous créez un rôle IAM dans votre AWS compte avec les autorisations nécessaires pour créer une zone hébergée, toute personne pouvant assumer ce rôle peut créer une zone hébergée. Votre AWS compte, auquel appartient le rôle, possède la ressource de zone hébergée.

Gestion de l’accès aux ressources

Une politique d'autorisation précise qui a accès à quoi. Cette section présente les options de création de politiques d'autorisation pour Amazon Route 53. Pour obtenir des informations d'ordre général sur la syntaxe et les descriptions des politiques IAM, consultez Présentation des politiques AWS IAM dans le Guide de l'utilisateur IAM.

Les stratégies attachées à une identité IAM sont appelées stratégies basées sur l'identité (stratégies IAM) et les stratégies attachées à une ressource sont appelées stratégies basées sur une ressource. Route 53 prend en charge uniquement les stratégies basées sur l'identité (stratégies IAM).

Rubriques

- Politiques basées sur une identité (politiques IAM)
- Politiques basées sur les ressources

Politiques basées sur une identité (politiques IAM)

Vous pouvez attacher des politiques à des identités IAM. Par exemple, vous pouvez effectuer les opérations suivantes :

- Attacher une stratégie d'autorisation à un utilisateur ou à un groupe dans votre compte – Un administrateur de compte peut utiliser une stratégie d'autorisation associée à un utilisateur particulier pour autoriser cet utilisateur à créer des ressources Amazon Route 53.
- Associer une politique d'autorisation à un rôle (accorder des autorisations entre comptes) : vous pouvez autoriser un utilisateur créé par un autre AWS compte à effectuer des actions Route 53. Pour ce faire, vous attachez une politique d'autorisations à un rôle IAM, puis vous autorisez l'utilisateur dans l'autre compte à assumer le rôle. L'exemple suivant explique comment cela fonctionne pour les deux comptes AWS , le compte A et le compte B :
  1. L'administrateur du Compte A crée un rôle IAM et attache une politique d'autorisations à ce rôle qui accorde des autorisations de création ou d'accès à des ressources qui sont la propriété du Compte A.
  2. L'administrateur du compte A accorde une politique d'approbation au rôle. La politique d'approbation identifie le Compte B comme le compte principal pouvant assumer le rôle.
  3. L'administrateur du Compte B peut ensuite déléguer des autorisations pour assumer le rôle à des utilisateurs ou groupes du Compte B. Cela permet aux utilisateurs du Compte B de créer ou d'accéder aux ressources du Compte A.

  Pour plus d'informations sur la façon de déléguer des autorisations aux utilisateurs d'un autre AWS compte, consultez la section Gestion des accès dans le guide de l'utilisateur IAM.

L'exemple de stratégie suivant permet à un utilisateur d'exécuter l'action `CreateHostedZone` afin de créer une zone hébergée publique pour n'importe quel compte AWS :

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53:CreateHostedZone"
            ],
            "Resource":"*"
        }
    ]
}
```

Si vous souhaitez que la politique s'applique également aux zones hébergées privées, vous devez accorder des autorisations pour utiliser l'`AssociateVPCWithHostedZone`action Route 53 et deux EC2 actions Amazon, `DescribeVpcs` et`DescribeRegion`, comme indiqué dans l'exemple suivant :

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53:CreateHostedZone",
                "route53:AssociateVPCWithHostedZone"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs",
                "ec2:DescribeRegions"
            ],
            "Resource": "*"
        }
    ]
}
```

Pour plus d'informations sur l'attachement de stratégies aux identités pour Route 53, consultez Utilisation des stratégies basées sur l'identité (stratégies IAM) pour Amazon Route 53. Pour plus d'informations sur les utilisateurs, les groupes, les rôles et les autorisations, consultez Identités (utilisateurs, groupes et rôles) dans le Guide de l'utilisateur IAM.

Politiques basées sur les ressources

D'autres services, tels que Amazon S3, prennent également en charge l'attachement de stratégies d'autorisation aux ressources. Par exemple, vous pouvez attacher une politique à un compartiment S3 pour gérer les autorisations d'accès à ce compartiment. Amazon Route 53 ne prend pas en charge l'attachement de stratégies aux ressources.

Spécification des éléments d'une stratégie : ressources, actions, effets et mandataires

Amazon Route 53 inclut des actions d'API (consultez la Référence d'API Amazon Route 53) que vous pouvez utiliser sur chaque ressource Route 53 (voirARNs pour les ressources Amazon Route 53). Vous pouvez accorder à un utilisateur ou à un utilisateur fédéré les autorisations nécessaires pour effectuer tout ou partie de ces actions. Notez que certaines actions d'API, telles que l'enregistrement d'un domaine, requièrent des autorisations pour effectuer plusieurs actions.

Voici les éléments de base d'une politique :

- Ressource : vous utilisez un nom Amazon Resource Name (ARN) pour identifier la ressource à laquelle s'applique la politique. Pour de plus amples informations, veuillez consulter ARNs pour les ressources Amazon Route 53.
- Action : vous utilisez des mots clés d'action pour identifier les opérations de ressource que vous voulez accorder ou refuser. Par exemple, en fonction de l'élément `Effect` indiqué, l'autorisation `route53:CreateHostedZone` accorde ou refuse à un utilisateur la possibilité d'exécuter l'action `CreateHostedZone` Route 53.
- Effet : vous spécifiez l'effet, autoriser ou refuser, lorsqu'un utilisateur tente d'exécuter l'action sur la ressource spécifiée. Si vous n'accordez pas explicitement l'accès à une action, l'accès est implicitement refusé. Vous pouvez aussi explicitement refuser l'accès à une ressource, ce que vous pouvez faire afin de vous assurer qu'un utilisateur n'y a pas accès, même si une politique différente accorde l'accès.
- Principal – dans les politiques basées sur une identité (politiques IAM), l'utilisateur auquel la politique est attachée est le principal implicite. Pour les politiques basées sur une ressource, vous spécifiez l'utilisateur, le compte, le service ou une autre entité qui doit recevoir les autorisations (s'applique uniquement aux politiques basées sur une ressource). Route 53 ne prend pas en charge les stratégies basées sur une ressource.

Pour plus d'informations sur la syntaxe et les descriptions des politiques IAM, consultez Référence de politique AWS IAM dans le Guide de l'utilisateur IAM.

Pour obtenir une des tableaux présentant toutes les opérations d'API Route 53, ainsi que les ressources auxquelles elles s'appliquent, consultez Autorisations d'API Amazon Route 53 : référence des actions, ressources et conditions.

Spécification de conditions dans une politique

Lorsque vous accordez des autorisations, vous pouvez utiliser le langage d'access policy IAM pour indiquer quand une politique doit prendre effet. Par exemple, il est possible d'appliquer une politique après seulement une date spécifique. Pour plus d'informations sur la spécification des conditions dans un langage de stratégie, veuillez consulter la rubrique Éléments de stratégie IAM JSON : Condition dans le Guide de l'utilisateur IAM.

Pour exprimer des conditions, vous utilisez des clés de condition prédéfinies. Il n'existe pas de clés de condition spécifiques à Route 53. Cependant, il existe de AWS larges clés d'état que vous pouvez utiliser selon vos besoins. Pour obtenir la liste complète des touches AWS larges, consultez la section Clés disponibles pour connaître les conditions dans le guide de l'utilisateur IAM.

Utilisation des stratégies basées sur l'identité (stratégies IAM) pour Amazon Route 53

Cette rubrique fournit des exemples de stratégies basées sur l'identité qui montrent comment un administrateur de compte peut lier des stratégies d'autorisations à des identités IAM et accorder ainsi des autorisations pour effectuer des opérations sur les ressources Amazon Route 53.

> **Important**
>
> Nous vous recommandons d'examiner d'abord les rubriques de présentation qui détaillent les concepts de base et les options de gestion de l'accès à vos ressources Route 53. Pour de plus amples informations, veuillez consulter Présentation de la gestion des autorisations d'accès à vos ressources Amazon Route 53.

> **Note**
>
> Lors de l'autorisation d'accès, la zone hébergée et Amazon VPC doivent appartenir à la même partition. Une partition est un groupe de Régions AWS. Chacune Compte AWS est limitée à une partition.
> Les partitions prises en charge sont les suivantes :
>
> - `aws` - Régions AWS
> - `aws-cn` - Régions chinoises
> - `aws-us-gov` - AWS GovCloud (US) Region

Pour plus d'informations, consultez la section Access Management (Gestion des accès) et Amazon Route 53 endpoints and quotas (points de terminaison et quotas Amazon Route 53) dans la Référence générale AWS .

Rubriques

- Autorisations requises pour utiliser la console Amazon Route 53
- Exemples d'autorisations pour un propriétaire d'enregistrement de domaine
- Autorisations de clé gérées par le client Route 53 requises pour la signature DNSSEC
- Exemples de politiques gérées par le client

Voici un exemple de stratégie d'autorisation. Le `Sid`, ou ID de l'instruction, est facultatif :

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": "*"
        }
    ]
}
```

La stratégie comprend deux déclarations :

- La première instruction accorde des autorisations aux actions requises pour créer et gérer des zones hébergées publiques et leurs enregistrements. Le caractère générique (*) dans le nom de ressource Amazon (ARN) donne accès à toutes les zones hébergées détenues par le AWS compte courant.
- La deuxième déclaration accorde des autorisations à toutes les actions qui sont nécessaires pour créer et gérer les surveillance de l'état.

Pour une liste des actions et l'ARN que vous spécifiez pour accorder ou refuser l'autorisation d'utiliser chaque action, consultez la section Autorisations d'API Amazon Route 53 : référence des actions, ressources et conditions.

Autorisations requises pour utiliser la console Amazon Route 53

Pour accorder un accès complet à la console Amazon Route 53, vous accordez les autorisations dans la stratégie d'autorisations suivante :

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"
        }
    ]
```

```
}
```

Voici pourquoi les autorisations sont obligatoires :

`route53:*`

Permet d'exécuter toutes les actions Route 53, sauf les actions suivantes :

- Créez et mettez à jour des enregistrements d'alias pour lesquels la valeur d'Alias Target est une CloudFront distribution, un équilibreur de charge Elastic Load Balancing, un environnement Elastic Beanstalk ou un bucket Amazon S3. (Avec ces autorisations, vous pouvez créer des enregistrements d'alias pour lesquels la valeur de Alias Target est un autre enregistrement dans la même zone hébergée.)
- Utiliser des zones hébergées privées.
- Utiliser des domaines.
- Créez, supprimez et visualisez les CloudWatch alarmes.
- Afficher CloudWatch les métriques dans la console Route 53.

`route53domains:*`

Permet d'utiliser des domaines.

> **Important**
>
> Si vous répertoriez les actions `route53` individuellement, vous devez inclure `route53:CreateHostedZone` pour utiliser des domaines. Lorsque vous enregistrez un domaine, une zone hébergée est créée simultanément. Une stratégie qui inclut l'autorisation d'enregistrer des domaines doit donc également inclure l'autorisation de créer des zones hébergées.

Pour l'enregistrement de domaine, Route 53 ne prend pas en charge l'octroi ou le refus d'autorisations à des ressources individuelles.

`route53resolver:*`

Permet d'utiliser Route 53 Resolver.

`ssm:GetParametersByPath`

Vous permet de récupérer des régions accessibles au public lorsque vous créez de nouveaux enregistrements d'alias, des zones hébergées privées et des surveillances de l'état.

`cloudfront:ListDistributions`

Permet de créer et de mettre à jour des enregistrements d'alias pour lesquels la valeur d'Alias Target est une CloudFront distribution.

Ces autorisations ne sont pas nécessaires si vous n'utilisez pas la console Route 53. Route 53 l'utilise uniquement pour obtenir une liste des distributions à afficher dans la console.

`elasticloadbalancing:DescribeLoadBalancers`

Permet de créer et de mettre à jour des enregistrements d'alias pour lesquels la valeur de Alias Target (Cible de l'alias) est un équilibreur de charge ELB.

Ces autorisations ne sont pas nécessaires si vous n'utilisez pas la console Route 53. Route 53 l'utilise uniquement pour obtenir une liste des équilibreurs de charge à afficher dans la console.

`elasticbeanstalk:DescribeEnvironments`

Permet de créer et de mettre à jour des enregistrements d'alias pour lesquels la valeur de Alias Target (Cible de l'alias) est un environnement Elastic Beanstalk.

Ces autorisations ne sont pas nécessaires si vous n'utilisez pas la console Route 53. Route 53 l'utilise uniquement pour obtenir une liste des environnements à afficher dans la console.

`s3:ListAllMyBuckets`, **`s3:GetBucketLocation`** et **`s3:GetBucketWebsite`**

Permet de créer et de mettre à jour des enregistrements d'alias pour lesquels la valeur de Alias Target (Cible de l'alias) est un compartiment Amazon S3. (Vous pouvez créer un alias dans un compartiment Amazon S3 uniquement si le compartiment est configuré en tant que point de terminaison de site web ; `s3:GetBucketWebsite` obtient les informations de configuration nécessaires.)

Ces autorisations ne sont pas nécessaires si vous n'utilisez pas la console Route 53. Route 53 l'utilise uniquement pour obtenir une liste des compartiments à afficher dans la console.

`ec2:DescribeVpcs` et **`ec2:DescribeRegions`**

Permet d'utiliser des zones hébergées privées.

Toutes les autorisations **`ec2`** répertoriées

Permet d'utiliser Route 53 Resolver.

`sns:ListTopics`, **`sns:ListSubscriptionsByTopic`**, **`sns:CreateTopic`**, **`cloudwatch:DescribeAlarms`**, **`cloudwatch:PutMetricAlarm`**, **`cloudwatch:DeleteAlarms`**

Vous permet de créer, de supprimer et de consulter les CloudWatch alarmes.

`cloudwatch:GetMetricStatistics`

Vous permet de créer des CloudWatch bilans de santé métriques.

Ces autorisations ne sont pas nécessaires si vous n'utilisez pas la console Route 53. Route 53 l'utilise uniquement pour obtenir des statistiques à afficher dans la console.

`apigateway:GET`

Permet de créer et de mettre à jour des enregistrements d'alias pour lesquels la valeur Alias Target (Cible de l'alias) est une API Amazon API Gateway.

Cette autorisation n'est pas nécessaire si vous n'utilisez pas la console Route 53. Route 53 l'utilise uniquement pour obtenir une liste de APIs à afficher dans la console.

`kms:*`

Vous permet de travailler avec AWS KMS pour activer la signature DNSSEC.

Exemples d'autorisations pour un propriétaire d'enregistrement de domaine

Avec les autorisations d'ensemble d'enregistrements de ressources, vous pouvez définir des autorisations granulaires qui limitent ce que l' AWS utilisateur peut mettre à jour ou modifier. Pour de plus amples informations, veuillez consulter Utilisation de conditions de politique IAM pour un contrôle d'accès précis.

Dans certains scénarios, un propriétaire de zone hébergée peut être responsable de la gestion globale de la zone hébergée, tandis qu'une autre personne de l'organisation est responsable d'un sous-ensemble de ces tâches. Un propriétaire de zone hébergée qui a activé la signature DNSSEC, par exemple, peut souhaiter créer une politique IAM qui inclut l'autorisation pour quelqu'un d'autre d'ajouter et de supprimer des enregistrements d'ensembles de ressources (RRs) dans la zone hébergée, entre autres tâches. Les autorisations spécifiques qu'un propriétaire de zone hébergée choisit d'activer pour un propriétaire d'enregistrement ou d'autres personnes dépendent de la stratégie de leur organisation.

Voici un exemple de politique IAM qui permet au propriétaire d'un enregistrement d'apporter des modifications aux RRs politiques de trafic et aux contrôles de santé. Un propriétaire d'enregistrement doté de cette stratégie n'est pas autorisé à effectuer des opérations au niveau de la zone, telles que la création ou la suppression d'une zone, l'activation ou la désactivation de la journalisation des requêtes, la création ou la suppression d'un jeu de délégations réutilisable ou la modification des paramètres DNSSEC.

```
{
      "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": [
        "*"
      ]
}
```

Autorisations de clé gérées par le client Route 53 requises pour la signature DNSSEC

Lorsque vous activez la signature DNSSEC pour Route 53, Route 53 crée une clé de signature clé (KSK) basée sur une clé gérée par le client dans (). AWS Key Management Service AWS KMS Vous pouvez utiliser une clé gérée par le client existante qui prend en charge la signature DNSSEC ou en créer une nouvelle. Route 53 doit être autorisé à accéder à votre clé gérée par le client afin de pouvoir créer la clé KSK pour vous.

Pour activer Route 53 pour accéder à votre clé gérée par le client, assurez-vous que votre stratégie de clé gérée par le client contient les instructions suivantes :

```
{
            "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
                }
            }
        }
```

Le problème de député confus est un problème de sécurité dans lequel une entité sans autorisation pour une action peut contraindre une entité plus privilégiée à le faire. Pour vous AWS KMS en protéger, vous pouvez éventuellement limiter les autorisations accordées à un service sur une ressource dans le cadre d'une politique basée sur les ressources en fournissant une combinaison de `aws:SourceArn` conditions (`aws:SourceAccount`les deux ou une seule). `aws:SourceAccount`est l'identifiant de AWS compte du propriétaire d'une zone hébergée. `aws:SourceArn`est l'ARN d'une zone hébergée.

Voici deux exemples d'autorisations que vous pouvez ajouter :

```
{
    "Sid": "Allow Route 53 DNSSEC Service",
    …
    "Resource": "*",
    "Condition": {
```

```
        "StringEquals": {
            "aws:SourceAccount": "111122223333"
        },
        "ArnEquals": {
            "aws:SourceArn": "arn:aws:route53:::hostedzone/HOSTED_ZONE_ID"
        }
    }
},
```

- Ou -

```
{
    "Sid": "Allow Route 53 DNSSEC Service",
    …
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": ["1111-2222-3333","4444-5555-6666"]
        },
        "ArnLike": {
            "aws:SourceArn": "arn:aws:route53:::hostedzone/*"
        }
    }
},
```

Pour de plus amples informations, veuillez consulter Le problème du député confus dans le Guide de l'utilisateur IAM.

Exemples de politiques gérées par le client

Vous pouvez créer vos propres stratégies IAM personnalisées pour accorder des autorisations pour des actions Route 53. Vous pouvez attacher ces politiques personnalisées aux groupes IAM qui nécessitent les autorisations spécifiées. Ces politiques fonctionnent lorsque vous utilisez l'API Route 53 AWS SDKs, la ou la AWS CLI. Les exemples suivants présentent des autorisations pour plusieurs cas d'utilisation courants. Pour accéder à la stratégie qui accorde à un utilisateur l'accès complet à Route 53, consultez Autorisations requises pour utiliser la console Amazon Route 53.

Exemples

- Exemple 1 : Autoriser l'accès en lecture à toutes les zones hébergées
- Exemple 2 : Autoriser la création et la suppression de zones hébergées

- Exemple 3 : Autoriser l'accès complet à tous les domaines (zones hébergées publiques uniquement)
- Exemple 4 : Autoriser la création de points de terminaison Route 53 Resolver entrants et sortants

Exemple 1 : Autoriser l'accès en lecture à toutes les zones hébergées

La stratégie d'autorisation suivante accorde à l'utilisateur l'autorisation de répertorier toutes les zones hébergées et d'afficher tous les enregistrements d'une zone hébergée.

JSON

```
{
    "Version": "2012-10-17",
    "Statement":[
        {
            "Effect":"Allow",
            "Action":[
                "route53:GetHostedZone",
                "route53:ListResourceRecordSets"
            ],
            "Resource":"*"
        },
        {
            "Effect":"Allow",
            "Action":["route53:ListHostedZones"],
            "Resource":"*"
        }
    ]
}
```

Exemple 2 : Autoriser la création et la suppression de zones hébergées

La stratégie d'autorisation suivante accorde aux utilisateurs l'autorisation de créer et de supprimer des zones hébergées, et de suivre l'avancement des modifications.

JSON

```
{
    "Version": "2012-10-17",
```

```
    "Statement":[
        {
            "Effect":"Allow",
            "Action":["route53:CreateHostedZone"],
            "Resource":"*"
        },
        {
            "Effect":"Allow",
            "Action":["route53:DeleteHostedZone"],
            "Resource":"*"
        },
        {
            "Effect":"Allow",
            "Action":["route53:GetChange"],
            "Resource":"*"
        }
    ]
}
```

Exemple 3 : Autoriser l'accès complet à tous les domaines (zones hébergées publiques uniquement)

La stratégie d'autorisation suivante accorde aux utilisateurs l'autorisation d'exécuter toutes les actions sur les enregistrements de domaines, y compris l'enregistrement de domaines et la création de zones hébergées.

JSON

```
{
    "Version": "2012-10-17",
    "Statement":[
        {
            "Effect":"Allow",
            "Action":[
                "route53domains:*",
                "route53:CreateHostedZone"
            ],
            "Resource":"*"
        }
    ]
}
```

Lorsque vous enregistrez un domaine, une zone hébergée est créée simultanément. Une stratégie qui inclut l'autorisation d'enregistrer des domaines doit donc également inclure l'autorisation de créer des zones hébergées. (Pour l'enregistrement de domaine, Route 53 ne prend pas en charge l'octroi d'autorisations à des ressources individuelles.)

Pour plus d'informations sur les autorisations requises pour utiliser des zones hébergées privées, consultez Autorisations requises pour utiliser la console Amazon Route 53.

Exemple 4 : Autoriser la création de points de terminaison Route 53 Resolver entrants et sortants

La stratégie d'autorisations suivante permet aux utilisateurs d'utiliser la console Route 53 pour créer des points de terminaison Resolver entrants et sortants.

Certaines de ces autorisations sont nécessaires uniquement pour créer des points de terminaison dans la console. Vous pouvez omettre ces autorisations si vous souhaitez accorder des autorisations uniquement pour créer des points de terminaison entrants et sortants par programmation :

- `route53resolver:ListResolverEndpoints` permet aux utilisateurs de voir la liste des points de terminaison entrants ou sortants afin qu'ils puissent vérifier qu'un point de terminaison a été créé.
- `DescribeAvailabilityZones` est nécessaire pour afficher la liste des zones de disponibilité.
- `DescribeVpcs`est nécessaire pour afficher une liste deVPCs.

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": "*"
        }
    ]
}
```

Utilisation des rôles liés à un service pour Amazon Route 53 Resolver

Route 53 Resolver utilise des rôles liés à un service AWS Identity and Access Management (IAM). Un rôle lié à un service est un type unique de rôle IAM lié directement à Resolver. Les rôles liés au service sont prédéfinis par Resolver et incluent toutes les autorisations dont le service a besoin pour appeler d'autres AWS services en votre nom.

Un rôle lié à un service simplifie la configuration de Resolver, car vous n'avez pas besoin d'ajouter manuellement les autorisations requises. Resolver définit les autorisations de ses rôles liés à un service ; sauf définition contraire, seul Resolver peut endosser ses rôles. Les autorisations définies comprennent la politique d'approbation et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

Vous pouvez supprimer un rôle lié à un service uniquement après la suppression préalable des ressources connexes. Vos ressources Resolver sont ainsi protégées, car vous ne pouvez pas involontairement supprimer l'autorisation d'accéder aux ressources.

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés à un service, veuillez consulter la section Services AWS qui fonctionnent avec IAM et recherchez les services avec un Yes (Oui) dans la colonne Rôle lié à un service. Choisissez un Yes (Oui) ayant un lien permettant de consulter la documentation du rôle lié à un service, pour ce service.

Rubriques

- Autorisations des rôles liés à un service pour Resolver
- Création d'un rôle lié à un service pour Resolver
- Modification d'un rôle lié à un service pour Resolver
- Suppression d'un rôle lié à un service pour Resolver
- Régions prises en charge pour les rôles liés à un service Resolver

Autorisations des rôles liés à un service pour Resolver

Résolveur utilise le rôle lié à un service **`AWSServiceRoleForRoute53Resolver`** pour fournir des journaux de requêtes en votre nom.

La stratégie d'autorisations liée au rôle permet à Resolver de réaliser les actions suivantes sur l'ensemble de vos ressources :

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": "*"
    }
  ]
}
```

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour plus d’informations, consultez Service-Linked Role Permissions (autorisations du rôle lié à un service) dans le Guide de l’utilisateur IAM.

Création d'un rôle lié à un service pour Resolver

Vous n’avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous créez une association de configuration du journal des requêtes du résolveur dans la console Amazon Route 53, dans l' AWS CLI API ou dans l' AWS API, Resolver crée le rôle lié au service pour vous.

> **Important**
>
> Ce rôle lié à un service peut apparaître dans votre compte si vous avez effectué une action dans un autre service qui utilise les fonctions prises en charge par ce rôle. De même, si vous utilisiez Resolver avant le 12 août 2020, quand il commençait à prendre en charge les rôles liés à un service, Resolver créait le rôle `AWSServiceRoleForRoute53Resolver` dans votre compte. Pour plus d'informations, consultez A New Role Appeared in My IAM Account (Un nouveau rôle est apparu dans mon compte IAM).

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous créez une association de configuration de journalisation des requêtes de Resolver, le rôle lié à un service `AWSServiceRoleForRoute53Resolver` est recréé pour vous.

Modification d'un rôle lié à un service pour Resolver

Resolver ne vous permet pas de modifier le rôle lié à un service `AWSServiceRoleForRoute53Resolver`. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour plus d'informations, consultez Modification d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Suppression d'un rôle lié à un service pour Resolver

Si vous n'avez plus besoin d'utiliser une fonctionnalité ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous n'avez aucune entité inutilisée qui n'est pas surveillée ou gérée activement. Cependant, vous devez nettoyer les ressources de votre rôle lié à un service avant de pouvoir les supprimer manuellement.

> **Note**
>
> Si le service Resolver utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression peut échouer. Si cela se produit, patientez quelques minutes et réessayez.

Pour supprimer les ressources Resolver utilisées par le service **`AWSServiceRoleForRoute53Resolver`**

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Développez le menu de la console Route 53. Dans le coin supérieur gauche de la console, sélectionnez l'icone des trois barres horizontales

   (≡
3. Dans le menu Resolver, choisissez Query logging (Journalisation des requêtes).
4. Cochez la case en regard du nom de votre configuration de journalisation des requêtes, puis choisissez Delete (Supprimer).
5. Dans la zone de texte Delete query logging configuration (Supprimer la configuration de journalisation des requêtes), sélectionnez Stop logging queries (Arrêter les requêtes de journalisation).

   Cela va dissocier la configuration du VPC. Vous pouvez également dissocier la configuration de journalisation des requêtes par programme. Pour plus d'informations, consultez disassociate-resolver-query-log-config.
6. Une fois les requêtes de journalisation arrêtées, vous pouvez éventuellement taper **`delete`** dans le champ et choisir Delete (Supprimer) pour supprimer la configuration de journalisation des requêtes. Toutefois, cela n'est pas nécessaire pour supprimer les ressources utilisées par `AWSServiceRoleForRoute53Resolver`.

Pour supprimer manuellement le rôle lié à un service à l'aide d'IAM

Utilisez la console IAM, le AWS CLI, ou l' AWS API pour supprimer le rôle lié au `AWSServiceRoleForRoute53Resolver` service. Pour plus d'informations, consultez Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Régions prises en charge pour les rôles liés à un service Resolver

Resolver ne prend pas en charge l'utilisation de rôles liés à un service dans toutes les régions où le service est disponible. Vous pouvez utiliser le rôle `AWSServiceRoleForRoute53Resolver` dans les régions suivantes :

Nom de la région	Identité de la région	Prise en charge dans Resolver
US East (Virginie du Nord)	us-east-1	Oui
USA Est (Ohio)	us-east-2	Oui
USA Ouest (Californie du Nord)	us-west-1	Oui
USA Ouest (Oregon)	us-west-2	Oui
Asie-Pacifique (Mumbai)	ap-south-1	Oui
Asie-Pacifique (Osaka)	ap-northeast-3	Oui
Asie-Pacifique (Séoul)	ap-northeast-2	Oui
Asie-Pacifique (Singapour)	ap-southeast-1	Oui
Asie-Pacifique (Sydney)	ap-southeast-2	Oui
Asie-Pacifique (Tokyo)	ap-northeast-1	Oui
Canada (Centre)	ca-central-1	Oui
Europe (Francfort)	eu-central-1	Oui
Europe (Irlande)	eu-west-1	Oui
Europe (Londres)	eu-west-2	Oui
Europe (Paris)	eu-west-3	Oui
Amérique du Sud (São Paulo)	sa-east-1	Oui
Chine (Pékin)	cn-north-1	Oui
Chine (Ningxia)	cn-northwest-1	Oui
AWS GovCloud (US)	us-gov-east-1	Oui
AWS GovCloud (US)	us-gov-west-1	Oui

AWS politiques gérées pour Amazon Route 53

Une politique AWS gérée est une politique autonome créée et administrée par AWS. AWS les politiques gérées sont conçues pour fournir des autorisations pour de nombreux cas d'utilisation courants afin que vous puissiez commencer à attribuer des autorisations aux utilisateurs, aux groupes et aux rôles.

N'oubliez pas que les politiques AWS gérées peuvent ne pas accorder d'autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont accessibles à tous les AWS clients. Nous vous recommandons de réduire encore les autorisations en définissant des politiques gérées par le client qui sont propres à vos cas d'utilisation.

Vous ne pouvez pas modifier les autorisations définies dans les politiques AWS gérées. Si les autorisations définies dans une politique AWS gérée sont AWS mises à jour, la mise à jour affecte toutes les identités principales (utilisateurs, groupes et rôles) auxquelles la politique est attachée. AWS est le plus susceptible de mettre à jour une politique AWS gérée lorsqu'une nouvelle Service AWS est lancée ou lorsque de nouvelles opérations d'API sont disponibles pour les services existants.

Pour plus d'informations, consultez Politiques gérées par AWS dans le Guide de l'utilisateur IAM.

AWS politique gérée : AmazonRoute 53 FullAccess

Vous pouvez associer la politique `AmazonRoute53FullAccess` à vos identités IAM.

Cette stratégie accorde un accès complet aux ressources Route 53, y compris l'enregistrement de domaine et la surveillance de l'état, mais à l'exclusion de Resolver.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- `route53:*` – Permet d'exécuter toutes les actions Route 53, sauf les actions suivantes :
  - Créez et mettez à jour des enregistrements d'alias pour lesquels la valeur d'Alias Target est une CloudFront distribution, un équilibreur de charge Elastic Load Balancing, un environnement Elastic Beanstalk ou un bucket Amazon S3. (Avec ces autorisations, vous pouvez créer des enregistrements d'alias pour lesquels la valeur de Alias Target est un autre enregistrement dans la même zone hébergée.)
  - Utiliser des zones hébergées privées.

  - Utiliser des domaines.
  - Créez, supprimez et visualisez les CloudWatch alarmes.
  - Afficher CloudWatch les métriques dans la console Route 53.
- `route53domains:*` – Permet d'utiliser des domaines.
- `cloudfront:ListDistributions`— Vous permet de créer et de mettre à jour des enregistrements d'alias pour lesquels la valeur d'Alias Target est une CloudFront distribution.

  Cette autorisation n'est pas nécessaire si vous n'utilisez pas la console Route 53. Route 53 l'utilise uniquement pour obtenir une liste des distributions à afficher dans la console.
- `cloudfront:GetDistributionTenantByDomain`— Utilisé pour récupérer les distributions CloudFront multi-locataires afin de vous permettre de créer et de mettre à jour des enregistrements d'alias pour lesquels la valeur d'Alias Target est un tenant de CloudFront distribution.
- `cloudfront:GetConnectionGroup`— Utilisé pour récupérer les distributions CloudFront multi-locataires afin de vous permettre de créer et de mettre à jour des enregistrements d'alias pour lesquels la valeur d'Alias Target est un tenant de CloudFront distribution.
- `cloudwatch:DescribeAlarms`— Associé à `sns:ListTopics` et`sns:ListSubscriptionsByTopic`, vous permet de créer, de supprimer et de visualiser des CloudWatch alarmes.
- `cloudwatch:GetMetricStatistics`— Vous permet de créer des CloudWatch bilans de santé métriques.

  Ces autorisations ne sont pas nécessaires si vous n'utilisez pas la console Route 53. Route 53 l'utilise uniquement pour obtenir des statistiques à afficher dans la console.
- `cloudwatch:GetMetricData`— Vous permet d'afficher l'état de vos indicateurs de CloudWatch santé.
- `ec2:DescribeVpcs`— Permet d'afficher une liste de VPCs.
- `ec2:DescribeVpcEndpoints` – Permet d'afficher une liste de points de terminaison d'un VPC.
- `ec2:DescribeRegions` – Permet d'afficher une liste des zones de disponibilité.
- `elasticloadbalancing:DescribeLoadBalancers` – Permet de créer et de mettre à jour des enregistrements d'alias pour lesquels la valeur de Alias Target (Cible de l'alias) est un équilibreur de charge Elastic Load Balancing.

  Ces autorisations ne sont pas nécessaires si vous n'utilisez pas la console Route 53. Route 53 l'utilise uniquement pour obtenir une liste des équilibreurs de charge à afficher dans la console.

- `elasticbeanstalk:DescribeEnvironments` – Permet de créer et de mettre à jour des enregistrements d'alias pour lesquels la valeur de Alias Target (Cible de l'alias) est un environnement Elastic Beanstalk.

  Ces autorisations ne sont pas nécessaires si vous n'utilisez pas la console Route 53. Route 53 l'utilise uniquement pour obtenir une liste des environnements à afficher dans la console.
- `es:ListDomainNames`— Vous permet d'afficher les noms de tous les domaines Amazon OpenSearch Service détenus par l'utilisateur actuel dans la région active.
- `es:DescribeDomains`— Vous permet d'obtenir la configuration des domaines Amazon OpenSearch Service spécifiés.
- `lightsail:GetContainerServices`— Vous permet d'utiliser les services de conteneur Lightsail pour créer et mettre à jour des enregistrements d'alias pour lesquels la valeur d'Alias Target est un domaine Lightsail.
- `s3:ListBucket`, `s3:GetBucketLocation` et `s3:GetBucketWebsite` – Permet de créer et de mettre à jour des enregistrements d'alias pour lesquels la valeur de Alias Target (Cible de l'alias) est un compartiment Amazon S3. (Vous pouvez créer un alias dans un compartiment Amazon S3 uniquement si le compartiment est configuré en tant que point de terminaison de site web ; `s3:GetBucketWebsite` obtient les informations de configuration nécessaires.)

  Ces autorisations ne sont pas nécessaires si vous n'utilisez pas la console Route 53. Route 53 les utilise uniquement pour obtenir une liste des compartiments à afficher dans la console.
- `sns:ListTopics`,`sns:ListSubscriptionsByTopic`, `cloudwatch:DescribeAlarms` — Vous permet de créer, de supprimer et d'afficher des CloudWatch alarmes.
- `tag:GetResources`— Vous permet d'afficher les tags de vos ressources. Par exemple, les noms de vos bilans de santé.
- `apigateway:GET` – Permet de créer et de mettre à jour des enregistrements d'alias pour lesquels la valeur Alias Target (Cible de l'alias) est une API Amazon API Gateway.

Pour plus d'informations sur les autorisations, consultez[Autorisations d'API Amazon Route 53 : référence des actions, ressources et conditions](#).

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 politique gérée : AmazonRoute 53 ReadOnlyAccess

Vous pouvez associer la politique `AmazonRoute53ReadOnlyAccess` à vos identités IAM.

Cette stratégie accorde un accès en lecture seule aux ressources Route 53, y compris l'enregistrement de domaine et la surveillance de l'état, mais à l'exclusion de Resolver.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- `route53:Get*` – Récupère les ressources Route 53.
- `route53:List*` – Récupère les ressources Route 53.
- `route53:TestDNSAnswer` – Retourne la valeur que Route 53 renvoie en réponse à une requête DNS.

Pour plus d'informations sur les autorisations, consultez Autorisations d'API Amazon Route 53 : référence des actions, ressources et conditions.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53:Get*",
                "route53:List*",
                "route53:TestDNSAnswer"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWS politique gérée : AmazonRoute 53 DomainsFullAccess

Vous pouvez associer la politique `AmazonRoute53DomainsFullAccess` à vos identités IAM.

Cette stratégie accorde un accès complet aux ressources d'enregistrement de domaine Route 53.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- `route53:CreateHostedZone` – Permet de créer une zone hébergée Route 53.
- `route53domains:*` – Permet d'enregistrer des noms de domaine et d'effectuer des opérations associées.

Pour plus d'informations sur les autorisations, consultez Autorisations d'API Amazon Route 53 : référence des actions, ressources et conditions.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53:CreateHostedZone",
                "route53domains:*"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWS politique gérée : AmazonRoute 53 DomainsReadOnlyAccess

Vous pouvez associer la politique `AmazonRoute53DomainsReadOnlyAccess` à vos identités IAM.

Cette stratégie accorde à l'accès en lecture seule aux ressources d'enregistrement de domaine Route 53.

Détails de l’autorisation

Cette politique inclut les autorisations suivantes.

- `route53domains:Get*` – Permet de récupérer une liste de domaines à partir de Route 53.
- `route53domains:List*` – Permet d'afficher une liste de domaines Route 53.

Pour plus d'informations sur les autorisations, consultez[Autorisations d'API Amazon Route 53 : référence des actions, ressources et conditions](#).

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53domains:Get*",
                "route53domains:List*"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWS politique gérée : AmazonRoute 53 ResolverFullAccess

Vous pouvez associer la politique `AmazonRoute53ResolverFullAccess` à vos identités IAM.

Cette stratégie accorde un accès complet aux ressources du résolveur Route 53.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- `route53resolver:*` – Permet de créer et de gérer des ressources Resolver sur la console Route 53.
- `ec2:DescribeSubnets` – Permet de répertorier vos sous-réseaux Amazon VPC.
- `ec2:CreateNetworkInterface`,`ec2:DeleteNetworkInterface`, et `ec2:ModifyNetworkInterfaceAttribute` – Permet de créer, modifier et supprimer des interfaces réseau.
- `ec2:DescribeNetworkInterfaces` – Permet d'afficher une liste d'interfaces réseau.
- `ec2:DescribeSecurityGroups` – Permet d'afficher une liste de tous vos groupes de sécurité.

- `ec2:DescribeVpcs`— Permet d'afficher une liste de VPCs.
- `ec2:DescribeAvailabilityZones` – Permet d'afficher la liste des zones qui sont disponibles pour vous.

Pour plus d'informations sur les autorisations, consultez Autorisations d'API Amazon Route 53 : référence des actions, ressources et conditions.

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 politique gérée : AmazonRoute 53 ResolverReadOnlyAccess

Vous pouvez associer la politique `AmazonRoute53ResolverReadOnlyAccess` à vos identités IAM.

Cette stratégie accorde à l'accès en lecture seule aux ressources de Route 53 Resolver.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- `route53resolver:Get*`— Récupère les ressources du résolveur.
- `route53resolver:List*` – Permet de récupérer la liste des ressources Resolver.
- `ec2:DescribeNetworkInterfaces` – Permet d'afficher une liste d'interfaces réseau.
- `ec2:DescribeSecurityGroups` – Permet d'afficher une liste de tous vos groupes de sécurité.

Pour plus d'informations sur les autorisations, consultezAutorisations d'API Amazon Route 53 : référence des actions, ressources et conditions.

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 politique gérée : Route53 ResolverServiceRolePolicy

Vous ne pouvez pas joindre de `Route53ResolverServiceRolePolicy` à vos entités IAM. Cette stratégie est attachée à un rôle lié au service qui permet à Route 53 Resolver d'accéder aux services

et ressources AWS qui sont utilisés ou gérés par Resolver. Pour de plus amples informations, veuillez consulter Utilisation des rôles liés à un service pour Amazon Route 53 Resolver.

AWS politique gérée : AmazonRoute 53 ProfilesFullAccess

Vous pouvez associer la politique `AmazonRoute53ProfilesReadOnlyAccess` à vos identités IAM.

Cette politique accorde un accès complet aux ressources du profil Amazon Route 53.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- `route53profiles`— Vous permet de créer et de gérer des ressources de profil sur la console Route 53.
- `ec2`— Permet aux directeurs d'obtenir des informations sur VPCs.

Pour plus d'informations sur les autorisations, consultezAutorisations d'API Amazon Route 53 : référence des actions, ressources et conditions.

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 politique gérée : AmazonRoute 53 ProfilesReadOnlyAccess

Vous pouvez associer la politique `AmazonRoute53ProfilesReadOnlyAccess` à vos identités IAM.

Cette politique accorde un accès en lecture seule aux ressources du profil Amazon Route 53.

Détails de l'autorisation

Pour plus d'informations sur les autorisations, consultez[Autorisations d'API Amazon Route 53 : référence des actions, ressources et conditions](#).

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": [
                "*"
            ]
        }
    ]
}
```

Mises à jour de Route 53 vers les politiques AWS gérées

Consultez les détails des mises à jour des politiques AWS gérées pour Route 53 depuis que ce service a commencé à suivre ces modifications. Pour obtenir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au flux RSS de la page Historique du document de Route 53.

Modification	Description	Date
AmazonRoute53 FullAccess — Politique mise à jour	Ajoute des autorisations pour `cloudwatch:GetMetricData` `tag:GetResources` ,`es:ListDomainNames` ,`es:DescribeDomains` ,`cloudfront:GetDistributionTenantByDomain` ,	01 juin 2025

Modification	Description	Date
	`cloudfront:GetConnectionGroup` et `lightsail:GetContainerServices` . Ces autorisations vous permettent de récupérer jusqu'à 500 indicateurs de CloudWatch santé, jusqu'à 100 noms de bilans de santé, d'obtenir la configuration du domaine pour les domaines Amazon OpenSearch Service spécifiés et de répertorier les noms de tous les domaines Amazon OpenSearch Service détenus par l'utilisateur actuel dans la région active, de récupérer les distributions CloudFront multi-locataires et d'obtenir les services de conteneur Lightsail.	
AmazonRoute53 ProfilesFullAccess — Politique mise à jour	Ajoute des autorisations pour `GetProfilePolicy` et `PutProfilePolicy` . Il s'agit d'actions IAM avec autorisation uniquement. Si ces autorisations ne sont pas accordées à un principal IAM, une erreur se produira lors de la tentative de partage du profil à l'aide du AWS RAM service.	27 août 2024

Modification	Description	Date
AmazonRoute53 ProfilesReadOnlyAccess — Politique mise à jour	Ajoute des autorisations pour`GetProfilePolicy` . Il s'agit d'une action IAM avec autorisation uniquement. Si cette autorisation n'est pas accordée à un principal IAM, une erreur se produira lors de la tentative d'accès à la politique du profil à l'aide du AWS RAM service.	27 août 2024
AmazonRoute53 ResolverFullAccess — Politique mise à jour	Ajout d'un identifiant de déclaration (Sid) pour identifier de manière unique la politique.	5 août 2024
AmazonRoute53 ResolverReadOnlyAccess — Politique mise à jour	Ajout d'un identifiant de déclaration (Sid) pour identifier de manière unique la politique.	5 août 2024
AmazonRoute53 ProfilesFullAccess — Nouvelle politique	Amazon Route 53 a ajouté une nouvelle politique permettant un accès complet aux ressources du profil Amazon Route 53.	22 avril 2024
AmazonRoute53 ProfilesReadOnlyAccess — Nouvelle politique	Amazon Route 53 a ajouté une nouvelle politique permettant l'accès en lecture seule aux ressources du profil Amazon Route 53.	22 avril 2024

Modification	Description	Date
Route53 ResolverServiceRolePolicy — Nouvelle politique	Amazon Route 53 a ajouté une nouvelle politique associée à un rôle lié à un service qui permet à Route 53 Resolver d'accéder aux AWS services et aux ressources utilisés ou gérés par Resolver.	14 juillet 2021
AmazonRoute53 ResolverReadOnlyAccess — Nouvelle politique	Amazon Route 53 a ajouté une nouvelle politique pour autoriser l'accès en lecture seule aux ressources du résolveur Route 53.	14 juillet 2021
AmazonRoute53 ResolverFullAccess — Nouvelle politique	Amazon Route 53 a ajouté une nouvelle politique permettant un accès complet aux ressources du résolveur Route 53.	14 juillet 2021
AmazonRoute53 DomainsReadOnlyAccess — Nouvelle politique	Amazon Route 53 a ajouté une nouvelle politique pour autoriser l'accès en lecture seule aux ressources des domaines Route 53.	14 juillet 2021
AmazonRoute53 DomainsFullAccess — Nouvelle politique	Amazon Route 53 a ajouté une nouvelle politique permettant un accès complet aux ressources des domaines Route 53.	14 juillet 2021

Modification	Description	Date
AmazonRoute53 ReadOnlyAccess — Nouvelle politique	Amazon Route 53 a ajouté une nouvelle politique pour autoriser l'accès en lecture seule aux ressources Route 53.	14 juillet 2021
AmazonRoute53 FullAccess — Nouvelle politique	Amazon Route 53 a ajouté une nouvelle politique permettant un accès complet aux ressources de Route 53.	14 juillet 2021
Route 53 a commencé à suivre les modifications	Route 53 a commencé à suivre les modifications apportées AWS à ses politiques gérées.	14 juillet 2021

Utilisation de conditions de politique IAM pour un contrôle d'accès précis

Dans Route 53, vous pouvez spécifier des conditions lors de l'octroi d'autorisations à l'aide d'une politique IAM (consultez Contrôle d'accès). Par exemple, vous pouvez :

- Accorder des autorisations pour autoriser l'accès à un ensemble d'enregistrements de ressources unique
- Accordez des autorisations pour permettre aux utilisateurs d'accéder à tous les ensembles d'enregistrements de ressources d'un type d'enregistrement DNS spécifique dans une zone hébergée, par exemple les enregistrements A et AAAA.
- Accordez des autorisations pour permettre aux utilisateurs d'accéder à un ensemble d'enregistrements de ressources dont le nom contient une chaîne spécifique.
- Accordez des autorisations pour permettre aux utilisateurs d'effectuer uniquement un sous-ensemble des `CREATE | UPSERT | DELETE` actions sur la console Route 53 ou lors de l'utilisation de l'ChangeResourceRecordSetsAPI.
- Accordez des autorisations pour permettre aux utilisateurs d'associer ou de dissocier des zones hébergées privées d'un VPC spécifique.

- Accordez des autorisations pour permettre aux utilisateurs de répertorier les zones hébergées associées à un VPC spécifique.
- Accordez des autorisations permettant aux utilisateurs d'accéder à la création d'une nouvelle zone hébergée privée et de l'associer à un VPC spécifique.
- Accordez des autorisations pour permettre aux utilisateurs de créer ou de supprimer une autorisation d'association VPC.

Vous pouvez également créer des autorisations qui combinent n'importe laquelle des autorisations granulaires.

Normalisation des valeurs clés de la condition Route 53

Les valeurs que vous saisissez pour les conditions de politique doivent être formatées, ou normalisées, comme suit :

Pour **`route53:ChangeResourceRecordSetsNormalizedRecordNames`** :

- Toutes les lettres doivent être en minuscules.
- le nom DNS ne doit pas contenir de point arrière.
- Les caractères autres que a à z, 0 à 9, - (tiret), _ (trait de soulignement) et . (point, comme délimiteur entre les étiquettes) doivent utiliser des codes d'échappement au format \code octal à trois chiffres. Par exemple,`\052` est le code octal du caractère *.

Pour **`route53:ChangeResourceRecordSetsActions`**, la valeur peut être l'une valeurs des suivantes et doit être en majuscules :

- CREATE
- UPSERT
- DELETE

Pour **`route53:ChangeResourceRecordSetsRecordTypes`** :

- La valeur doit être en majuscules et peut être n'importe quel type d'enregistrement DNS pris en charge par Route 53. Pour de plus amples informations, veuillez consulter Types d'enregistrements DNS pris en charge.

Pour **`route53:VPCs`** :

- La valeur doit être au format de`VPCId=<vpc-id>,VPCRegion=<region>`.
- La valeur de `<vpc-id>` et `<region>` doit être en minuscules, par exemple et. `VPCId=vpc-123abc VPCRegion=us-east-1`
- Les clés de contexte et les valeurs distinguent les majuscules et minuscules.

> **Important**
>
> Pour obtenir l'autorisation d'autoriser ou de restreindre les actions que vous souhaitez, vous devez suivre ces conventions. Seuls `VPCId` les `VPCRegion` éléments sont acceptés par cette clé de condition, les autres AWS ressources, telles que Compte AWS, ne sont pas prises en charge.

Vous pouvez utiliser le plugin Access Analyzer ou Policy Simulator dans le Guide de l'utilisateur IAM pour vérifier que votre politique accorde ou restreint les autorisations comme prévu. Vous pouvez également valider les autorisations en appliquant une politique IAM à un utilisateur ou à un rôle de test pour effectuer des opérations Route 53.

Spécification de conditions : utilisation de clés de condition

AWS fournit un ensemble de clés de condition prédéfinies (clés AWS de condition étendues) pour tous les AWS services qui prennent en charge le contrôle d'accès IAM. Par exemple, vous pouvez utiliser la clé de condition `aws:SourceIp` pour vérifier l'adresse IP du demandeur avant de permettre l'exécution d'une action. Pour plus d'informations et la liste des clés à l'échelle d' AWS, consultez Clés disponibles pour les conditions dans le Guide de l'utilisateur IAM.

> **Note**
>
> Route 53 ne prend pas en charge les clés de condition basées sur des balises.

Le tableau suivant indique les clés de condition spécifiques au service Route 53 qui s'appliquent à Route 53.

Clé de condition Route 53	Opérations d'API	Type de la valeur	Description
`route53:ChangeResourceRecordSetsNormalizedRecordNames`	ChangeResourceRecordSets	Multi-valeurs	Représente une liste de noms d'enregistrements DNS dans la demande deChangeResourceRecordSets. Pour obtenir le comportement attendu, les noms DNS de la politique IAM doivent être normalisés comme suit : • Toutes les lettres doivent être en minuscules. • le nom DNS ne doit pas contenir de point arrière. • Les caractères autres que a à z, 0 à 9, - (tiret), _ (trait de soulignement) et . (point, comme délimiteur entre les étiquettes) doivent utiliser des codes d'échappement au format \code octal à trois chiffres.
`route53:ChangeResourceRecordSetsRecordTypes`	ChangeResourceRecordSets	Multi-valeurs	Représente une liste de types d'enregistrements DNS dans la demande de `ChangeResourceRecordSets` . `ChangeResourceRecordSetsRecordTypes` peut être n'importe quel type d'enregistrement DNS pris en charge par Route 53. Pour de plus amples informations, veuillez consulter Types d'enregistrements DNS pris en charge. Tout doit être saisi en majuscules dans la politique.
`route53:ChangeResourceRecor`	ChangeResourceRecordSets	Multi-valeurs	Représente une liste des actions de la demande de `ChangeResourceRecordSets` .

Clé de condition Route 53	Opérations d'API	Type de la valeur	Description
`dSetsActions`			`ChangeResourceRecordSetsActions` peut être n'importe laquelle des valeurs suivantes (doit être en majuscule) : • CREATE • UPSERT • DELETE
`route53:VPCs`	Associé VPCWith HostedZone Dissocier VPCFrom HostedZone ListHostedZonesByVPC CreateHostedZone Créer une VPCAssociation autorisation Supprimer VPCAssociation l'autorisation	Multi-valeurs	Représente une liste de VPCs dans la demande de `AssociateVPCWithHostedZone` `DisassociateVPCFromHostedZone` , `ListHostedZonesByVPC` `CreateHostedZone` ,`CreateVPCAssociationAuthorization` ,,`DeleteVPCAssociationAuthorization` , et, au format "VPCId=<vpc-id>, VPCRegion = <region>

Exemples de politiques : utilisation de conditions pour un accès précis

Chacun des exemples de cette section définit la clause Effect sur Allow et spécifie uniquement les actions, ressources et paramètres autorisés. L'accès est autorisé uniquement à ce qui est explicitement indiqué dans la politique IAM.

Dans certains cas, il est possible de réécrire ces politiques afin qu'elles soient basées sur le refus (autrement dit, définition de la clause Effect sur Deny et inversion de toute la logique de la politique). Cependant, nous vous recommandons d'éviter d'utiliser les politiques basées sur le refus, car elles sont difficiles à écrire correctement, par comparaison avec les stratégies basées sur l'autorisation. Cela est particulièrement vrai pour Route 53 en raison de la normalisation du texte requise.

Accorder des autorisations limitant l'accès aux enregistrements DNS avec des noms spécifiques

La politique d'autorisations suivante accorde les autorisations qui autorise les actions `ChangeResourceRecordSets` sur la zone hébergée Z12345 pour example.com et marketing.example.com. Elle utilise la clé de condition `route53:ChangeResourceRecordSetsNormalizedRecordNames` pour limiter les actions de l'utilisateur uniquement sur les enregistrements correspondant aux noms spécifiés.

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` est un opérateur de condition IAM qui s'applique aux clés à valeurs multiples. La condition dans la politique ci-dessus n'autorisera l'opération que lorsque tous les changements dans `ChangeResourceRecordSets` auront le nom DNS example.com. Pour plus d'informations, consultez Opérateurs de condition IAM etCondition IAM avec plusieurs clés ou valeurs dans le Guide de l'utilisateur IAM.

Pour implémenter l'autorisation qui fait correspondre les noms avec certains suffixes, vous pouvez utiliser le caractère générique IAM (*) dans la politique avec l'opérateur de condition `StringLike` ou `StringNotLike`. La politique suivante autorisera l'opération lorsque toutes les changements dans l'opération `ChangeResourceRecordSets` auront des noms DNS qui se terminent par « -beta.example.com ».

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**
>
> Le caractère générique IAM n'est pas identique au caractère générique du nom de domaine. Consultez l'exemple suivant pour savoir comment utiliser le caractère générique avec un nom de domaine.

Accorder des autorisations limitant l'accès aux enregistrements DNS correspondant à un nom de domaine contenant un caractère générique

La politique d'autorisations suivante accorde les autorisations qui autorise les actions `ChangeResourceRecordSets` sur la zone hébergée Z12345 pour example.com. Elle utilise la clé de condition `route53:ChangeResourceRecordSetsNormalizedRecordNames` pour limiter les actions de l'utilisateur uniquement aux enregistrements correspondant à *.example.com.

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` est le code octal du caractère * dans le nom DNS, et `\` dans `\052` est échappé pour être `\\` afin de suivre la syntaxe JSON.

Accorder des autorisations limitant l'accès à des enregistrements DNS spécifiques

La politique d'autorisations suivante accorde les autorisations qui autorise les actions `ChangeResourceRecordSets` sur la zone hébergée Z12345 pour example.com. Elle utilise la combinaison de trois clés de condition pour limiter les actions des utilisateurs afin de permettre uniquement la création ou la modification d'enregistrements DNS avec un nom et un type de DNS spécifiques.

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"]
                }
            }
          }
        ]
}
```

Accorder des autorisations limitant l'accès à la création et la modification uniquement de types d'enregistrements DNS spécifiques

La politique d'autorisations suivante accorde les autorisations qui autorise les actions `ChangeResourceRecordSets` sur la zone hébergée Z12345 pour example.com. Elle utilise la clé de condition `route53:ChangeResourceRecordSetsRecordTypes` pour limiter les actions de l'utilisateur uniquement sur les enregistrements correspondant aux types spécifiés (A et AAAA).

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "route53:ChangeResourceRecordSets",
            "Resource": "arn:aws:route53:::hostedzone/Z11111112222222333333",
            "Condition": {
```

```
                "ForAllValues:StringEquals":{
                     "route53:ChangeResourceRecordSetsRecordTypes": ["A", "AAAA"]
                }
            }
          }
        ]
}
```

Accorder des autorisations qui spécifient le VPC dans lequel le principal IAM peut opérer

La politique d'autorisation suivante accorde des autorisations qui autorisent`AssociateVPCWithHostedZone`,`DisassociateVPCFromHostedZone`,`ListHostedZonesBy` `CreateHostedZoneCreateVPCAssociationAuthorization`, et `DeleteVPCAssociationAuthorization` les actions sur le VPC spécifié par le vpc-id.

> **Important**
>
> La valeur de la condition doit être au format de`VPCId=<vpc-id>,VPCRegion=<region>`. Si vous spécifiez un ARN VPC dans la valeur de la condition, la clé de condition ne prendra pas effet.

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": "*"
        }
    ]
}
```

Autorisations d'API Amazon Route 53 : référence des actions, ressources et conditions

Lorsque vous configurez Contrôle d'accès et rédigez une politique d'autorisation que vous pouvez associer à une identité IAM (politiques basées sur l'identité), vous pouvez utiliser les listes d'actions, de ressources et de clés de condition pour Route 53, les actions, les ressources et les clés de condition pour Route 53 Resolver, et les actions, ressources et clés de condition pour les profils Amazon Route 53 permettant de partager les paramètres DNS avec VPCs la référence d'autorisation de service. Les pages incluent chaque action de l'API Amazon Route 53, les actions auxquelles vous devez accorder des autorisations d'accès et la AWS ressource à laquelle vous devez accorder l'accès. Vous spécifiez les actions dans le champ `Action` de la politique ainsi que la valeur des ressources dans le champ `Resource` de la politique.

Vous pouvez utiliser des AWS touches de condition larges dans vos politiques Route 53 pour exprimer des conditions. Pour obtenir la liste complète des touches AWS-wide, consultez la section Clés disponibles dans le guide de l'utilisateur IAM.

> **Note**
>
> Lors de l'autorisation d'accès, la zone hébergée et Amazon VPC doivent appartenir à la même partition. Une partition est un groupe de Régions AWS. Chacune Compte AWS est limitée à une partition.
> Les partitions prises en charge sont les suivantes :
>
> - `aws` - Régions AWS
> - `aws-cn` - Régions chinoises

- `aws-us-gov` - AWS GovCloud (US) Region

Pour plus d'informations, consultez Gestion d'accès dans le document AWS Référence générale.

> **Note**
>
> Pour indiquer une action, utilisez le préfixe applicable (`route53`, `route53domains` ou `route53resolver`) suivi du nom de l'opération d'API, par exemple :
>
> - `route53:CreateHostedZone`
> - `route53domains:RegisterDomain`
> - `route53resolver:CreateResolverEndpoint`

Journalisation et surveillance dans Amazon Route 53

Amazon Route 53 fournit une journalisation des requêtes DNS et la capacité à surveiller vos ressources à l'aide de surveillances de l'état. En outre, Route 53 s'intègre à d'autres AWS services pour fournir une journalisation et une surveillance supplémentaires :

Journalisation des requêtes DNS

Vous pouvez configurer Route 53 pour consigner des informations sur les requêtes que reçoit Route 53, par exemple le domaine ou le sous-domaine qui a été demandé, la date et l'heure de la demande, et le type d'enregistrement DNS comme A ou AAAA.

Pour de plus amples informations, veuillez consulter Journalisation des requêtes DNS publiques.

Utilisation AWS CloudTrail pour enregistrer les actions de la console et de programmation

CloudTrail fournit un enregistrement des actions Route 53 entreprises par un utilisateur, un rôle ou un AWS service. À l'aide des informations collectées par CloudTrail, vous pouvez suivre les demandes effectuées, les adresses IP d'où proviennent les demandes, l'auteur de la demande, la date à laquelle elle a été faite et des informations supplémentaires. Pour de plus amples informations, veuillez consulter Journalisation des appels d'API Amazon Route 53 avec AWS CloudTrail.

Surveillance des registres de domaines

Le tableau de bord Route 53 fournit des informations détaillées sur l'état de vos enregistrements de domaine, telles que le statut des transferts de domaines et les domaines dont la date d'expiration approche.

Pour de plus amples informations, veuillez consulter Surveillance des registres de domaines.

Utiliser les bilans de santé de Route 53 et Amazon CloudWatch pour surveiller vos ressources

Vous pouvez surveiller vos ressources en créant des bilans de santé Route 53, qui permettent de collecter et CloudWatch de traiter les données brutes pour en faire des indicateurs lisibles en temps quasi réel.

Pour de plus amples informations, veuillez consulter Surveillance de vos ressources grâce aux bilans de santé d'Amazon Route 53 et à Amazon CloudWatch.

Utiliser Amazon CloudWatch pour surveiller les points de terminaison Route 53 Resolver

Vous pouvez l'utiliser CloudWatch pour surveiller le nombre de requêtes DNS transmises par les points de terminaison du résolveur.

Pour de plus amples informations, veuillez consulter Surveillance des points de terminaison Route 53 Resolver avec Amazon CloudWatch.

En utilisant AWS Trusted Advisor

Trusted Advisor s'appuie sur les meilleures pratiques apprises en servant AWS les clients. Trusted Advisor inspecte votre AWS environnement, puis émet des recommandations lorsque des opportunités se présentent pour économiser de l'argent, améliorer la disponibilité et les performances du système ou contribuer à combler les failles de sécurité. Tous les AWS clients ont accès à cinq Trusted Advisor chèques. Les clients disposant d'un plan de support Business ou Enterprise peuvent consulter tous les Trusted Advisor chèques.

Pour de plus amples informations, veuillez consulter Trusted Advisor.

Validation de la conformité pour Amazon Route 53

Des auditeurs tiers évaluent la sécurité et la conformité d'Amazon Route 53 dans le cadre de plusieurs programmes de AWS conformité. Il s’agit notamment des certifications SOC, PCI, FedRAMP, HIPAA et d’autres.

Pour une liste des AWS services concernés par des programmes de conformité spécifiques, voir AWS Services concernés par programme de conformité. Pour obtenir des informations générales, consultez Programmes de conformitéAWS.

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, consultez la section Téléchargement de rapports dans AWS Artifact.

Votre responsabilité de conformité lors de l'utilisation de Route 53 est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise, ainsi que par la législation et la réglementation applicables. Si votre utilisation de Route 53 est soumise au respect de normes telles que HIPAA, PCI ou FedRAMP, fournit des ressources pour vous aider à : AWS

- Guides de démarrage rapide sur la sécurité et la conformité : ces guides de déploiement abordent les considérations architecturales et indiquent les étapes à suivre pour déployer des environnements de base axés sur la sécurité et la conformité sur. AWS
- Livre blanc sur l'architecture pour la sécurité et la conformité HIPAA – Le livre blanc décrit comment les entreprises peuvent utiliser AWS pour créer des applications conformes à HIPAA.
- AWS Ressources relatives à la conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- AWS Config— Ce AWS service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- AWS Security Hub— Ce AWS service fournit une vue complète de l'état de votre sécurité interne, AWS ce qui vous permet de vérifier votre conformité aux normes et aux meilleures pratiques du secteur de la sécurité.

La résilience dans Amazon Route 53

L'infrastructure AWS mondiale est construite autour des AWS régions et des zones de disponibilité. AWS Les régions fournissent plusieurs zones de disponibilité physiquement séparées et isolées, connectées par un réseau à faible latence, à haut débit et hautement redondant. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone de disponibilité à l'autre sans interruption. Les zones de disponibilité sont plus hautement disponibles, tolérantes aux pannes et évolutives que les infrastructures traditionnelles à un ou plusieurs centres de données.

Route 53 divise sa fonctionnalité en un plan de contrôle et un plan de données. Le service Route 53, comme la plupart des services AWS , inclut un plan de contrôle qui vous permet d'effectuer des

opérations de gestion telles que la création, la mise à jour et la suppression de ressources et un plan de données fournissant les fonctionnalités principales du service. Pour plus d'informations sur les plans de contrôle et de données dans Route 53, consultez Concepts de plan de données et contrôle.

Route 53 est avant tout un service mondial, mais les fonctionnalités suivantes prennent en charge AWS les régions :

- Si vous utilisez Route 53 Resolver pour configurer des configurations hybrides, vous créez des points de terminaison dans AWS les régions de votre choix et vous spécifiez des adresses IP dans plusieurs zones de disponibilité. Pour les points de terminaison sortants, vous créez des règles dans la même région que celle où vous avez créé le point de terminaison. Pour de plus amples informations, veuillez consulter Qu'est-ce que c'est Amazon Route 53 Resolver ?.
- Vous pouvez configurer les contrôles de santé de Route 53 pour vérifier l'état des ressources que vous créez dans des régions spécifiques, telles que les EC2 instances Amazon et les équilibreurs de charge Elastic Load Balancing.
- Lorsque vous créez une surveillance de l'état qui surveille un point de terminaison, vous pouvez, si vous le souhaitez, spécifier les régions à partir desquelles vous souhaitez voir Route 53 effectuer des surveillances de l'état.

Pour plus d'informations sur AWS les régions et les zones de disponibilité, consultez la section Infrastructure AWS mondiale.

Sécurité de l'infrastructure dans Amazon Route 53

En tant que service géré, Amazon Route 53 est protégé par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et sur la manière dont AWS l'infrastructure est protégée, consultez la section Sécurité du AWS cloud. Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans le cadre AWS bien architecturé du pilier de sécurité.

Vous utilisez des appels d'API AWS publiés pour accéder à Route 53 via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Ses suites de chiffrement PFS (Perfect Forward Secrecy) comme DHE (Ephemeral Diffie-Hellman) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un principal IAM. Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

Envoi des résultats depuis le pare-feu DNS Route 53 Resolver vers Security Hub

AWS Security Hubvous fournit une vue complète de l'état de votre sécurité AWS et vous aide à vérifier que votre environnement est conforme aux normes et aux meilleures pratiques du secteur de la sécurité. Security Hub collecte des données de sécurité provenant de l'ensemble Comptes AWS des produits partenaires tiers pris en charge et vous aide à analyser les tendances en matière de sécurité et à identifier les problèmes de sécurité les plus prioritaires. Services AWS

En intégrant le pare-feu DNS Route 53 Resolver à Security Hub, vous pouvez envoyer les résultats du pare-feu DNS au Security Hub. Security Hub inclut ensuite ces résultats dans son analyse de votre posture de sécurité.

Table des matières

- Comment fonctionnent les résultats dans Security Hub
  - Types de résultats envoyés par le pare-feu DNS
  - Réessayer lorsque Security Hub n'est pas disponible
  - Mise à jour des résultats existants dans Security Hub
- Découverte typique du pare-feu DNS
- Activation et configuration de l'intégration
- Arrêt de la transmission des résultats à Security Hub

Comment fonctionnent les résultats dans Security Hub

Dans Security Hub, un résultat est un enregistrement observable d'un contrôle de sécurité ou d'une détection liée à la sécurité. Certains résultats proviennent de problèmes détectés par d'autres partenaires Services AWS ou par des partenaires tiers. Security Hub dispose également de ses propres contrôles de sécurité qu'il utilise pour détecter les problèmes de sécurité et générer des résultats.

Security Hub fournit des outils permettant de gérer les résultats provenant de toutes ces sources. Vous pouvez afficher et filtrer les listes de résultats et afficher les détails d'un résultat. Pour plus d'informations, consultez la section Révision des détails des recherches et de l'historique des recherches dans Security Hub dans le guide de AWS Security Hub l'utilisateur. Vous pouvez

également mettre à jour automatiquement les résultats ou les envoyer à une action personnalisée. Pour plus d'informations, consultez la section Modifier automatiquement les résultats du Security Hub et prendre des mesures en conséquence dans le Guide de AWS Security Hub l'utilisateur.

Tous les résultats de Security Hub utilisent un format JSON standard appelé AWS Security Finding Format (ASFF). L'ASFF inclut des détails sur la source du problème de sécurité, les ressources concernées et l'état actuel de la découverte. Pour de plus amples informations, veuillez consulter AWS Security Finding Format (ASFF) dans le Guide de l'utilisateur AWS Security Hub .

Le pare-feu DNS est l'un des systèmes Services AWS qui envoie les résultats à Security Hub.

Types de résultats envoyés par le pare-feu DNS

Le pare-feu DNS possède les intégrations suivantes :

- Listes de domaines gérés : résultats de sécurité relatifs aux requêtes bloquées ou alertées pour les domaines associés aux listes de domaines AWS gérés.
- Listes de domaines personnalisées : résultats de sécurité liés aux requêtes bloquées ou signalées pour les domaines associés à la liste de domaines du client.
- DNS Firewall Advanced : résultats de sécurité liés aux requêtes bloquées ou alertées par DNS Firewall Advanced.

Security Hub ingère les résultats du pare-feu DNS au format ASFF (AWS Security Finding Format). Dans le format ASFF, le champ `Types` fournit le type de résultat. Les résultats du pare-feu DNS peuvent avoir les valeurs suivantes pour`Types`.

- `TTPs/Impact/Impact:Runtime-MaliciousDomainRequest.Reputation`

Réessayer lorsque Security Hub n'est pas disponible

Si Security Hub n'est pas disponible, DNS Firewall essaie à nouveau d'envoyer les résultats jusqu'à ce qu'ils soient reçus.

Mise à jour des résultats existants dans Security Hub

Le pare-feu DNS mettra à jour les résultats existants si le même résultat est à nouveau observé.

Découverte typique du pare-feu DNS

Security Hub ingère les résultats du pare-feu DNS au format ASFF (AWS Security Finding Format).

Voici un exemple de découverte typique du pare-feu DNS dans ASFF.


```
{
            "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"
```

```
        }
```

Activation et configuration de l'intégration

Pour intégrer le pare-feu DNS à Security Hub, vous devez d'abord activer Security Hub. Pour plus d'informations sur l'activation de Security Hub, consultez la section Enabling Security Hub dans le guide de AWS Security Hub l'utilisateur.

Arrêt de la transmission des résultats à Security Hub

Pour arrêter d'envoyer les résultats du pare-feu DNS à Security Hub, vous pouvez utiliser la console Security Hub ou l'API Security Hub.

Pour obtenir des instructions, consultez la section Désactivation du flux de résultats d'une intégration dans le guide de l'AWS Security Hub utilisateur.

Surveillance d'Amazon Route 53

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances de vos AWS solutions. Vous devez collecter des données de surveillance provenant de toutes les parties de votre AWS solution afin de pouvoir corriger plus facilement une défaillance multipoint, le cas échéant. Toutefois, avant de commencer la surveillance, vous devez créer un plan de surveillance qui contient les réponses aux questions suivantes :

- Quels sont les objectifs de la surveillance ?
- Quelles sont les ressources à surveiller ?
- À quelle fréquence les ressources doivent-elles être surveillées ?
- Quels outils de surveillance utiliser ?
- Qui exécute les tâches de supervision ?
- Qui doit être informé en cas de problème ?

Rubriques

- Journalisation des requêtes DNS publiques
- Journalisation des requêtes Resolver
- Surveillance des registres de domaines
- Surveillance de vos ressources grâce aux bilans de santé d'Amazon Route 53 et à Amazon CloudWatch
- Surveillance des zones hébergées à l'aide d'Amazon CloudWatch
- Surveillance des points de terminaison Route 53 Resolver avec Amazon CloudWatch
- Surveillance des groupes de règles du pare-feu DNS Route 53 Resolver avec Amazon CloudWatch
- Gestion des événements du pare-feu DNS Route 53 Resolver à l'aide de Amazon EventBridge
- Journalisation des appels d'API Amazon Route 53 avec AWS CloudTrail

Journalisation des requêtes DNS publiques

Vous pouvez configurer Amazon Route 53 pour qu'il journalise les informations concernant les requêtes DNS publiques reçues par Route 53, telles que les suivantes :

- Domaine ou sous-domaine demandé
- Date et heure de la requête
- Type de registre DNS (comme A ou AAAA)
- Emplacement périphérique Route 53 ayant répondu à la requête DNS
- Code de réponse DNS, tel que `NoError` ou `ServFail`

Une fois que vous avez configuré la journalisation des requêtes, Route 53 envoie les CloudWatch journaux à Logs. Vous utilisez CloudWatch les outils Logs pour accéder aux journaux de requêtes.

Les journaux des requêtes contiennent uniquement les requêtes acheminées par les résolveurs DNS vers Route 53. Si un résolveur DNS a déjà mis en cache la réponse à une requête (par exemple, l'adresse IP d'un équilibreur de charge pour example.com), le résolveur continuera à renvoyer la réponse en cache sans réacheminer la requête à Route 53 jusqu'à ce que la durée de vie (TTL) du registre correspondant arrive à expiration.

Selon le nombre de requêtes DNS qui sont soumises pour un nom de domaine (example.com) ou nom de sous-domaine (www.example.com), les résolveurs auxquels vos utilisateurs ont recours et la durée de vie (TTL) du registre, les journaux de requêtes peuvent contenir des informations concernant une seule requête sur les plusieurs milliers de requêtes qui sont soumises aux résolveurs DNS. Pour en savoir plus sur la façon dont les requêtes DNS fonctionnent, consultez Acheminement du trafic Internet vers votre site web ou votre application web.

Si vous n'avez pas besoin d'informations de connexion détaillées, vous pouvez utiliser CloudWatch les métriques Amazon pour connaître le nombre total de requêtes DNS auxquelles Route 53 répond pour une zone hébergée. Pour de plus amples informations, veuillez consulter Affichage des métriques de requête DNS pour une zone hébergée publique.

Rubriques

- Configuration de la journalisation des requêtes DNS
- Utilisation d'Amazon CloudWatch pour accéder aux journaux de requêtes DNS
- Modification de la période de conservation des journaux et exportation de journaux vers Amazon S3
- Arrêt de la journalisation des requêtes
- Valeurs qui apparaissent dans les journaux de requête DNS
- Exemple de journal de requête

Configuration de la journalisation des requêtes DNS

Pour lancer la journalisation des requêtes DNS pour une zone hébergée, effectuez les tâches suivantes dans la console Amazon Route 53 :

- Choisissez le groupe de CloudWatch journaux dans lequel vous souhaitez que Route 53 publie des journaux, ou créez un nouveau groupe de journaux.

  > **Note**
  >
  > Le groupe de journaux doit résider dans la région USA East (N. Virginia) (USA Est [Virginie du Nord]).

- Choisissez Create (Créer) pour terminer.

> **Note**
>
> Si des utilisateurs envoient des requêtes DNS pour votre domaine, vous devriez commencer à voir ces requêtes dans les journaux plusieurs minutes après avoir créé la configuration de journalisation.

Pour configurer la journalisation des requêtes DNS

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le panneau de navigation, choisissez Hosted zones (Zones hébergées).
3. Choisissez la zone hébergée pour laquelle vous souhaitez configurer la journalisation des requêtes.
4. Dans le volet Détails de la zone hébergée, choisissez Configurer la journalisation des requêtes.
5. Choisissez un groupe de journaux existant ou créez un groupe de journaux.
6. Si vous recevez une alerte sur les autorisations (cela se produit si vous n'avez pas configuré la journalisation des requêtes avec la nouvelle console auparavant), effectuez l'une des opérations suivantes :

   - Si vous avez déjà 10 stratégies de ressources, vous ne pouvez plus en créer. Sélectionnez l'une de vos stratégies de ressources, puis sélectionnezModifier. L'édition donnera à Route

53 l'autorisation d'écrire des journaux dans vos groupes de journaux. Choisissez Enregistrer. L'alerte disparaît et vous pouvez passer à l'étape suivante.

- Si vous n'avez jamais configuré la journalisation des requêtes auparavant (ou si vous n'avez pas encore créé 10 politiques de ressources), vous devez autoriser Route 53 à écrire des journaux dans vos groupes de CloudWatch journaux. Choisissez Grant permissions (Accorder des autorisations). L'alerte disparaît et vous pouvez passer à l'étape suivante.

7. Choisissez Autorisations - facultatif pour voir un tableau indiquant si la politique de ressources correspond au groupe de CloudWatch journaux et si Route 53 est autorisée à publier des journaux sur CloudWatch.
8. Choisissez Créer.

Utilisation d'Amazon CloudWatch pour accéder aux journaux de requêtes DNS

Amazon Route 53 envoie les journaux de requêtes directement à CloudWatch Logs ; les journaux ne sont jamais accessibles via Route 53. Vous utilisez plutôt CloudWatch les journaux pour afficher les journaux en temps quasi réel, rechercher et filtrer les données, et exporter les journaux vers Amazon S3.

Route 53 crée un flux de CloudWatch journaux pour chaque emplacement périphérique Route 53 qui répond aux requêtes DNS pour la zone hébergée spécifiée et envoie les journaux de requêtes au flux de journaux applicable. Le format du nom de chaque flux de journal est*`hosted-zone-id`*/*`edge-location-ID`*, par exemple,`Z1D633PJN98FT9/DFW3`.

Chaque position périphérique est identifiée par un code à trois lettres et un numéro attribué arbitrairement, par exemple,. DFW3 Le code sur trois lettres correspond généralement au code IATA (International Air Transport Association) d'un aéroport proche de l'emplacement périphérique. (Ces abréviations peuvent changer à l'avenir.) Pour obtenir la liste des emplacements périphériques, consultez « Le réseau global Route 53 » sur la page Description détaillée de Route 53.

> **Note**
>
> Il se peut que certains préfixes ou suffixes ne respectent pas la convention ci-dessus. Ces attributs de codage sont destinés à un usage interne uniquement.

Pour plus d'informations, consultez la documentation pertinente :

- Guide de l'utilisateur d'Amazon CloudWatch Logs
- Référence de l'API Amazon CloudWatch Logs
- CloudWatch Section Logs de la référence des AWS CLI commandes
- Valeurs qui apparaissent dans les journaux de requête DNS

Modification de la période de conservation des journaux et exportation de journaux vers Amazon S3

Par défaut, CloudWatch Logs stocke les journaux de requêtes indéfiniment. Vous pouvez éventuellement spécifier une période de conservation afin que CloudWatch Logs supprime les journaux antérieurs à cette période de conservation. Pour plus d'informations, consultez la section Conservation des données du journal des modifications dans CloudWatch Logs du guide de CloudWatch l'utilisateur Amazon.

Si vous souhaitez conserver les données des CloudWatch journaux mais que vous n'avez pas besoin d'outils de journalisation pour les visualiser et les analyser, vous pouvez exporter les journaux vers Amazon S3, ce qui peut réduire vos coûts de stockage. Pour plus d'informations, veuillez consulter Exportation de données de journal vers Amazon S3.

Pour plus d'informations sur la tarification, veuillez consulter la page dédiée à ce sujet :

- « Amazon CloudWatch Logs » sur la page de CloudWatch tarification
- Tarification Amazon S3

> **Note**
>
> Lorsque vous configurez Route 53 pour consigner des requêtes DNS, vous ne devez régler aucun frais logiciel.

Arrêt de la journalisation des requêtes

Si vous souhaitez qu'Amazon Route 53 arrête d'envoyer des journaux de requêtes à CloudWatch Logs, effectuez la procédure suivante pour supprimer la configuration de journalisation des requêtes.

Pour supprimer une configuration de journalisation des requêtes

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le panneau de navigation, choisissez Hosted zones (Zones hébergées).
3. Sélectionnez le nom de la zone hébergée pour laquelle vous souhaitez supprimer la configuration de journalisation des requêtes.
4. Dans le volet Hosted zone details (Détails de la zone hébergée), choisissez Delete query logging configuration (Supprimer la configuration de la journalisation des requêtes).
5. Choisissez Supprimer pour confirmer.

Valeurs qui apparaissent dans les journaux de requête DNS

Chaque fichier journal contient une entrée de journal par requête DNS qu'Amazon Route 53 a reçu de la part de résolveurs DNS à l'emplacement périphérique correspondant. Chaque entrée du journal contient les valeurs suivantes :

Version de format du journal

Numéro de version de ce journal de requêtes. Si nous ajoutons des champs au journal ou modifions le format des champs existants, nous incrémentons cette valeur.

Horodatage de la requête

La date et l'heure de la réponse de Route 53 à cette requête, au format ISO 8601 et en temps universel coordonné (UTC), par exemple `2017-03-16T19:20:25.177Z`.

Pour plus d'informations sur le format ISO 8601, consultez l'article Wikipédia ISO 8601. Pour plus d'informations sur UTC, consultez l'article Wikipédia Temps universel coordonné.

ID de la zone hébergée

ID de la zone hébergée associée à l'ensemble des requêtes DNS du journal.

Nom de la requête

Domaine ou sous-domaine spécifié dans la requête.

Type de requête

Type de registre DNS indiqué dans la requête, ou `ANY`. Pour en savoir plus sur les types pris en charge par Route 53, veuillez consulter Types d'enregistrements DNS pris en charge.

Code de réponse

Code de réponse DNS retourné par Route 53 en réponse à la requête DNS.

Protocole de couche 4

Protocole utilisé pour soumettre la requête, à savoir `TCP` ou `UDP`.

Emplacement périphérique Route 53

L'emplacement périphérique Route 53 qui a répondu à la requête. Chaque position de bord est identifiée par un code à trois lettres et un nombre arbitraire, DFW3 par exemple. Le code sur trois lettres correspond généralement au code IATA (International Air Transport Association) d'un aéroport proche de l'emplacement périphérique. (Ces abréviations peuvent changer à l'avenir.)

Pour obtenir la liste des emplacements périphériques, veuillez consulter « Le réseau global Route 53 » sur la page Description détaillée de Route 53.

Resolver IP address (Adresse IP du résolveur)

L'adresse IP du résolveur DNS qui envoyé la requête à Route 53.

Sous-réseau client EDNS

Adresse IP partielle du client dont émane la requête, si elle peut être obtenue auprès du résolveur DNS.

Pour plus d'informations, consultez le projet IETF Client Subnet in DNS Requests.

Exemple de journal de requête

Voici un exemple de journal de requête (Région est un espace réservé) :

```
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 -
```

Journalisation des requêtes Resolver

Vous pouvez enregistrer les requêtes DNS suivantes :

- Les requêtes provenant d'Amazon Virtual Private Cloud VPCs que vous spécifiez, ainsi que les réponses à ces requêtes DNS.
- Requêtes provenant de ressources locales qui utilisent un point de terminaison Resolver entrant.
- Requêtes qui utilisent un point de terminaison Resolver sortant pour la résolution DNS récursive.
- Requêtes qui utilisent des règles Route 53 Resolver DNS Firewall pour bloquer, autoriser ou surveiller les listes de domaines.

Les journaux de requêtes Resolver incluent des valeurs telles que :

- La AWS région dans laquelle le VPC a été créé
- L'ID du VPC d'origine de la requête
- L'adresse IP de l'instance d'origine de la requête
- L'ID d'instance de la ressource d'origine de la requête
- La date et l'heure auxquelles la requête a été effectuée pour la première fois
- Le nom DNS demandé (tel que prod.example.com)
- Type de registre DNS (par exemple, A ou AAAA)
- Code de réponse DNS, tel que `NoError` ou `ServFail`
- Les données de réponse DNS, telles que l'adresse IP retournée en réponse à la requête DNS
- Une réponse à une action de règle de pare-feu DNS

Pour lire une liste détaillée de toutes les valeurs enregistrées et lire un exemple, veuillez consulter Valeurs qui apparaissent dans les journaux de requête Resolver.

> **Note**
>
> Comme c'est le cas pour les résolveurs DNS, les résolveurs mettent en cache les requêtes DNS pendant une durée déterminée par le time-to-live (TTL) du résolveur. Le résolveur Route 53 met en cache les requêtes qui proviennent de vous VPCs et répond depuis le cache chaque fois que cela est possible pour accélérer les réponses. La journalisation

des requêtes Resolver enregistre uniquement les requêtes uniques, et non les requêtes auxquelles Resolver est capable de répondre à partir du cache.
Supposons, par exemple, qu'une EC2 instance appartenant à l'une des configurations de journalisation des requêtes enregistre des requêtes soumette une demande pour accounting.example.com. VPCs Resolver met en cache la réponse à cette requête et consigne la requête. Si l'interface réseau Elastic de la même instance effectue une requête pour accounting.example.com dans la durée de vie (TTL) du cache de Resolver, Resolver répond à la requête depuis le cache. La deuxième requête n'est pas consignée.

Vous pouvez envoyer les journaux à l'une des AWS ressources suivantes :

- Groupe de CloudWatch journaux Amazon CloudWatch Logs (Logs)
- Compartiment Amazon S3 (S3)
- Flux de diffusion Firehose

Pour de plus amples informations, veuillez consulter AWS ressources auxquelles vous pouvez envoyer les journaux de requêtes du résolveur.

Rubriques

- AWS ressources auxquelles vous pouvez envoyer les journaux de requêtes du résolveur
- Gestion des configurations de journalisation des requêtes Resolver

AWS ressources auxquelles vous pouvez envoyer les journaux de requêtes du résolveur

> **Note**
>
> Si vous prévoyez de consigner les requêtes pour les charges de travail avec des requêtes élevées par seconde (QPS), vous devez utiliser Amazon S3 pour vous assurer que vos journaux de requêtes ne sont pas limités lorsqu'ils sont écrits sur votre destination. Si vous utilisez Amazon CloudWatch, vous pouvez augmenter la limite de demandes par seconde pour l'`PutLogEvents`opération. Pour en savoir plus sur l'augmentation de vos CloudWatch limites, consultez la section Quotas de CloudWatch journaux dans le guide de CloudWatch l'utilisateur Amazon.

Vous pouvez envoyer les journaux de requêtes du Resolver aux AWS ressources suivantes :

Groupe de CloudWatch journaux Amazon CloudWatch Logs (Amazon Logs)

Vous pouvez analyser les journaux à l'aide de Logs Insights et créer des métriques et des alarmes.

Pour plus d'informations, consultez le guide de l'utilisateur Amazon CloudWatch Logs.

Compartiment Amazon S3 (S3)

Un compartiment S3 est économique pour un archivage à long terme. La latence est généralement plus élevée.

Toutes les options de chiffrement côté serveur S3 sont prises en charge. Pour plus d'informations, consultez la section Protection des données avec un chiffrement côté serveur dans le Guide de l'utilisateur d'Amazon S3.

Si le compartiment S3 se trouve dans un compte que vous possédez, les autorisations requises sont automatiquement ajoutées à votre stratégie de compartiment. Si vous souhaitez envoyer des journaux à un compartiment S3 dans un compte que vous ne possédez pas, le propriétaire du compartiment S3 doit ajouter des autorisations pour votre compte dans sa stratégie de compartiment. Par exemple :

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/*"
        },
        {
            "Effect": "Allow",
            "Principal": {
```

```
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::your_bucket_name"
        },
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "iam_user_arn_or_account_number_for_root"
            },
            "Action": "s3:ListBucket",
            "Resource": "arn:aws:s3:::your_bucket_name"
        }
    ]
}
```

> **Note**
>
> Si vous souhaitez stocker des journaux dans un compartiment S3 central pour votre organisation, nous vous recommandons de configurer vos paramètres de journalisation des requêtes à partir d'un compte centralisé (avec les autorisations nécessaires pour écrire dans un compartiment central) et d'utiliser RAM pour partager la configuration entre les comptes.

Pour en savoir plus, consultez Guide de l'utilisateur Amazon Simple Storage Service.

Flux de diffusion Firehose

Vous pouvez diffuser les journaux en temps réel vers Amazon OpenSearch Service, Amazon Redshift ou d'autres applications.

Pour plus d'informations, consultez le guide du développeur Amazon Data Firehose.

Pour plus d'informations sur la tarification de la journalisation des requêtes Resolver, consultez les CloudWatch tarifs Amazon.

CloudWatch Les frais de Vended Logs s'appliquent lors de l'utilisation des journaux Resolver, même lorsque les journaux sont publiés directement sur Amazon S3. Pour plus d'informations, consultez la section Tarification des journaux sur Amazon CloudWatch .

Gestion des configurations de journalisation des requêtes Resolver

Configuration (journalisation des requêtes Resolver)

Pour commencer à enregistrer les requêtes DNS provenant de votre VPCs, vous devez effectuer les tâches suivantes dans la console Amazon Route 53 :

Pour configurer la journalisation des requêtes Resolver

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Développez le menu de la console Route 53. Dans le coin supérieur gauche de la console, sélectionnez l'icone des trois barres horizontales

   (≡
3. Dans le menu Resolver, choisissez Query logging (Journalisation des requêtes).
4. Dans le sélecteur de région, choisissez la AWS région dans laquelle vous souhaitez créer la configuration de journalisation des requêtes. Il doit s'agir de la même région que celle dans laquelle vous avez créé VPCs celle pour laquelle vous souhaitez enregistrer les requêtes DNS. Si vous avez plusieurs VPCs régions, vous devez créer au moins une configuration de journalisation des requêtes pour chaque région.
5. Choisissez Configure query logging (Configurer la journalisation des requêtes).
6. Indiquez l'une des valeurs suivantes :

   Nom de la configuration de journalisation des requêtes

   Saisissez un nom pour votre configuration de journalisation des requêtes. Le nom s'affiche dans la console, dans la liste des configurations de journalisation des requêtes. Saisissez un nom qui vous aidera à retrouver la configuration plus tard.

   Destination des journaux de requête

   Choisissez le type de AWS ressource à laquelle Resolver doit envoyer les journaux de requêtes. Pour plus d'informations sur le choix entre les options (groupe de CloudWatch journaux, compartiment S3 et flux de diffusion Firehose), consultez. AWS ressources auxquelles vous pouvez envoyer les journaux de requêtes du résolveur

   Après avoir choisi le type de ressource, vous pouvez créer une autre ressource de ce type ou choisir une ressource existante créée par le AWS compte courant.

> **Note**
>
> Vous ne pouvez choisir que les ressources créées dans la AWS région que vous avez choisie à l'étape 4, la région dans laquelle vous créez la configuration de journalisation des requêtes. Si vous choisissez de créer une nouvelle ressource, celle-ci sera créée dans la même région.

VPCs pour enregistrer les requêtes pour

Cette configuration d'enregistrement des requêtes enregistrera les requêtes DNS qui proviennent du fichier VPCs que vous avez choisi. Cochez la case correspondant à chaque VPC de la région actuelle pour laquelle vous souhaitez que Resolver journalise les requêtes, puis sélectionnez Choose (Choisir).

> **Note**
>
> La diffusion des journaux VPC ne peut être activée qu'une seule fois pour un type de destination spécifique. Les journaux ne peuvent pas être diffusés vers plusieurs destinations du même type. Par exemple, les journaux VPC ne peuvent pas être livrés à 2 destinations Amazon S3.

7. Choisissez Configure query logging (Configurer la journalisation des requêtes).

> **Note**
>
> Vous devriez commencer à voir ces requêtes DNS exécutées par les ressources de votre VPC dans les journaux quelques minutes après avoir créé avec succès la configuration de journalisation.

Valeurs qui apparaissent dans les journaux de requête Resolver

Chaque fichier journal contient une entrée de journal par requête DNS qu'Amazon Route 53 a reçu de la part de résolveurs DNS à l'emplacement périphérique correspondant. Chaque entrée du journal contient les valeurs suivantes :

version

Le numéro de version de ce journal de requêtes. La version actuelle est `1.1`.

La valeur de la version est une version majeure et mineure au format **`major_version.minor_version`**. Par exemple, vous pouvez avoir une valeur `version` de `1.7`, où 1 est la version majeure, et 7 est la version mineure.

La version majeure est incrémentée si Route 53 apporte à la structure du journal une modification qui n'est pas rétrocompatible. Cela inclut la suppression d'un champ JSON déjà existant ou la modification de la représentation du contenu d'un champ (par exemple, un format de date).

La version mineure est incrémentée si Route 53 ajoute de nouveaux champs au fichier journal. Cela peut se produire si de nouvelles informations sont disponibles pour certaines ou toutes les requêtes DNS existantes dans un VPC.

account_id

L'ID du AWS compte qui a créé le VPC.

region

La AWS région dans laquelle vous avez créé le VPC.

vpc_id

L'ID du VPC d'origine de la requête.

query_timestamp

La date et l'heure à laquelle la requête a été soumise, au format ISO 8601 et en temps universel coordonné (UTC), par exemple `2017-03-16T19:20:177Z`.

Pour plus d'informations sur le format ISO 8601, consultez l'article Wikipédia ISO 8601. Pour plus d'informations sur UTC, consultez l'article Wikipédia Temps universel coordonné.

query_name

Le nom de domaine (example.com) ou nom de sous-domaine (www.example.com) indiqué dans la requête.

query_type

Type de registre DNS indiqué dans la requête, ou `ANY`. Pour en savoir plus sur les types pris en charge par Route 53, veuillez consulter Types d'enregistrements DNS pris en charge.

query_class

La classe de la requête.

rcode

Le code de réponse DNS retourné par Resolver en réponse à la requête DNS. Il indique si la requête était valide ou non. Le code de réponse le plus courant est `NOERROR`, ce qui signifie que la requête était valide. Si la réponse indique qu'elle n'est pas valide, Resolver retourne un code de réponse qui explique pourquoi elle ne l'est pas. Pour une liste des codes de réponse possibles, consultez le DNS RCODEs sur le site Web de l'IANA.

answer_type

Le type de registre DNS (tel que A, MX ou CNAME) de la valeur renvoyée par Resolver en réponse à la requête. Pour en savoir plus sur les types pris en charge par Route 53, veuillez consulter Types d'enregistrements DNS pris en charge.

rdata

La valeur retournée par Resolver en réponse à la requête. Par exemple, pour un enregistrement A, il s'agit d'une adresse IP au IPv4 format. Pour un registre CNAME, il s'agit du nom de domaine dans le registre CNAME.

answer_class

La classe de la réponse du résolveur à la requête.

srcaddr

Adresse IP de l'hôte à l'origine de la requête.

srcport

Le port de l'instance d'origine de la requête.

transport

Le protocole utilisé pour soumettre la requête DNS.

srcids

IDs du `instanceresolver_endpoint`, et de `resolver_network_interface` celui d'où provient ou est passée la requête DNS.

instance

L'ID de l'instance d'origine de la requête.

> **Note**
>
> Si vous voyez un ID d'instance dans les journaux de Amazon Route 53 Resolver requêtes qui n'est pas visible dans votre compte, cela peut être dû au fait que la requête DNS provient soit AWS CloudShell d'Amazon EKS, soit de la console Fargate, que vous avez utilisée. AWS Lambda

resolver_endpoint

L'ID du point de terminaison du résolveur qui transmet la requête DNS aux serveurs DNS locaux.

firewall_rule_group_id

L'ID du groupe de règles de pare-feu DNS correspondant au nom de domaine de la requête. Ce champ n'est renseigné que si le pare-feu DNS a trouvé une correspondance pour une règle dont l'action est définie pour alerter ou bloquer.

Pour plus d'informations sur les groupes de règles de pare-feu, consultez Règles et groupes de règles de pare-feu DNS.

firewall_rule_action

L'action indiquée par la règle qui correspond au nom de domaine de la requête. Ce champ n'est renseigné que si le pare-feu DNS a trouvé une correspondance pour une règle dont l'action est définie pour alerter ou bloquer.

firewall_domain_list_id

La liste des domaines indiquée par la règle qui correspond au nom de domaine de la requête. Ce champ n'est renseigné que si le pare-feu DNS a trouvé une correspondance pour une règle dont l'action est définie pour alerter ou bloquer.

additional_properties

Informations supplémentaires sur les événements de livraison du journal. is_delayed : s'il y a un retard dans la livraison des journaux.

Exemple de journal de requête Route 53 Resolver

Voici un exemple de journal de requête d'un résolveur :

```
    {
      "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"
  }
```

Partage des configurations de journalisation des requêtes de Resolver avec d'autres comptes AWS

Vous pouvez partager les configurations de journalisation des requêtes que vous avez créées à l'aide d'un AWS compte avec d'autres AWS comptes. Pour partager des configurations, la console Route 53 Resolver s'intègre à AWS Resource Access Manager. Pour plus d'informations sur Resource Access Manager, consultez le Guide de l'utilisateur Resource Access Manager.

Remarques :

Association à VPCs des configurations de journalisation de requêtes partagées

Si un autre AWS compte a partagé une ou plusieurs configurations avec le vôtre, vous pouvez l' VPCs associer à la configuration de la même manière que vous l' VPCs associez aux configurations que vous avez créées.

Suppression ou annulation du partage d'une configuration

Si vous partagez une configuration avec d'autres comptes, puis que vous la supprimez ou que vous arrêtez de la partager, et si une ou plusieurs d'entre VPCs elles sont associées à la configuration, Route 53 Resolver arrête d'enregistrer les requêtes DNS provenant de ces VPCs comptes.

Nombre maximum de configurations de journalisation des requêtes VPCs pouvant être associées à une configuration

Lorsqu'un compte crée une configuration et la partage avec un ou plusieurs autres comptes, le nombre maximum de comptes VPCs pouvant être associés à la configuration est appliqué par compte. Par exemple, si votre organisation possède 10 000 comptes, vous pouvez créer la configuration de journalisation des requêtes dans le compte central et la partager AWS RAM pour la partager avec les comptes de l'organisation. Les comptes de l'organisation associeront ensuite la configuration à leur VPCs comptage par rapport aux associations VPC de configuration du journal des requêtes de leur compte par Région AWS limite de 100. Toutefois, s' VPCs ils se trouvent tous dans un seul compte, il peut être nécessaire d'augmenter les limites de service du compte.

Pour consulter les quotas Resolver actuels, consultez Quotas sur Route 53 Resolver.

Autorisations

Pour partager une règle avec un autre AWS compte, vous devez être autorisé à utiliser l'PutResolverQueryLogConfigPolicyaction.

Restrictions relatives au AWS compte avec lequel une règle est partagée

Le compte avec lequel une règle est partagée ne peut pas modifier ni supprimer la règle.

Identification

Seul le compte qui a créé une règle peut ajouter, supprimer ou consulter les balises de la règle.

Pour consulter le statut de partage actuel d'une règle (y compris le compte qui a partagé la règle ou le compte avec lequel une règle est partagée) et partager des règles avec un autre compte, exécutez la procédure suivante.

Pour afficher le statut de partage et partager des configurations de journalisation des requêtes avec un autre compte AWS

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le panneau de navigation, choisissez Query Logging (Journalisation des requêtes).
3. Dans la barre de navigation, choisissez la région dans laquelle vous avez créé la règle.

   La colonne Sharing status (Statut de partage) affiche le statut de partage actuel des règles qui ont été créées par le compte actuel ou qui sont partagées avec le compte actuel :

   - Non partagé : le AWS compte actuel a créé la règle, et celle-ci n'est partagée avec aucun autre compte.
   - Shared by me (Partagé par moi) : le compte actuel a créé la règle et l'a partagée avec un ou plusieurs comptes.
   - Shared with me (Partagé avec moi) : un autre compte a créé la règle et l'a partagée avec le compte actuel.
4. Choisissez le nom de la règle dont vous souhaitez afficher les informations de partage ou que vous souhaitez partager avec un autre compte.

   Sur la `rule name` page Règle :, la valeur sous Propriétaire indique l'ID du compte qui a créé la règle. Il s'agit du compte actuel, à moins que la valeur Sharing status (Statut de partage) soit Shared with me (Partagée avec moi). Dans ce cas, l'option Owner (Propriétaire) désigne le compte qui a créé la règle et l'a partagée avec le compte actuel.

   L'état du partage est également affiché.
5. Choisissez Partager la configuration pour ouvrir la AWS RAM console
6. Pour créer un partage de ressources, suivez les étapes décrites dans la section Création d'un partage de ressources AWS RAM dans le guide de AWS RAM l'utilisateur.

> **Note**
>
> Vous ne pouvez pas mettre à jour les paramètres de partage. Si vous voulez modifier l'un des paramètres suivants, vous devez repartager une règle avec les nouveaux paramètres, puis supprimer les anciens paramètres de partage.

Surveillance des registres de domaines

Le tableau de bord Amazon Route 53 fournit des informations détaillées sur le statut de vos registres de domaine, y compris les éléments suivants :

- Statut des nouveaux registres de domaine
- Statut des transferts de domaines vers Route 53
- Liste des domaines qui approchent de la date d'expiration

Nous recommandons de vérifier régulièrement le tableau de bord dans la console Route 53, en particulier une fois que vous avez enregistré un nouveau domaine ou transféré un domaine vers Route 53, afin de confirmer que vous n'avez aucun problème à traiter.

Nous vous recommandons également de confirmer que les informations sur le contact pour vos domaines sont à jour. Lorsque la date d'expiration d'un domaine approche, nous envoyons au contact inscrit pour le domaine un e-mail contenant des informations sur la date d'expiration du domaine et comment le renouveler.

Surveillance de vos ressources grâce aux bilans de santé d'Amazon Route 53 et à Amazon CloudWatch

Vous pouvez surveiller vos ressources en créant des bilans de santé Amazon Route 53, qui permettent de collecter et CloudWatch de traiter des données brutes pour en faire des indicateurs lisibles en temps quasi réel. Ces statistiques sont enregistrées pour une durée de deux semaines de sorte que vous pouvez accéder aux informations historiques et acquérir un meilleur point de vue sur les performances de vos ressources. Par défaut, les données métriques pour les bilans de santé de Route 53 sont automatiquement envoyées à des CloudWatch intervalles d'une minute.

Pour plus d'informations sur les surveillances d'état Route 53, veuillez consulter Surveillance des bilans de santé à l'aide CloudWatch. Pour plus d'informations CloudWatch, consultez Qu'est-ce qu'Amazon CloudWatch ? dans le guide de CloudWatch l'utilisateur Amazon.

Métriques et dimensions pour les surveillances d'état Route 53

Lorsque vous créez un bilan de santé, Amazon Route 53 commence à envoyer des métriques et des dimensions une fois par minute CloudWatch à la ressource que vous spécifiez. La console

Route 53 vous permet d'afficher le statut de vos surveillances d'état. Vous pouvez également utiliser les procédures suivantes pour afficher les métriques dans la CloudWatch console ou à l'aide du AWS Command Line Interface (AWS CLI).

Pour afficher les métriques à l'aide de la CloudWatch console

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans le panneau de navigation, sélectionnez Metrics (Métriques).
3. Sous l'onglet Toutes les métriques, choisissez Route 53.
4. Choisissez Health Check Metrics (Métriques de surveillance d'état).

Pour consulter les statistiques à l'aide du AWS CLI

- À partir d'une invite de commande, utilisez la commande suivante :

```
aws cloudwatch list-metrics --namespace "AWS/Route53"
```

Rubriques

- CloudWatch métriques pour les bilans de santé de Route 53
- Dimensions pour les métriques de surveillance d'état Route 53

CloudWatch métriques pour les bilans de santé de Route 53

L'espace de nom `AWS/Route53` inclut les métriques suivantes pour les surveillances d'état Route 53 :

ChildHealthCheckHealthyCount

Pour une vérification de l'état calculée, le nombre de vérifications de l'état saines.

Statistiques valides : moyenne (recommandé), minimum, maximum

Unités : nombre

ConnectionTime

Le temps moyen, en millisecondes, qui a été nécessaire aux outils de surveillance d'état Route 53 pour établir une connexion TCP avec le point de terminaison. Vous pouvez consulter

`ConnectionTime` pour une surveillance d'état de contrôle soit dans toutes les régions, soit pour une région géographique sélectionnée.

Statistiques valides : moyenne (recommandé), minimum, maximum

Unités : millisecondes

HealthCheckPercentageHealthy

Le pourcentage des outils de surveillance d'état Route 53 qui considèrent le point de terminaison sélectionné comme sain.

Statistiques valides : moyenne, minimum, maximum

Unités : pourcentage

HealthCheckStatus

État du point de terminaison du bilan de santé en CloudWatch cours de vérification. 1 indique un état sain et 0 indique un état malsain.

Statistiques valides : minimum, moyenne et maximum

Unités : aucune

SSLHandshakeHeure

Le temps moyen, en millisecondes, qui a été nécessaire aux outils de surveillance d'état Route 53 pour établir la liaison SSL. Vous pouvez consulter `SSLHandshakeTime` pour une surveillance d'état de contrôle soit dans toutes les régions, soit pour une région géographique sélectionnée.

Statistiques valides : moyenne (recommandé), minimum, maximum

Unités : millisecondes

TimeToFirstByte

Le temps moyen, en millisecondes, qui a été nécessaire aux outils de surveillance d'état Route 53 pour recevoir le premier octet de la réponse à une requête HTTP ou HTTPS. Vous pouvez consulter `TimeToFirstByte` pour une surveillance d'état de contrôle soit dans toutes les régions, soit pour une région géographique sélectionnée.

Statistiques valides : moyenne (recommandé), minimum, maximum

Unités : millisecondes

Dimensions pour les métriques de surveillance d'état Route 53

Les métriques Route 53 pour les surveillances d'état utilisent l'espace de noms `AWS/Route53` et fournissent des métriques pour `HealthCheckId`. Lors de l'extraction des métriques, vous devez fournir à la fois la dimension `HealthCheckId`.

En outre, pour `ConnectionTime`, `SSLHandshakeTime` et `TimeToFirstByte`, vous pouvez spécifier le cas échéant `Region`. Si vous omettez`Region`, CloudWatch renvoie des statistiques pour toutes les régions. Si vous incluez`Region`, CloudWatch renvoie les statistiques uniquement pour la région spécifiée.

Pour de plus amples informations, veuillez consulter Surveillance des bilans de santé à l'aide CloudWatch.

Surveillance des zones hébergées à l'aide d'Amazon CloudWatch

Vous pouvez surveiller vos zones hébergées publiquement en utilisant Amazon CloudWatch pour collecter et traiter les données brutes en indicateurs lisibles en temps quasi réel. Les métriques sont disponibles peu de temps après que Route 53 ait reçu les requêtes DNS sur lesquelles les métriques sont basées. CloudWatch les données métriques des zones hébergées Route 53 ont une granularité d'une minute.

Pour plus d'informations, consultez la documentation suivante :

- Pour un aperçu et des informations sur la façon d'afficher les métriques dans la CloudWatch console Amazon et sur la façon de récupérer des métriques à l'aide du AWS Command Line Interface (AWS CLI), voir Affichage des métriques de requête DNS pour une zone hébergée publique
- Pour plus d'informations sur la période de conservation des métriques, consultez GetMetricStatisticsle Amazon CloudWatch API Reference.
- Pour plus d'informations CloudWatch, consultez Qu'est-ce qu'Amazon CloudWatch ? dans le guide de CloudWatch l'utilisateur Amazon.
- Pour plus d'informations sur CloudWatch les métriques, consultez la section Utilisation CloudWatch des métriques Amazon dans le guide de CloudWatch l'utilisateur Amazon.

Rubriques

- CloudWatch métriques pour les zones hébergées publiques de la Route 53

- CloudWatch dimension pour les métriques de la zone hébergée publique Route 53

CloudWatch métriques pour les zones hébergées publiques de la Route 53

L'espace de noms `AWS/Route53` inclut les métriques suivantes pour les zones hébergées Route 53 :

DNSQueries

Pour une zone hébergée, le nombre de requêtes DNS auxquelles Route 53 répond au cours d'une période indiquée.

Statistiques valides : Sum, SampleCount

Unités : nombre

Région : Route 53 est un service global. Pour obtenir les métriques de zone hébergée, vous devez spécifier USA Est (Virginie du Nord) pour la région.

DNSSECInternalDéfaillance

La valeur est 1 si un objet de la zone hébergée est dans un état INTERNAL_FAILURE. Sinon, la valeur est 0.

Statistiques valides : somme

Unités : nombre

Volume : 1 par 4 heures par zone hébergée

Région : Route 53 est un service global. Pour obtenir les métriques de zone hébergée, vous devez spécifier USA Est (Virginie du Nord) pour la région.

DNSSECKeySigningKeysNeedingAction

Nombre de clés de signature (KSKs) ayant l'état ACTION_NEEDED (en raison d'une défaillance du KMS).

Statistiques valides : Sum, SampleCount

Unités : nombre

Volume : 1 par 4 heures par zone hébergée

Région : Route 53 est un service global. Pour obtenir les métriques de zone hébergée, vous devez spécifier USA Est (Virginie du Nord) pour la région.

DNSSECKeySigningKeyMaxNeedingActionAge

Le temps écoulé depuis que la clé de signature de clé (KSK) a été définie sur l'état ACTION_NEED.

Statistiques valides : maximum

Unités : secondes

Volume : 1 par 4 heures par zone hébergée

Région : Route 53 est un service global. Pour obtenir les métriques de zone hébergée, vous devez spécifier USA Est (Virginie du Nord) pour la région.

DNSSECKeySigningKeyAge

Le temps écoulé depuis la création de la clé de signature de clé (KSK) (et non depuis son activation).

Statistiques valides : maximum

Unités : secondes

Volume : 1 par 4 heures par zone hébergée

Région : Route 53 est un service global. Pour obtenir les métriques de zone hébergée, vous devez spécifier USA Est (Virginie du Nord) pour la région.

CloudWatch dimension pour les métriques de la zone hébergée publique Route 53

Les métriques Route 53 pour les zones hébergées utilisent l'espace de noms `AWS/Route53` et fournissent des métriques pour `HostedZoneId`. Pour obtenir le nombre de requêtes DNS, vous devez spécifier l'ID de la zone hébergée dans la dimension `HostedZoneId`.

Surveillance des points de terminaison Route 53 Resolver avec Amazon CloudWatch

Vous pouvez utiliser Amazon CloudWatch pour surveiller le nombre de requêtes DNS transmises par les points de terminaison Route 53 Resolver. Amazon CloudWatch collecte et traite les données

brutes pour en faire des indicateurs lisibles en temps quasi réel. Ces statistiques sont enregistrées pour une durée de deux semaines de sorte que vous pouvez accéder aux informations historiques et acquérir un meilleur point de vue sur les performances de vos ressources. Par défaut, les données métriques des points de terminaison du Resolver sont automatiquement envoyées toutes les cinq CloudWatch minutes. L'intervalle de cinq minutes est également le plus petit intervalle auquel les données des métriques peuvent être envoyées.

Pour plus d'informations sur Resolver, veuillez consulter Qu'est-ce que c'est Amazon Route 53 Resolver ?. Pour plus d'informations CloudWatch, consultez Qu'est-ce qu'Amazon CloudWatch ? dans le guide de CloudWatch l'utilisateur Amazon.

Métriques et dimensions pour Route 53 Resolver

Lorsque vous configurez Resolver pour transférer les requêtes DNS vers votre réseau ou vice versa, Resolver commence à envoyer des métriques et des dimensions toutes les cinq minutes à CloudWatch peu près au nombre de requêtes transférées. Vous pouvez utiliser les procédures suivantes pour afficher les métriques dans la CloudWatch console ou à l'aide du AWS Command Line Interface (AWS CLI).

Pour afficher les métriques du Resolver à l'aide de la console CloudWatch

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans la barre de navigation, choisissez la région dans laquelle vous avez créé le point de terminaison.
3. Dans le panneau de navigation, sélectionnez Metrics (Métriques).
4. Sous l'onglet Toutes les métriques, choisissez Route 53 Resolver.
5. Choisissez By Endpoint (Par point de terminaison) pour afficher le nombre de requêtes pour un point de terminaison indiqué. Ensuite, choisissez les points de terminaison pour lesquels vous souhaitez afficher le nombre de requêtes.

   Choisissez Across All Endpoints pour afficher le nombre de requêtes pour tous les points de terminaison entrants ou pour tous les endpoints sortants créés par le compte actuel. AWS Choisissez ensuite InboundQueryVolumeou OutboundQueryVolumepour afficher les dénombrements souhaités.

Pour consulter les statistiques à l'aide du AWS CLI

- À partir d'une invite de commande, utilisez la commande suivante :

```
aws cloudwatch list-metrics --namespace "AWS/Route53Resolver"
```

Rubriques

- CloudWatch métriques pour Route 53 Resolver
- Dimensions pour les métriques Route 53 Resolver

CloudWatch métriques pour Route 53 Resolver

L'espace de noms `AWS/Route53Resolver` inclut des métriques pour les points de terminaison Route 53 Resolver et les adresses IP.

Rubriques

- Métriques pour les points de terminaison Resolver
- Métriques pour les adresses IP Resolver

Métriques pour les points de terminaison Resolver

L'espace de noms `AWS/Route53Resolver` inclut les métriques suivantes pour les points de terminaison Route 53 Resolver.

EndpointHealthyENICount

Le nombre d'interfaces réseau Elastic dans l'état `OPERATIONAL`. Cela signifie que les interfaces réseau Amazon VPC pour ce point de terminaison (indiqué par `EndpointId`) sont correctement configurées et en mesure de transmettre les requêtes DNS entrantes ou sortantes entre votre réseau et Resolver.

Statistiques valides : Minimum, Maximum, Average

Unités : nombre

EndpointUnhealthyENICount

Le nombre d'interfaces réseau Elastic dans l'état `AUTO_RECOVERING`.

Cela signifie que le résolveur tente de récupérer une ou plusieurs des interfaces réseau Amazon VPC qui sont associées au point de terminaison (indiqué par `EndpointId`). Pendant le

processus de récupération, le point de terminaison fonctionne avec une capacité limitée et ne peut pas traiter les requêtes DNS tant qu'il n'est pas entièrement récupéré.

Statistiques valides : Minimum, Maximum, Average

Unités : nombre

InboundQueryVolume

Pour les points de terminaison entrants, le nombre de requêtes DNS transférées de votre réseau vers le vôtre VPCs via le point de terminaison spécifié par. `EndpointId`

Statistiques valides : somme

Unités : nombre

OutboundQueryVolume

Pour les points de terminaison sortants, le nombre de requêtes DNS transmises de vous VPCs à votre réseau via le point de terminaison spécifié par. `EndpointId`

Statistiques valides : somme

Unités : nombre

OutboundQueryAggregateVolume

Pour les points de terminaison sortants, le nombre total de requêtes DNS transférées depuis Amazon VPCs vers votre réseau, y compris les suivantes :

- Le nombre de requêtes DNS transférées de vous VPCs vers votre réseau via le point de terminaison spécifié par`EndpointId`.
- Lorsque le compte actuel partage les règles du résolveur avec d'autres comptes, les requêtes provenant de VPCs ce compte sont créées par d'autres comptes et transmises à votre réseau via le point de terminaison spécifié par`EndpointId`.

Statistiques valides : somme

Unités : nombre

ResolverEndpointCapacityStatus

État de capacité du point de terminaison du résolveur. La métrique indique l'état actuel d'utilisation de la capacité, dans lequel : 0 = OK (capacité opérationnelle normale), 1 = Avertissement (au moins une interface Elastic Network dépasse 50 % d'utilisation de la capacité) et 2 = Critical (au moins une interface Elastic Network dépasse 75 % d'utilisation de la capacité).

L'état de capacité est déterminé par plusieurs facteurs, notamment le volume des requêtes, la latence des requêtes, les protocoles DNS, la taille des paquets DNS et l'état du suivi des connexions.

Statistiques valides : maximum

Unités : aucune

> **Note**
>
> Dans certains cas, il est possible que vous observiez des lacunes dans cette métrique. Ces lacunes peuvent se produire lorsque vos interfaces réseau sont soumises à une maintenance ou à des mises à jour planifiées consécutives. Après la remise en service d'une interface réseau, il faut au moins une minute à notre service pour collecter les données opérationnelles et publier cette métrique. Ces lacunes n'indiquent pas que votre terminal Resolver est en panne. Si vous configurez une CloudWatch alarme pour cette métrique, nous vous recommandons ce qui suit :
>
> - Réglez l'alarme sur « Traiter les données manquantes comme ignorées ».
>
> Ou
>
> - Configurez une période d'évaluation de plus de cinq minutes pour le seuil d'alarme.
>
> Ces paramètres aideront à réduire les fausses alarmes lors des activités de maintenance normales.

Meilleures pratiques pour la gestion de la capacité des terminaux Resolver

Pour résoudre les problèmes de capacité, nous recommandons généralement d'augmenter le nombre d'interfaces réseau élastiques pour votre point de terminaison Resolver. Cependant, des considérations importantes doivent être prises en compte pour des types de terminaux spécifiques :

Pour les points de terminaison entrants, l'équilibrage de la charge de trafic dépend du client. Par conséquent, les avertissements de capacité ou les alertes critiques peuvent indiquer un « point chaud » où un sous-ensemble d'interfaces réseau élastiques est utilisé de manière disproportionnée.

- Pour identifier les problèmes potentiels d'équilibrage de charge, examinez les InboundQueryVolumemétriques de chaque interface Elastic Network individuellement.

Pour les points de terminaison sortants, le trafic est automatiquement équilibré entre les interfaces réseau élastiques. Les problèmes de capacité peuvent être dus à des problèmes liés au serveur de noms cible ou au fait que les requêtes à latence élevée ou les délais d'expiration surchargent les interfaces réseau du résolveur.

- Dans ces cas, le simple fait d'augmenter les interfaces réseau élastiques risque de ne pas être efficace, et nous vous recommandons de corriger le serveur de noms cible.

Métriques pour les adresses IP Resolver

L'espace de noms `AWS/Route53Resolver` inclut les métriques suivantes pour chaque adresse IP associée à un point de terminaison Resolver entrant ou sortant. (Lorsque vous spécifiez un point de terminaison, Resolver crée une interface réseau Elastic Amazon VPC.)

InboundQueryVolume

Pour chaque adresse IP de vos points de terminaison entrants, le nombre de requêtes DNS transférées de votre réseau à l'adresse IP spécifiée. Chaque adresse IP est identifiée par l'ID d'adresse IP. Vous pouvez obtenir cette valeur en utilisant la console Route 53. Sur la page correspondant au point de terminaison applicable, dans la section Adresses IP, reportez-vous à la colonne ID d'adresse IP. Vous pouvez également obtenir la valeur par programmation en utilisant. ListResolverEndpointIpAddresses

Statistiques valides : somme

Unités : nombre

OutboundQueryAggregateVolume

Pour chaque adresse IP de vos points de terminaison sortants, le nombre total de requêtes DNS transférées d'Amazon VPCs vers votre réseau, y compris les suivantes :

- Le nombre de requêtes DNS transmises de votre part VPCs à votre réseau à l'aide de l'adresse IP spécifiée.
- Lorsque le compte courant partage les règles du résolveur avec d'autres comptes, les requêtes provenant de VPCs ce compte sont créées par d'autres comptes qui sont transmises à votre réseau en utilisant l'adresse IP spécifiée.

Chaque adresse IP est identifiée par l'ID d'adresse IP. Vous pouvez obtenir cette valeur en utilisant la console Route 53. Sur la page correspondant au point de terminaison applicable, dans

la section Adresses IP, reportez-vous à la colonne ID d'adresse IP. Vous pouvez également obtenir la valeur par programmation en utilisant. ListResolverEndpointIpAddresses

Statistiques valides : somme

Unités : nombre

Dimensions pour les métriques Route 53 Resolver

Les métriques Route 53 Resolver pour les points de terminaison entrants et sortants utilisent l'espace de noms `AWS/Route53Resolver` et fournissent des métriques pour `EndpointId`. Si vous spécifiez une valeur pour la `EndpointId` dimension, CloudWatch renvoie le nombre de requêtes DNS pour le point de terminaison spécifié. Si vous ne le spécifiez pas`EndpointId`, CloudWatch renvoie le nombre de requêtes DNS pour tous les points de terminaison créés par le AWS compte actuel.

La dimension `RniId` est prise en charge pour les métriques `OutboundQueryAggregateVolume` et `InboundQueryVolume`.

Surveillance des groupes de règles du pare-feu DNS Route 53 Resolver avec Amazon CloudWatch

Vous pouvez utiliser Amazon CloudWatch pour surveiller le nombre de requêtes DNS filtrées par les groupes de règles du pare-feu DNS Route 53 Resolver. Amazon CloudWatch collecte et traite les données brutes pour en faire des indicateurs lisibles en temps quasi réel. Ces statistiques sont enregistrées pour une durée de deux semaines de sorte que vous pouvez accéder aux informations historiques et acquérir un meilleur point de vue sur les performances de vos ressources. Par défaut, les données métriques relatives aux groupes de règles du pare-feu DNS sont automatiquement envoyées CloudWatch toutes les cinq minutes.

Pour en savoir plus sur le pare-feu DNS, veuillez consulter Utilisation du pare-feu DNS pour filtrer le trafic DNS sortant. Pour plus d'informations CloudWatch, consultez Qu'est-ce qu'Amazon CloudWatch ? dans le guide de CloudWatch l'utilisateur Amazon.

Métriques et dimensions pour le pare-feu DNS Route 53 Resolver

Lorsque vous associez un groupe de règles de pare-feu DNS Route 53 Resolver à un VPC pour filtrer les requêtes DNS, le pare-feu DNS commence à envoyer des métriques et des dimensions toutes les

5 minutes CloudWatch à environ les requêtes qu'il filtre. Pour plus d'informations sur la métrique et la dimension pour les pare-feu DNS, veuillez consulter CloudWatch métriques pour le pare-feu DNS Route 53 Resolver.

Vous pouvez utiliser les procédures suivantes pour afficher les métriques dans la CloudWatch console ou à l'aide du AWS Command Line Interface (AWS CLI).

Pour afficher les métriques du pare-feu DNS à l'aide de la CloudWatch console

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans la barre de navigation, sélectionnez la région que vous souhaitez afficher.
3. Dans le panneau de navigation, sélectionnez Metrics (Métriques).
4. Sous l'onglet Toutes les métriques, choisissez Route 53 Resolver.
5. Choisissez une métrique qui vous intéresse.

Pour consulter les statistiques à l'aide du AWS CLI

- À partir d'une invite de commande, utilisez la commande suivante :

```
aws cloudwatch list-metrics --namespace "AWS/Route53Resolver"
```

Rubriques

- CloudWatch métriques pour le pare-feu DNS Route 53 Resolver

CloudWatch métriques pour le pare-feu DNS Route 53 Resolver

Le nom d'espace `AWS/Route53Resolver` comprends des métriques pour les groupes de règles Route 53 Resolver DNS Firewall.

Rubriques

- Métriques pour les groupes de règles Route 53 Resolver DNS Firewall
- Métriques pour VPCs
- Métriques pour le groupe de règles de pare-feu et l'association de VPC
- Métriques pour une liste de domaines dans un groupe de règles de pare-feu

Métriques pour les groupes de règles Route 53 Resolver DNS Firewall

FirewallRuleGroupQueryVolume

Le nombre de requêtes DNS Firewall correspondant à un groupe de règles de pare-feu (indiqué par `FirewallRuleGroupId`).

Dimensions : `FirewallRuleGroupId`

Statistiques valides : somme

Unités : nombre

Métriques pour VPCs

VpcFirewallQueryVolume

Le nombre de requêtes DNS Firewall à partir d'un VPC (indiqué par `VpcId`).

Dimensions : `VpcId`

Statistiques valides : somme

Unités : nombre

Métriques pour le groupe de règles de pare-feu et l'association de VPC

FirewallRuleGroupVpcQueryVolume

Le nombre de requêtes DNS Firewall de vos VPC (indiqué par `VpcId`) correspondant à un groupe de règles de pare-feu (indiqué par `FirewallRuleGroupId`).

Dimensions : `FirewallRuleGroupId, VpcId`

Statistiques valides : somme

Unités : nombre

Métriques pour une liste de domaines dans un groupe de règles de pare-feu

FirewallRuleQueryVolume

Le nombre de requêtes DNS Firewall correspondant à une liste de domaines de pare-feu (indiqué par `FirewallDomainListId`) dans un groupe de règles de pare-feu (indiqué par `FirewallRuleGroupId`).

Dimensions : `FirewallRuleGroupId, FirewallDomainListId`

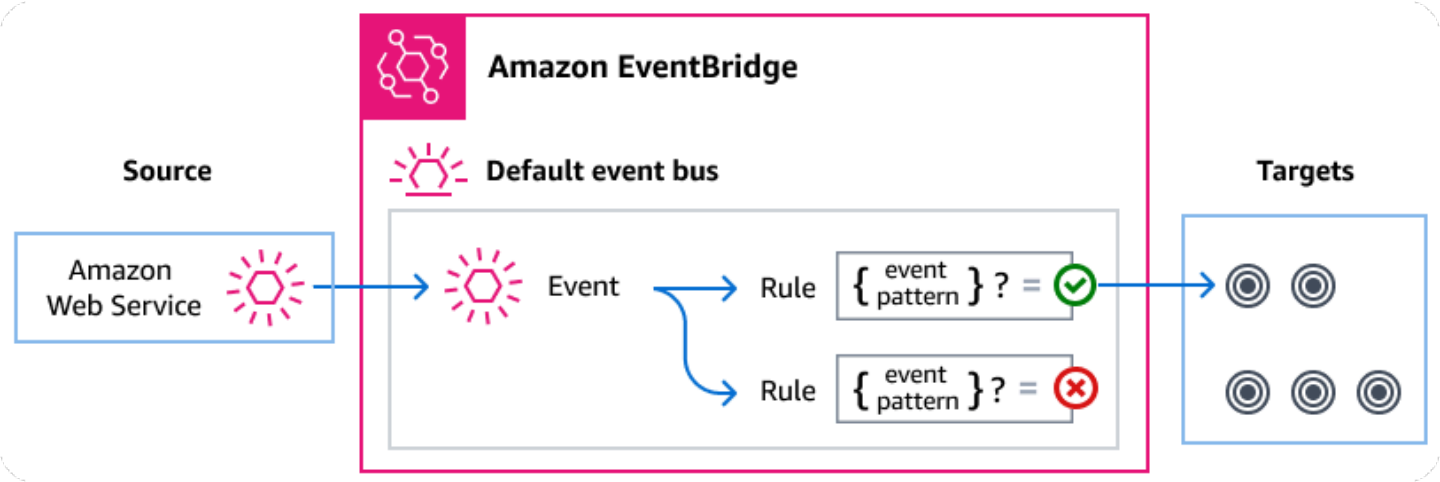
Statistiques valides : somme

Unités : nombre

Gestion des événements du pare-feu DNS Route 53 Resolver à l'aide de Amazon EventBridge

Amazon EventBridge est un service sans serveur qui utilise des événements pour connecter les composants de l'application entre eux, ce qui vous permet de créer plus facilement des applications évolutives pilotées par des événements. Une architecture pilotée par les événements est un style de création de systèmes logiciels faiblement couplés qui fonctionnent ensemble en émettant des événements et en y répondant. Les événements représentent une modification d'une ressource ou d'un environnement.

Comme c'est le cas pour de nombreux AWS services, le pare-feu DNS génère et envoie des événements au bus d'événements EventBridge par défaut. (Le bus d'événements par défaut est automatiquement configuré dans chaque AWS compte.) Un bus d'événements est un routeur qui reçoit des événements et les transmet à zéro ou plusieurs destinations, ou cibles. Les règles que vous définissez pour le bus d'événements évaluent les événements au fur et à mesure qu'ils arrivent. Chaque règle vérifie si un événement correspond au modèle d'événements de la règle. Si l'événement correspond, le bus d'événements envoie l'événement aux cibles spécifiées.



Rubriques

- Événements du pare-feu DNS Route 53 Resolver
- Envoi d'événements de pare-feu DNS Route 53 Resolver à l'aide EventBridge de règles
- Amazon EventBridge autorisations
- EventBridge Ressources supplémentaires
- Référence détaillée des événements du pare-feu DNS Route 53 Resolver

Événements du pare-feu DNS Route 53 Resolver

Route 53 Resolver envoie automatiquement les événements du pare-feu DNS au bus d' EventBridge événements par défaut. Vous pouvez créer des règles sur le bus d'événements ; chaque règle inclut un modèle d'événement et une ou plusieurs cibles. Les événements qui correspondent au modèle d'événements d'une règle sont transmis aux cibles spécifiées dans la mesure du possible. Les événements peuvent être livrés hors service.

Les événements suivants sont générés par le pare-feu DNS. Pour plus d'informations, consultez EventBridgele guide de Amazon EventBridge l'utilisateur. .

Type de détail de l'événement	Description
Bloc de pare-feu DNS	Toute action de blocage effectuée sur un domaine.
Alerte de pare-feu DNS	Toute action d'alerte exécutée sur un domaine.

Envoi d'événements de pare-feu DNS Route 53 Resolver à l'aide EventBridge de règles

Pour que le bus d'événements EventBridge par défaut envoie les événements du pare-feu DNS à une cible, vous devez créer une règle contenant un modèle d'événements correspondant aux données des événements du pare-feu DNS souhaités.

La création d'une règle comprend les étapes générales suivantes :

1. Création d'un modèle d'événement pour la règle qui spécifie :
   - Route 53 Resolver est la source des événements évalués par la règle.
   - (Facultatif) : Toute autre donnée d'événement à comparer.

   Pour de plus amples informations, consultez ???.
2. (Facultatif) : Création d'un transformateur d'entrée qui personnalise les données de l'événement EventBridge avant de les transmettre à la cible de la règle.

   Pour plus d'informations, consultez la section Transformation des entrées dans le guide de EventBridge l'utilisateur.
3. Spécifier la ou les cibles auxquelles vous souhaitez EventBridge envoyer des événements qui correspondent au modèle d'événement.

   Les cibles peuvent être d'autres AWS services, des applications software-as-a-service (SaaS), des destinations d'API ou d'autres points de terminaison personnalisés. Pour plus d'informations, veuillez consulter la rubrique Cibles dans le Guide de l'utilisateur EventBridge .

Pour obtenir des instructions complètes sur la création de règles de bus d'événements, voir Création de règles réagissant aux événements dans le Guide de EventBridge l'utilisateur.

Création de modèles d'événements pour les événements du pare-feu DNS Route 53 Resolver

Lorsque le pare-feu DNS envoie un événement au bus d'événements par défaut, il EventBridge utilise le modèle d'événement défini pour chaque règle afin de déterminer si l'événement doit être transmis aux cibles de la règle. Un modèle d'événement correspond aux données des événements de pare-feu DNS souhaités. Chaque modèle d'événement est un objet JSON qui contient :

- Un attribut `source` qui identifie le service qui envoie l'événement. Pour les événements du pare-feu DNS, la source est`aws.route53resolver`.
- (Facultatif) : un attribut `detail-type` qui contient un tableau des types d'événements à associer.
- (Facultatif) : un attribut `detail` qui contient toute autre donnée d'événement à rechercher.

Par exemple, le modèle d'événement suivant correspond à la fois aux événements d'alerte et de blocage du pare-feu DNS :

```
{
  "source": ["aws.route53resolver"],
  "detail-type": ["DNS Firewall Block", "DNS Firewall Alert"]
}
```

Alors que le modèle d'événement suivant correspond à une action BLOCK :

```
{
  "source": ["aws.route53resolver"],
  "detail-type": ["DNS Firewall Block"]
}
```

Le pare-feu DNS envoie le même événement pour le même domaine une seule fois par période de 6 heures. Par exemple :

1. L'instance i-123 a envoyé une requête DNS exampledomain.com à l'instant T1. Le pare-feu DNS envoie une alerte ou un événement de blocage car il s'agit de la première occurrence.
2. L'instance i-123 a envoyé un DNSquery exempledomain.com à l'heure T1+30 minutes. Le pare-feu DNS n'envoie pas d'alerte ni d'événement de blocage car il s'agit d'un événement récurrent dans un délai de 6 heures.
3. L'instance i-123 a envoyé une requête DNS exampledomain.com à l'heure T1+7 heures. Le pare-feu DNS envoie une alerte ou un événement de blocage lorsque celui-ci se produit en dehors du délai de 6 heures.

Pour plus d'informations sur la rédaction de modèles d'événements, consultez la section Modèles d'événements dans le guide de EventBridge l'utilisateur.

Test des modèles d'événements pour les événements du pare-feu DNS dans EventBridge

Vous pouvez utiliser le EventBridge Sandbox pour définir et tester rapidement un modèle d'événement, sans avoir à terminer le processus plus vaste de création ou de modification d'une règle. À l'aide du Sandbox, vous pouvez définir un modèle d'événement et utiliser un exemple d'événement pour confirmer que le modèle correspond aux événements souhaités. EventBridge vous permettent de créer une nouvelle règle à l'aide de ce modèle d'événement, directement depuis le sandbox.

Pour plus d'informations, consultez la section Tester un modèle d'événement à l'aide du EventBridge Sandbox dans le guide de l'EventBridge utilisateur.

Création d'une EventBridge règle et d'une cible pour le pare-feu DNS

La procédure suivante explique comment créer une règle qui permet EventBridge d'envoyer des événements pour toutes les actions d'alerte et de blocage du pare-feu DNS, et d'ajouter une AWS Lambda fonction en tant que cible pour la règle.

1. AWS CLI À utiliser pour créer une EventBridge règle :

```
aws events put-rule \
--event-pattern "{\"source\":
[\"aws.route53resolver\"],\"detail-type\":
[\"DNS Firewall Block\", \"DNS Firewall Alert\"]}" \
--name dns-firewall-rule
```

2. Attachez une fonction Lambda comme cible pour la règle :

```
AWS events put-targets --rule dns-firewall-rule --targets
Id=1,Arn=arn:aws:lambda:us-east-1:111122223333:function:<your_function>
```

3. Pour ajouter les autorisations requises pour appeler la cible, exécutez la commande Lambda AWS CLI suivante :

```
AWS lambda add-permission --function-name <your_function> --statement-
id 1 --action 'lambda:InvokeFunction' --principal events.amazonaws.com
```

Amazon EventBridge autorisations

Le pare-feu DNS ne nécessite aucune autorisation supplémentaire pour transmettre des événements à Amazon EventBridge.

Les cibles que vous spécifiez peuvent nécessiter des autorisations ou une configuration spécifiques. Pour plus de détails sur l'utilisation de services spécifiques pour les cibles, voir Amazon EventBridge les cibles dans le guide de Amazon EventBridge l'utilisateur.

EventBridge Ressources supplémentaires

Reportez-vous aux rubriques suivantes du guide de Amazon EventBridge l'utilisateur pour plus d'informations sur le traitement et la gestion des événements. EventBridge

- Pour des informations détaillées sur le fonctionnement des bus d'événements, consultez la section bus Amazon EventBridge d'événements.
- Pour plus d'informations sur la structure des événements, consultez la section Événements.
- Pour plus d'informations sur la création de modèles d'événements EventBridge à utiliser lors de la mise en correspondance d'événements avec des règles, voir Modèles d'événements.
- Pour plus d'informations sur la création de règles pour spécifier quels événements sont EventBridge traités, consultez la section Règles.
- Pour plus d'informations sur la manière de spécifier les services ou autres destinations auxquels les EventBridge événements correspondants sont envoyés, consultez la section Cibles.

Référence détaillée des événements du pare-feu DNS Route 53 Resolver

Tous les événements issus AWS des services ont un ensemble commun de champs contenant des métadonnées relatives à l'événement, telles que le AWS service à l'origine de l'événement, l'heure à laquelle l'événement a été généré, le compte et la région dans lesquels l'événement a eu lieu, etc. Pour les définitions de ces champs généraux, voir la référence relative à la structure des événements dans le guide de Amazon EventBridge l'utilisateur.

En outre, chaque événement possède un champ `detail` qui contient des données spécifiques à cet événement en particulier. La référence ci-dessous définit les champs détaillés des différents événements du pare-feu DNS.

Lorsque vous l'utilisez EventBridge pour sélectionner et gérer les événements du pare-feu DNS, il est utile de garder à l'esprit les points suivants :

- Le `source` champ pour tous les événements du pare-feu DNS est défini suraws.`route53resolver`.
- Le champ `detail-type` indique le type d'événement.

  Par exemple, `DNS Firewall Block` ou `DNS Firewall Alert`.
- Le champ `detail` contient les données spécifiques à cet événement en particulier.

Pour plus d'informations sur la création de modèles d'événements permettant aux règles de correspondre aux événements du pare-feu DNS, consultez la section Modèles d'événements dans le guide de Amazon EventBridge l'utilisateur.

Pour plus d'informations sur les événements et leur EventBridge traitement, reportez-vous à la section Amazon EventBridge Événements du Guide de Amazon EventBridge l'utilisateur.

Rubriques

- Détails de l'événement d'alerte du pare-feu DNS
- Détails de l'événement de blocage du pare-feu DNS

Détails de l'événement d'alerte du pare-feu DNS

Vous trouverez ci-dessous les champs détaillés des événements relatifs à l'état de l'alerte.

Les `detail-type` champs `source` et sont inclus car ils contiennent des valeurs spécifiques pour les événements de la Route 53.

```
{...,
 "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`

Identifie le type d'événement.

Pour cet événement, cette valeur est`DNS Firewall Alert`.

`source`

Identifie le service qui a généré l'événement. Pour les événements du pare-feu DNS, cette valeur est`aws.route53resolver`.

`detail`

Un objet JSON qui contient des informations sur l'événement. Le service qui génère l'événement détermine le contenu de ce champ.

Pour cet événement, ces données incluent :

`account-id`

L'ID du Compte AWS qui a créé le VPC.

`last-observed-at`

L'horodatage du moment où la Alert/Block requête a été effectuée dans le VPC.

`query-name`

Le nom de domaine (example.com) ou nom de sous-domaine (www.example.com) indiqué dans la requête.

`query-type`

Soit le type d'enregistrement DNS spécifié dans la demande, soit ANY. Pour en savoir plus sur les types pris en charge par Route 53, veuillez consulter Types d'enregistrements DNS pris en charge.

`query-class`

La classe de la requête.

`transport`

Le protocole utilisé pour soumettre la requête DNS.

`firewall-rule-action`

L'action indiquée par la règle qui correspond au nom de domaine de la requête. `ALERT` ou `BLOCK`.

`firewall-rule-group-id`

L'ID du groupe de règles de pare-feu DNS correspondant au nom de domaine de la requête. Pour plus d'informations sur les groupes de règles de pare-feu, consultez la section Pare-feu DNSRègles et groupes de règles de pare-feu DNS.

`firewall-domain-list-id`

La liste des domaines indiquée par la règle qui correspond au nom de domaine de la requête.

`firewall-protection`

Protection avancée du pare-feu DNS, soit DGA, soit DNS_TUNNELING. Pour plus d'informations, consultez la section Pare-feu DNSRoute 53 Resolver DNS Firewall Advanced.

`resourcese`

Contient les types de ressources et des informations supplémentaires les concernant.

`resource-type`

Spécifie le type de ressource, tel qu'un point de terminaison du résolveur ou une instance VPC.

`resource-type``-detail`

Informations supplémentaires sur la ressource.

Example Événement d'alerte du pare-feu DNS

Voici un exemple d'événement d'alerte.


```
{
 "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"
 }
}
```

Détails de l'événement de blocage du pare-feu DNS

Vous trouverez ci-dessous les champs de détail pour*`event name`*.

Les `detail-type` champs `source` et sont inclus car ils contiennent des valeurs spécifiques pour les événements de la Route 53.

```
{...,
 "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`

Identifie le type d'événement.

Pour cet événement, cette valeur estDNS `Firewall Alert`.

`source`

Identifie le service qui a généré l'événement. Pour les événements du pare-feu DNS, cette valeur est `aws.route53resolver`.

`detail`

Un objet JSON qui contient des informations sur l'événement. Le service qui génère l'événement détermine le contenu de ce champ.

Pour cet événement, ces données incluent :

`account-id`

L'ID du Compte AWS qui a créé le VPC.

`last-observed-at`

L'horodatage du moment où la Alert/Block requête a été effectuée dans le VPC.

`query-name`

Le nom de domaine (example.com) ou nom de sous-domaine (www.example.com) indiqué dans la requête.

`query-type`

Soit le type d'enregistrement DNS spécifié dans la demande, soit ANY. Pour en savoir plus sur les types pris en charge par Route 53, veuillez consulter Types d'enregistrements DNS pris en charge.

`query-class`

La classe de la requête.

`transport`

Le protocole utilisé pour soumettre la requête DNS.

`firewall-rule-action`

L'action indiquée par la règle qui correspond au nom de domaine de la requête. `ALERT` ou `BLOCK`.

`firewall-rule-group-id`

L'ID du groupe de règles de pare-feu DNS correspondant au nom de domaine de la requête. Pour plus d'informations sur les groupes de règles de pare-feu, consultez la section Pare-feu DNSRègles et groupes de règles de pare-feu DNS.

`firewall-domain-list-id`

La liste des domaines indiquée par la règle qui correspond au nom de domaine de la requête.

`firewall-protection`

Protection avancée du pare-feu DNS, soit DGA, soit DNS_TUNNELING. Pour plus d'informations, consultez la section Pare-feu DNSRoute 53 Resolver DNS Firewall Advanced.

`resourcese`

Contient les types de ressources et des informations supplémentaires les concernant.

`resource-type`

Spécifie le type de ressource, tel qu'un point de terminaison du résolveur ou une instance VPC.

`resource-type``-detail`

Informations supplémentaires sur la ressource.

Example Exemple d'évènement

Voici un exemple d'événement de blocage.

```
{
 "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"
 }
}
```

Journalisation des appels d'API Amazon Route 53 avec AWS CloudTrail

Route 53 est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans Route 53. CloudTrail capture tous les appels d'API pour Route 53 sous forme d'événements, y compris les appels provenant de la console Route 53 et les appels de code vers Route 53 APIs. Si vous créez un suivi, vous pouvez activer la diffusion continue d' CloudTrail événements vers un compartiment Amazon S3, y compris des événements pour Route 53. Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents dans la CloudTrail console dans Historique des événements. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite à Route 53, l'adresse IP à partir de laquelle la demande a été faite, qui a fait la demande, quand elle a été faite et des détails supplémentaires.

Rubriques

- Informations sur la Route 53 dans CloudTrail
- Affichage des événements Route 53 avec l'historique des événements
- Compréhension des entrées des fichiers journaux Route 53

Informations sur la Route 53 dans CloudTrail

CloudTrail est activé sur votre AWS compte lorsque vous le créez. Lorsqu'une activité se produit sur Route 53, cette activité est enregistrée dans un CloudTrail événement avec d'autres événements de AWS service dans l'historique des événements. Vous pouvez consulter, rechercher et télécharger les événements récents dans votre AWS compte. Pour plus d'informations, consultez la section Affichage des événements avec l'historique des CloudTrail événements.

Pour un enregistrement continu des événements de votre AWS compte, y compris les événements de la Route 53, créez un parcours. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un journal d'activité dans la console, il s'applique à toutes les régions. Le journal enregistre les événements de toutes les régions de la AWS partition et transmet les fichiers journaux au compartiment Amazon S3 que vous spécifiez. En outre, vous pouvez configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez :

- Présentation de la création d'un journal d'activité
- CloudTrail services et intégrations pris en charge
- Configuration des notifications Amazon SNS pour CloudTrail
- Réception de fichiers CloudTrail journaux de plusieurs régions et réception de fichiers CloudTrail journaux de plusieurs comptes

Toutes les actions Route 53 sont enregistrées CloudTrail et documentées dans le manuel Amazon Route 53 API Reference. Par exemple, les appels aux `CreateHostedZoneCreateHealthCheck`, et `RegisterDomain` les actions génèrent des entrées dans les fichiers CloudTrail journaux.

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer les éléments suivants :

- Si la demande a été effectuée avec des informations d'identification d'utilisateur root ou IAM.
- Si la demande a été effectuée avec des informations d'identification de sécurité temporaires pour un rôle ou un utilisateur fédéré.
- Si la demande a été faite par un autre AWS service.

Pour de plus amples informations, veuillez consulter l'élément userIdentity CloudTrail .

Affichage des événements Route 53 avec l'historique des événements

CloudTrail vous permet de consulter les événements récents dans l'historique des événements. Pour afficher les événements des requêtes d'API Route 53, vous devez choisir US East (N. Virginia) (USA Est [Virginie du Nord]) dans le sélecteur de région en haut de la console. Pour plus d'informations, consultez la section Affichage des événements avec l'historique des CloudTrail événements dans le Guide de AWS CloudTrail l'utilisateur.

Compréhension des entrées des fichiers journaux Route 53

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique.

L'élément `eventName` identifie l'action qui s'est produite. (Dans CloudTrail les journaux, la première lettre est en minuscule pour les actions d'enregistrement de domaine, même si elle est en majuscule dans le nom des actions. Par exemple, `UpdateDomainContact` apparaît comme `updateDomainContact` dans les journaux). CloudTrail prend en charge toutes les actions de l'API Route 53. L'exemple suivant montre une entrée de CloudTrail journal illustrant les actions suivantes :

- Répertorier les zones hébergées associées à un AWS compte
- Créer une surveillance d'état
- Créer deux registres
- Supprimer une zone hébergée
- Mettre à jour des informations pour un domaine enregistré
- Créer un point de terminaison Route 53 Resolver sortant

```
{
    "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"
        }
    ]
}
```

Dépannage d'Amazon Route 53

Cette page couvre les sujets de résolution des problèmes suivants pour Amazon Route 53 :

1. Indisponibilité du domaine :
   - Découvrez les raisons courantes pour lesquelles votre domaine n'est pas disponible sur Internet, telles que la non-confirmation de l'adresse e-mail du titulaire, les problèmes de transfert du service DNS, les paramètres de serveur de noms incorrects ou la suppression de zones hébergées.
2. Suspension du domaine :
   - Découvrez les causes de la suspension (ClientHold statut) d'un domaine et comment obtenir la suspension de votre domaine, notamment les domaines expirés, les modifications d'e-mail non vérifiées des titulaires de nom de domaine et les problèmes de traitement des paiements.
3. Échec du transfert de domaine :
   - Découvrez les raisons courantes d'un échec de transfert de domaine vers Route 53, telles que le fait de ne pas autoriser le transfert, des codes d'autorisation non valides ou des problèmes liés aux noms de domaine internationalisés.
4. Les paramètres DNS ne prennent pas effet :
   - Résolvez les situations dans lesquelles les modifications de vos paramètres DNS n'ont pas encore pris effet, notamment la mise en cache du résolveur DNS, les mises à jour incorrectes du serveur de noms et le fait que plusieurs zones hébergées portent le même nom.
5. Erreur « Serveur introuvable » :
   - Trouvez des solutions aux erreurs « Serveur introuvable » dans votre navigateur, telles que des enregistrements manquants, des valeurs d'enregistrement incorrectes ou des ressources indisponibles.
6. Acheminement du trafic vers des compartiments S3 :
   - Résolvez les problèmes lorsque vous essayez d'acheminer le trafic vers un compartiment Amazon S3 configuré pour l'hébergement de sites Web.
7. Problèmes de facturation :
   - Découvrez les scénarios de facturation courants, notamment le fait d'être facturé deux fois pour la même zone hébergée, les factures multiples pour des domaines et les problèmes liés à l'enregistrement de domaines en cas de fermeture ou de fermeture définitive de la vôtre Compte AWS .

Rubriques

- Mon domaine n'est pas disponible sur Internet
- Mon domaine est suspendu (le statut est ClientHold)
- Le transfert de mon domaine à Amazon Route 53 a échoué
- J'ai modifié les paramètres DNS, mais ils ne sont pas entrés en vigueur
- Mon navigateur affiche le message d'erreur « Server not found »
- Je ne peux pas acheminer le trafic vers un compartiment Amazon S3 qui est configuré pour l'hébergement de site web
- J'ai été facturé deux fois pour la même zone hébergée
- Plusieurs factures m'ont été facturées pour mon domaine
- Mon AWS compte est fermé ou définitivement, et mon domaine est enregistré auprès de Route 53

Mon domaine n'est pas disponible sur Internet

Voici les motifs les plus courants de l'indisponibilité d'un domaine sur Internet.

Rubriques

- Vous avez enregistré un nouveau domaine, mais vous n'avez pas cliqué sur le lien figurant dans l'e-mail de confirmation
- Vous avez transféré l'enregistrement de domaine à Amazon Route 53, mais vous n'avez pas transféré le service DNS
- Vous avez transféré l'enregistrement de domaine et spécifié des serveurs de noms incorrects dans les paramètres du domaine
- Vous avez transféré le service DNS en premier, mais vous n'avez pas attendu assez longtemps avant de transférer l'enregistrement de domaine
- Vous avez supprimé la zone hébergée que Route 53 utilise pour acheminer le trafic Internet pour le domaine.
- Votre domaine a été suspendu

Vous avez enregistré un nouveau domaine, mais vous n'avez pas cliqué sur le lien figurant dans l'e-mail de confirmation

Lorsque vous enregistrez un nouveau domaine, l'ICANN exige que nous obtenions une confirmation que l'adresse e-mail du contact inscrit actuel est valide. Afin d'obtenir la confirmation, nous envoyons un e-mail qui contient un lien. (Si vous ne répondez pas au premier e-mail, nous le renvoyons deux autres fois.) Vous devez cliquer sur le lien dans un délai de 3 à 15 jours, selon le domaine de premier niveau. Au-delà de ce délai, le lien ne fonctionne plus.

Si vous ne cliquez pas sur le lien figurant dans l'e-mail dans le temps imparti, l'ICANN exige la suspension du domaine. Pour plus d'informations sur les modalités de renvoi de l'e-mail de confirmation au contact inscrit, consultez Renvoi des e-mails de confirmation et d'autorisation.

Vous avez transféré l'enregistrement de domaine à Amazon Route 53, mais vous n'avez pas transféré le service DNS

Si votre bureau d'enregistrement précédent offrait un service DNS gratuit avec l'enregistrement de domaine, il a peut-être arrêté de fournir le service DNS lorsque vous avez transféré l'enregistrement de domaine à Route 53. Effectuez la procédure suivante pour déterminer si c'est bien le problème et, le cas échéant, pour le résoudre.

Pour restaurer le service DNS si votre bureau d'enregistrement précédent l'a annulé après le transfert de votre enregistrement de domaine à Route 53

1. Contactez votre bureau d'enregistrement précédent et vérifiez s'il a annulé le service DNS pour votre domaine. Si c'est le cas, voici les trois moyens les plus rapides de restaurer le service DNS pour le domaine, dans l'ordre de préférence :

   - Si le bureau d'enregistrement précédent propose un service DNS payant, demandez-lui de restaurer le service DNS en utilisant les anciens enregistrements DNS et serveurs de noms de votre domaine.
   - Si le bureau d'enregistrement précédent ne fournit pas de service DNS payant sans enregistrement de domaine, demandez si vous pouvez lui retransférer l'enregistrement de domaine afin qu'il restaure le service DNS en utilisant les anciens enregistrements DNS et serveurs de noms de votre domaine.
   - Si vous pouvez retransférer l'enregistrement de domaine à votre bureau d'enregistrement précédent, mais qu'il ne dispose plus de vos enregistrements DNS, demandez si vous pouvez lui retransférer votre enregistrement de domaine et obtenir le même ensemble de serveurs de

noms que ceux qui étaient anciennement affectés au domaine. Si c'est possible, vous devrez recréer vos anciens enregistrements DNS vous-même. Cependant, dès que vous l'aurez fait, votre domaine sera à nouveau disponible.

Si votre bureau d'enregistrement précédent ne peut vous aider pour aucune de ces options, passez à l'étape 2.

> **Important**
>
> Si vous ne pouvez pas restaurer le service DNS en utilisant les serveurs de noms que vous avez spécifiés lorsque vous avez transféré votre domaine à Route 53, il peut s'écouler jusqu'à deux jours après l'exécution des étapes restantes de cette procédure avant que votre domaine devienne à nouveau disponible sur Internet. Les résolveurs DNS mettent généralement en cache les noms des serveurs de noms d'un domaine pendant 24 à 48 heures, et ce délai s'écoulera donc avant que tous les résolveurs DNS obtiennent les noms des nouveaux serveurs de noms.

2. Sélectionnez un nouveau service DNS, par exemple, Route 53.
3. En utilisant la méthode fournie par le nouveau service DNS, créez une zone hébergée et des enregistrements :

   a. Créez une zone hébergée portant le même nom que votre domaine, par exemple, example.com.

   b. Utilisez le fichier de zone que vous avez obtenu du bureau d'enregistrement précédent pour créer des enregistrements.

   Si vous avez choisi Route 53 comme nouveau service DNS, vous pouvez créer les enregistrements en important le fichier de zone. Pour de plus amples informations, veuillez consulter Création d'enregistrements par importation d'un fichier de zone.
4. Obtenez les serveurs de noms pour la nouvelle zone hébergée. Si vous avez choisi Route 53 comme service DNS, consultez Obtention de la liste des serveurs de noms d'une zone hébergée publique.
5. Remplacez les serveurs de nom de votre domaine par les serveurs de noms que vous avez obtenus à l'étape 4. Pour de plus amples informations, veuillez consulter Ajout ou modification de serveurs de noms et d'enregistrements de type glue pour un domaine.

Vous avez transféré l'enregistrement de domaine et spécifié des serveurs de noms incorrects dans les paramètres du domaine

Lorsque vous transférez l'enregistrement de domaine à Amazon Route 53, l'un des paramètres que vous spécifiez pour le domaine est l'ensemble de serveurs de noms qui répondra aux requêtes DNS pour le domaine. Ces serveurs de noms proviennent de la zone hébergée qui porte le même nom que le domaine. La zone hébergée contient des informations sur la façon dont vous souhaitez acheminer le trafic du domaine, par exemple, l'adresse IP d'un serveur web pour www.example.com.

Vous avez peut-être accidentellement spécifié les serveurs de noms d'une zone hébergée incorrecte, ce qui peut facilement arriver si vous avez plusieurs zones hébergées portant le même nom que le domaine. Pour vérifier que le domaine utilise les serveurs de noms de la zone hébergée correcte et, si nécessaire, mettre à jour les serveurs de noms du domaine, effectuez les procédures suivantes.

> **Important**
>
> Si vous avez spécifié des enregistrements de serveurs de noms incorrects lorsque vous avez transféré le domaine à Route 53, il peut s'écouler jusqu'à deux jours après la correction des serveurs de noms du domaine avant que le service DNS soit entièrement restauré. En effet, les résolveurs DNS sur Internet ne demandent généralement les serveurs de noms qu'une seule fois tous les deux jours et mettent la réponse en cache.

Pour obtenir les serveurs de noms pour votre zone hébergée

1. Si vous utilisez un autre service DNS pour le domaine, utilisez la méthode fournie par le service DNS pour obtenir les serveurs de noms pour la zone hébergée. Passez ensuite à la procédure suivante.

   Si vous utilisez Route 53 comme service DNS pour le domaine, connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation, choisissez Hosted Zones (Zones hébergées).
3. Sur la page Hosted Zones (Zones hébergées), sélectionnez la case d'option (pas le nom) de la zone hébergée.

> **Important**
>
> Si vous avez plusieurs zones hébergées portant le même nom, assurez-vous que vous obtenez les serveurs de noms pour la zone hébergée appropriée.

4. Dans le volet droit, notez les quatre serveurs répertoriés dans Name Servers (Serveurs de noms).

Pour confirmer que le domaine utilise les serveurs de noms corrects

1. Si vous utilisez un autre service DNS pour le domaine, connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/

   Si vous utilisez Route 53, passez à l'étape suivante.
2. Dans le panneau de navigation, sélectionnez Registered Domains (Domaines enregistrés).
3. Choisissez le nom du domaine dont vous souhaitez modifier les paramètres.
4. Sélectionnez Add or Edit Name Servers (Ajouter ou modifier des serveurs de noms).
5. Comparez la liste des serveurs de noms que vous avez obtenus lors de la procédure précédente aux serveurs de noms répertoriés dans la boîte de dialogue Edit Name Servers for domain name (Modifier les serveurs de noms pour le nom de domaine).
6. Si les serveurs de noms répertoriés ne correspondent pas aux serveurs de noms que vous avez obtenus lors de la procédure précédente, modifiez les serveurs de noms dans la boîte de dialogue, puis sélectionnez Update (Mettre à jour).

Vous avez transféré le service DNS en premier, mais vous n'avez pas attendu assez longtemps avant de transférer l'enregistrement de domaine

Lorsque vous avez transféré le service DNS à Amazon Route 53 ou à un autre service DNS, vous avez mis à jour la configuration de votre domaine avec le bureau d'enregistrement de domaine afin d'utiliser les serveurs de noms du nouveau service DNS.

Les résolveurs DNS, qui répondent aux demandes de votre domaine, mettent généralement en cache les noms des serveurs de noms pendant 24 à 48 heures. Si vous modifiez le service DNS pour un domaine et remplacez les serveurs de noms d'un service DNS par les serveurs de noms d'un autre

service DNS, il peut s'écouler jusqu'à 48 heures avant que les résolveurs DNS commencent à utiliser les nouveaux serveurs de noms et, par conséquent, le nouveau service DNS.

Voici comment le transfert de votre service DNS suivi trop rapidement du transfert de votre domaine peut entraîner l'indisponibilité de votre domaine sur Internet :

1. Vous avez transféré le service DNS pour votre domaine.
2. Vous avez transféré votre domaine à Route 53 avant que les résolveurs DNS aient commencé à utiliser les serveurs de noms de votre nouveau service DNS.
3. Votre bureau d'enregistrement précédent a annulé le service DNS pour votre domaine dès que le domaine a été transféré à Route 53.
4. Les résolveurs DNS acheminent toujours les requêtes vers votre ancien service DNS, mais il n'existe plus aucun enregistrement qui indique comment acheminer le trafic.

A l'expiration de la mise en cache des serveurs de noms de l'ancien service DNS, DNS va commencer à utiliser votre nouveau service DNS. Malheureusement, il n'existe aucun moyen d'accélérer ce processus.

Vous avez supprimé la zone hébergée que Route 53 utilise pour acheminer le trafic Internet pour le domaine.

Si Route 53 est le service DNS pour votre domaine et si vous supprimez la zone hébergée qui est utilisée pour acheminer le trafic Internet pour le domaine, le domaine deviendra indisponible sur Internet. Ceci est vrai, que le domaine soit ou non enregistré chez Route 53.

> **Important**
>
> La restauration des services Internet pour le domaine peut prendre jusqu'à 48 heures.

Pour restaurer le service Internet si vous supprimez une zone hébergée que Route 53 utilise pour acheminer le trafic Internet pour un domaine

1. Créez une autre zone hébergée portant le même nom que le domaine. Pour de plus amples informations, veuillez consulter Création d'une zone hébergée publique.
2. Recréez les enregistrements qui étaient présents dans la zone hébergée que vous avez supprimée. Pour de plus amples informations, veuillez consulter Utilisation des enregistrements.

3. Obtenez les noms des serveurs de noms que Route 53 a assignés à la nouvelle zone hébergée. Pour de plus amples informations, veuillez consulter Obtention de la liste des serveurs de noms d'une zone hébergée publique.
4. Mettez à jour l'enregistrement de domaine pour utiliser les serveurs de noms obtenus à l'étape 3 :
   - Si le domaine est enregistré auprès de Route 53, consultez Ajout ou modification de serveurs de noms et d'enregistrements de type glue pour un domaine.
   - Si le domaine est enregistré auprès d'un autre bureau d'enregistrement, utilisez la méthode fournie par le bureau d'enregistrement pour mettre à jour l'enregistrement de domaine afin d'utiliser les nouveaux noms de serveurs.
5. Attendez que la durée de vie (TTL) des serveurs de noms s'écoule pour les résolveurs récursifs qui ont mis en cache les noms des serveurs de noms pour la zone hébergée supprimée. Une fois la durée de vie (TTL) écoulée, lorsqu'un navigateur ou une application envoie une requête DNS pour le domaine ou l'un de ses sous-domaines, un résolveur récursif transfère la requête aux serveurs de noms Route 53 pour la nouvelle zone hébergée. Pour de plus amples informations, veuillez consulter Comment Amazon Route 53 achemine le trafic de votre domaine.

   La durée de vie (TTL) pour les serveurs de noms peut atteindre 48 heures, selon le domaine de premier niveau du domaine.

Votre domaine a été suspendu

Votre domaine peut être indisponible sur Internet, car vous l'avez suspendu. Pour de plus amples informations, veuillez consulter Mon domaine est suspendu (le statut est ClientHold).

Mon domaine est suspendu (le statut est ClientHold)

Si Amazon Route 53 suspend votre domaine, celui-ci devient indisponible sur Internet. Vous pouvez utiliser l'une des méthodes suivantes pour déterminer si un domaine a été suspendu :

- Sur la page Registered domains (Domaines enregistrés) de la console Route 53, recherchez le nom de domaine dans le tableau Alerts (Alertes) située au bas de la page. Si la valeur de la colonne Status (État) est clientHold, le domaine a été suspendu.
- Envoyez une requête WHOIS pour le domaine. Si la valeur de la colonne Domain Status (État du domaine) est clientHold, le domaine a été suspendu. La commande WHOIS est disponible dans de

nombreux systèmes d'exploitation. Elle est également disponible en tant qu'application web sur de nombreux sites web.

De plus, lorsque nous suspendons un domaine, nous envoyons généralement un e-mail à l'adresse e-mail du contact inscrit pour ce domaine. Toutefois, si le domaine a été suspendu suite à une décision judiciaire, le tribunal peut ne pas nous laisser en informer le contact inscrit.

Pour rendre un domaine à nouveau disponible sur Internet, vous devez obtenir l'annulation de sa suspension. Voici les motifs justifiant la suspension d'un domaine et la manière dont vous pouvez annuler cette suspension.

> **Note**
>
> Si vous avez besoin d'aide pour annuler la suspension de votre domaine, vous pouvez contacter le AWS Support gratuitement. Pour de plus amples informations, veuillez consulter Contacter le AWS Support à propos de problèmes d'enregistrement de domaine.

Rubriques

- Vous avez enregistré un nouveau domaine, mais vous n'avez pas cliqué sur le lien figurant dans l'e-mail de confirmation
- Vous avez désactivé le renouvellement automatique du domaine et celui-ci a expiré
- Vous avez modifié l'adresse e-mail du contact inscrit, mais vous n'avez pas vérifié que la nouvelle adresse e-mail est valide
- Nous ne sommes pas parvenus à traiter votre paiement pour le renouvellement automatique du domaine qui a expiré
- Nous avons suspendu le domaine en raison d'une violation de la politique d'utilisation acceptable d'AWS
- Nous avons suspendu le domaine en raison d'une décision judiciaire

Vous avez enregistré un nouveau domaine, mais vous n'avez pas cliqué sur le lien figurant dans l'e-mail de confirmation

Lorsque vous enregistrez un domaine AWS pour la première fois, l'ICANN exige que nous obtenions la confirmation que l'adresse e-mail du contact du titulaire est valide. Afin d'obtenir la confirmation,

nous envoyons un e-mail qui contient un lien. Vous devez cliquer sur le lien dans un délai de 3 à 15 jours, selon le domaine de premier niveau. Au-delà de ce délai, le lien ne fonctionne plus.

> **Note**
>
> Si vous avez déjà enregistré un ou plusieurs domaines auprès d'Amazon Route 53 et utilisé la même adresse e-mail du contact inscrit, nous n'envoyons pas d'e-mail de confirmation.

Si vous ne cliquez pas sur le lien figurant dans l'e-mail dans le temps imparti, l'ICANN exige la suspension du domaine. Pour plus d'informations sur les modalités de renvoi de l'e-mail de confirmation au contact inscrit, consultez Renvoi des e-mails de confirmation et d'autorisation. Lorsque vous confirmez que l'adresse e-mail est valide, nous annulons immédiatement la suspension du domaine.

Vous avez désactivé le renouvellement automatique du domaine et celui-ci a expiré

Lorsque le renouvellement automatique d'un domaine est désactivé (valeur par défaut d'un domaine nouveau ou transféré), nous renouvelons automatiquement l'enregistrement du domaine peu de temps avant la date d'expiration. Si vous désactivez le renouvellement automatique, nous envoyons trois e-mails de rappel que l'enregistrement du domaine est sur le point d'expirer à l'adresse électronique du contact inscrit. Nous commençons à envoyer ces e-mails 45 jours avant l'expiration du domaine.

Si vous désactivez le renouvellement automatique du domaine et que vous ne prolongez pas manuellement la période d'enregistrement du domaine, nous suspendons généralement le domaine à la date d'expiration. Notez que les registres de certains domaines suppriment le domaine avant la date d'expiration.

Pour plus d'informations sur le renouvellement d'un domaine expiré, consultez Renouvellement d'un enregistrement de domaine.

Vous avez modifié l'adresse e-mail du contact inscrit, mais vous n'avez pas vérifié que la nouvelle adresse e-mail est valide

Si vous modifiez l'adresse e-mail du contact inscrit par une adresse que vous n'avez pas préalablement vérifiée, l'ICANN exige que nous obtenions une confirmation que l'adresse e-mail du

contact inscrit actuel est valide. Afin d'obtenir la confirmation, nous envoyons un e-mail qui contient un lien. Vous devez cliquer sur le lien dans un délai de 3 à 15 jours, selon le domaine de premier niveau. Au-delà de ce délai, le lien ne fonctionne plus.

Si vous ne cliquez pas sur le lien figurant dans l'e-mail dans le délai autorisé par le registre TLD, l'ICANN exige que nous suspendions le domaine. Pour plus d'informations sur les modalités de renvoi de l'e-mail de confirmation au contact inscrit, consultez Renvoi des e-mails de confirmation et d'autorisation. Lorsque vous confirmez que l'adresse e-mail est valide, nous annulons immédiatement la suspension du domaine.

Nous ne sommes pas parvenus à traiter votre paiement pour le renouvellement automatique du domaine qui a expiré

Si le renouvellement automatique est désactivé pour un domaine et que nous n'avons pas pu traiter le paiement (par exemple, en raison de l'expiration de votre carte de crédit), nous envoyons plusieurs e-mails à l'adresse électronique du contact inscrit concernant le domaine. Si nous ne recevons pas le paiement, nous suspendons généralement le domaine à la date d'expiration. Notez que les registres de certains domaines suppriment le domaine avant la date d'expiration.

Pour plus d'informations sur le renouvellement d'un domaine expiré, consultez Renouvellement d'un enregistrement de domaine.

Nous avons suspendu le domaine en raison d'une violation de la politique d'utilisation acceptable d' AWS

Si nous suspendons un domaine pour une violation de la AWS politique d'utilisation acceptable d', nous envoyons un e-mail de notification au contact inscrit pour ce domaine. (Nous n'envoyons pas d'e-mail de notification si le AWS compte est déjà suspendu pour fraude.)

Pour contester une suspension, envoyez un e-mail à trustandsafety@support.aws.com.

Nous avons suspendu le domaine en raison d'une décision judiciaire

Si un domaine a été suspendu en raison d'une décision judiciaire, nous ne pouvons pas annuler la suspension tant que la décision judiciaire n'a pas été levée. Pour contester la validité d'une décision de justice, envoyez un e-mail à trustandsafety@support.aws.com et joignez les documents applicables.

Le transfert de mon domaine à Amazon Route 53 a échoué

Voici des raisons courantes de l'échec du transfert d'un domaine vers Amazon Route 53.

Rubriques

- Vous n'avez pas cliqué sur le lien figurant dans l'e-mail d'autorisation
- Le code d'autorisation que vous avez obtenu à partir du bureau d'enregistrement n'est pas valide
- Erreur « Parameters in request are not valid » (Les paramètres de la demande ne sont pas valides) lors de la tentative de transfert d'un domaine .es vers Amazon Route 53
- Le nom de domaine internationalisé que vous transférez vers Amazon Route 53 est-il répertorié dans punycode ?

Vous n'avez pas cliqué sur le lien figurant dans l'e-mail d'autorisation

Lorsque vous transférez un enregistrement de domaine vers Amazon Route 53, l'ICANN, l'organisme de réglementation pour l'enregistrement de domaine, exige l'autorisation de transfert de la part du contact inscrit pour le domaine. Afin d'obtenir l'autorisation, nous vous envoyons un e-mail qui contient un lien. Vous devez cliquer sur le lien dans un délai de 5 à 15 jours, selon le domaine de premier niveau. Au-delà de ce délai, le lien ne fonctionne plus.

Si vous ne cliquez pas sur le lien figurant dans l'e-mail dans le temps imparti, l'ICANN exige l'annulation du transfert. Pour plus d'informations sur les modalités de renvoi de l'e-mail d'autorisation au contact inscrit, consultez Renvoi des e-mails de confirmation et d'autorisation.

Le code d'autorisation que vous avez obtenu à partir du bureau d'enregistrement n'est pas valide

Si vous demandez le transfert d'un domaine vers Amazon Route 53 et que vous ne recevez pas l'e-mail d'autorisation, consultez la page d'état dans la console Route 53. Si la page de statut indique que le code d'autorisation de transfert que vous avez obtenu de votre bureau d'enregistrement n'est pas valide, procédez comme suit :

1. Contactez le bureau d'enregistrement actuel pour le domaine et demandez un nouveau code d'autorisation. Assurez-vous des points suivants :
    - Durée de validité du nouveau code d'autorisation. Vous devez demander un transfert de domaine avant l'expiration du code.

- Le nouveau code d'autorisation est différent du code non valide. Si ce n'est pas le cas, demandez au bureau d'enregistrement actuel d'actualiser le code d'autorisation.

2. Envoyez une autre demande de transfert du domaine. Pour plus d'informations, consultez Étape 5 : Demander le transfert dans la rubrique Transfert d'un enregistrement de domaine vers Amazon Route 53.

Erreur « Parameters in request are not valid » (Les paramètres de la demande ne sont pas valides) lors de la tentative de transfert d'un domaine .es vers Amazon Route 53

Amazon Route 53 renvoie une erreur « Parameters in request are not valid » lorsque vous essayez de transférer un domaine .es vers Route 53 et que le type de contact du contact inscrit est Company (Société). Pour effectuer le transfert, modifiez le type de contact du titulaire en Person (Personne), et soumettez à nouveau.

Le nom de domaine internationalisé que vous transférez vers Amazon Route 53 est-il répertorié dans punycode ?

Lorsque vous enregistrez un nouveau nom de domaine ou créez des zones hébergées et des registres, vous pouvez spécifier des lettres autres que celles de a à z (par exemple, le ç en français), des caractères d'autres alphabets (par exemple, cyrillique ou arabe) et des caractères chinois, japonais ou coréens. Amazon Route 53 stocke ces noms de domaine internationalisés (IDNs) en Punycode, qui représente les caractères Unicode sous forme de chaînes ASCII.

Si vous obtenez une erreur lors du transfert d'un IDNs vers Route 53, utilisez un punycode pour le représenter et réessayez. Pour de plus amples informations, veuillez consulter Mise en forme des noms de domaine internationalisés.

J'ai modifié les paramètres DNS, mais ils ne sont pas entrés en vigueur

Si vous avez modifié les paramètres DNS, voici quelques motifs courants pour lesquels les modifications ne sont pas encore entrées en vigueur.

Rubriques

- Vous avez transféré le service DNS à Amazon Route 53 au cours des dernières 48 heures, par conséquent, DNS utilise encore votre service DNS précédent
- Vous avez récemment transféré le service DNS à Amazon Route 53, mais vous n'avez pas mis à jour les serveurs de noms avec le serveur d'inscriptions (registrar) de domaine
- Les résolveurs DNS utilisent toujours les anciens paramètres pour l'enregistrement
- Vous avez plusieurs zones hébergées portant le même nom et vous avez mis à jour celle qui n'est pas associée au domaine

Vous avez transféré le service DNS à Amazon Route 53 au cours des dernières 48 heures, par conséquent, DNS utilise encore votre service DNS précédent

Lorsque vous avez transféré le service DNS à Amazon Route 53, vous avez utilisé la méthode fournie par le serveur d'inscriptions de votre domaine pour remplacer les serveurs de noms du service DNS précédent par les quatre serveurs de noms de Route 53.

> **Note**
>
> Si vous n'êtes pas sûr d'avoir effectué cette opération, consultez Vous avez récemment transféré le service DNS à Amazon Route 53, mais vous n'avez pas mis à jour les serveurs de noms avec le serveur d'inscriptions (registrar) de domaine.

Les bureaux d'enregistrement utilisent généralement une TTL (durée de vie) de 24 à 48 heures pour les serveurs de noms. Cela signifie que lorsqu'un résolveur DNS obtient les serveurs de noms de votre domaine, il utilise ces informations pendant jusqu'à 48 heures avant d'envoyer une autre requête pour obtenir les serveurs de noms actuels pour le domaine. Si vous avez transféré le service DNS à Route 53 au cours des dernières 48 heures, puis modifié les paramètres DNS, certains résolveurs DNS utilisent toujours votre ancien service DNS pour acheminer le trafic pour le domaine.

Vous avez récemment transféré le service DNS à Amazon Route 53, mais vous n'avez pas mis à jour les serveurs de noms avec le serveur d'inscriptions (registrar) de domaine

Le bureau d'enregistrement de votre domaine dispose d'une grande variété d'informations sur le domaine, notamment les serveurs de noms pour le service DNS du domaine. Généralement, le

bureau d'enregistrement de domaine est également votre service DNS, si bien que les serveurs de noms qui sont associés à votre domaine appartiennent au bureau d'enregistrement. Ces serveurs de noms indiquent à DNS où obtenir les informations sur la façon dont vous souhaitez que le trafic de votre domaine soit acheminé, par exemple, à l'adresse IP d'un serveur web de votre domaine.

Lorsque vous transférez le service DNS à Amazon Route 53, vous devez utiliser la méthode qui est fournie par votre serveur d'inscriptions de domaine pour modifier les serveurs de noms qui sont associés à votre domaine. Vous remplacez généralement les serveurs de noms qui sont fournis par le bureau d'enregistrement par les quatre serveurs de noms Route 53 qui sont associés à la zone hébergée que vous avez créée pour le domaine.

Si vous avez créé une zone hébergée et des enregistrements pour votre domaine et spécifié des paramètres différents de ceux que vous avez utilisés pour le service DNS précédent, et si DNS achemine toujours le trafic vers les anciennes ressources, il est possible que vous n'ayez pas mis à jour les serveurs de noms avec le bureau d'enregistrement de domaine. Pour déterminer si le bureau d'enregistrement utilise les serveurs de noms pour votre zone hébergée Route 53 et, si nécessaire, pour mettre à jour les serveurs de noms pour le domaine, procédez comme suit :

Pour obtenir les serveurs de noms pour votre zone hébergée et mettre à jour les paramètres de serveur de noms avec le bureau d'enregistrement de domaine

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le panneau de navigation, choisissez Hosted Zones (Zones hébergées).
3. Sur la page Hosted Zone (Zones hébergées), sélectionnez le nom de la zone hébergée (pas le bouton de radio).

   > **Important**
   >
   > Si vous avez plusieurs zones hébergées portant le même nom, assurez-vous que vous obtenez les serveurs de noms pour la zone hébergée appropriée.

4. Dans la liste Record name (Nom de l'enregistrement), notez les quatre serveurs répertoriés dans Name Servers (Serveurs de noms).
5. A l'aide de la méthode fournie par le bureau d'enregistrement du domaine, affichez la liste des serveurs de noms du domaine.
6. Si les serveurs de noms du domaine correspondent aux serveurs de noms que vous avez obtenus à l'étape 4, la configuration de domaine est correcte.

Si les serveurs de noms du domaine ne correspondent pas aux serveurs de noms que vous avez obtenus à l'étape 4, mettez à jour le domaine pour utiliser les serveurs de noms Route 53.

7.

> **Important**
>
> Lorsque vous remplacez les serveurs de noms du domaine par les serveurs de noms de votre zone hébergée Route 53, il peut s'écouler jusqu'à deux jours avant que la modification prenne effet et que Route 53 devienne votre service DNS. En effet, les résolveurs DNS sur Internet ne demandent généralement les serveurs de noms qu'une seule fois tous les deux jours et mettent la réponse en cache.

Les résolveurs DNS utilisent toujours les anciens paramètres pour l'enregistrement

Si vous avez modifié les paramètres d'un enregistrement, mais que votre trafic est toujours acheminé vers l'ancienne ressource, par exemple, un serveur web de votre site web, une cause possible est que DNS conserve les paramètres précédents en cache. Chaque enregistrement a une valeur TTL (durée de vie) qui spécifie la durée, en secondes, pendant laquelle les résolveurs DNS doivent mettre en cache les informations contenues dans l'enregistrement, telles que l'adresse IP d'un serveur web. Jusqu'à ce que la durée spécifiée par la valeur TTL soit écoulée, les résolveurs DNS continueront à renvoyer l'ancienne valeur en réponse aux requêtes DNS. Si vous souhaitez connaître la valeur TTL d'un enregistrement, effectuez la procédure suivante.

> **Note**
>
> Pour les enregistrements d'alias, le TTL est déterminé par la AWS ressource vers laquelle l'enregistrement achemine le trafic. Pour de plus amples informations, veuillez consulter Choix entre des enregistrements avec ou sans alias.

Pour afficher la valeur TTL d'un enregistrement

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.

2. Sur la page Hosted Zones (Zones hébergées), choisissez le nom de la zone hébergée qui comprend l'enregistrement.
3. Dans la liste des enregistrements, recherchez l'enregistrement dont vous souhaitez connaître la valeur TTL et consultez la valeur de la colonne TTL.

> **Note**
>
> Si vous modifiez la valeur TTL maintenant, votre modification ne prendra pas effet plus rapidement. Les résolveurs DNS ont déjà la valeur mise en cache et il n'obtiendront le nouveau paramètre qu'une fois que la durée spécifiée par l'ancien paramètre sera écoulée.

Vous avez plusieurs zones hébergées portant le même nom et vous avez mis à jour celle qui n'est pas associée au domaine

Vous pouvez créer plusieurs zones hébergées portant le même nom, soit en utilisant le même compte, soit en utilisant plusieurs comptes. Pour spécifier la zone hébergée utilisée par Route 53 pour acheminer le trafic Internet pour votre domaine, vous obtenez les quatre serveurs de noms Route 53 pour cette zone hébergée et vous mettez à jour l'enregistrement de domaine pour utiliser ces serveurs de noms.

Si vous ajoutez, modifiez ou supprimez des enregistrements dans une zone hébergée mais que votre enregistrement de domaine utilise les serveurs de noms d'une autre zone hébergée, les réponses Route 53 aux requêtes DNS ne reflètent pas vos modifications. Pour déterminer si votre enregistrement de domaine utilise les serveurs de noms pour la zone hébergée dans laquelle vous avez mis à jour les enregistrements, effectuez les tâches suivantes :

1. Déterminez les serveurs de noms associés à l'enregistrement de votre domaine. Consultez Ajout ou modification de serveurs de noms ou d'enregistrements de type glue.
2. Comparez les serveurs de noms que vous avez obtenus à l'étape 1 avec les serveurs de noms affectés par Route 53 à la zone hébergée dans laquelle vous avez mis à jour les enregistrements. Consultez Obtention de la liste des serveurs de noms d'une zone hébergée publique.

Si les serveurs de noms pour l'enregistrement de domaine ne correspondent pas aux serveurs de noms de la zone hébergée dans laquelle vous avez mis à jour les enregistrements, vous avez deux options :

Modifier les enregistrements dans la zone hébergée qui est actuellement associée au domaine (recommandé)

Noter les modifications que vous avez apportées dans la zone hébergée qui n'est pas actuellement associée à votre enregistrement de domaine. Ensuite, allez dans la zone hébergée associée à l'enregistrement de domaine, et apportez les mêmes modifications. Cette méthode doit être privilégiée car les changements prennent effet presque immédiatement. Pour de plus amples informations, veuillez consulter Modification des enregistrements.

Mettre à jour votre enregistrement de domaine pour utiliser différents serveurs de noms

Modifiez l'enregistrement de votre domaine pour utiliser les serveurs de noms dans la zone hébergée que vous avez mise à jour.

> **Important**
>
> Si vous modifiez les serveurs de noms associés à votre enregistrement de domaine, votre domaine sera indisponible sur Internet pendant 2 jours maximum. En effet, les résolveurs DNS mettent généralement en cache les noms des serveurs de noms pendant 2 jours. Pour obtenir une vue d'ensemble du mode de fonctionnement du DNS, y compris des informations sur la mise en cache du résolveur, veuillez consulter Comment Amazon Route 53 achemine le trafic de votre domaine.

En modifiant les serveurs de noms associés à votre enregistrement de domaine, vous modifiez essentiellement le service DNS pour le domaine. Vous avez deux options, selon que le domaine est actuellement utilisé :

- Si le domaine est utilisé, veuillez consulter Configuration de Route 53 en tant que service DNS pour un domaine en cours d'utilisation.
- Si le domaine est actuellement inactif, effectuez les tâches suivantes :
  1. Obtenez les serveurs de noms de la zone hébergée que vous souhaitez utiliser pour acheminer le trafic vers votre domaine. Consultez Obtention de la liste des serveurs de noms d'une zone hébergée publique.
  2. Dans la zone hébergée pour laquelle vous avez obtenu les serveurs de noms à l'étape 1, vérifiez que l'enregistrement NS utilise les 4 mêmes serveurs de noms. Si ce n'est pas le cas, mettez à jour l'enregistrement NS. Consultez Modification des enregistrements.

3. Mettez à jour l'enregistrement de domaine pour utiliser les serveurs de noms obtenus à l'étape 1. Consultez Ajout ou modification de serveurs de noms ou d'enregistrements de type glue.

Mon navigateur affiche le message d'erreur « Server not found »

Si votre navigateur affiche le message d'erreur « Server not found » lorsque vous essayez d'accéder à un domaine (example.com) ou à un sous-domaine (www.example.com), voici quelques explications courantes.

Rubriques

- Vous n'avez pas créé d'enregistrement pour le nom de domaine ou de sous-domaine
- Vous avez créé un enregistrement mais vous avez spécifié une valeur incorrecte
- La ressource vers laquelle vous acheminez le trafic n'est pas disponible

Vous n'avez pas créé d'enregistrement pour le nom de domaine ou de sous-domaine

Si vous ne créez pas d'enregistrement pour le domaine ou le sous-domaine, DNS ne sait pas où acheminer le trafic lorsque quelqu'un saisit ce nom dans un navigateur. Pour de plus amples informations, veuillez consulter Utilisation des enregistrements.

Vous avez créé un enregistrement mais vous avez spécifié une valeur incorrecte

Lorsque vous créez un enregistrement, il est facile de spécifier une valeur incorrecte, telle que l'adresse IP d'un serveur Web ou le nom de domaine CloudFront attribué à votre distribution Web. Si l'enregistrement existe mais que vous obtenez toujours un message d'erreur « Server not found », nous vous recommandons de vérifier que la valeur est correcte.

La ressource vers laquelle vous acheminez le trafic n'est pas disponible

Si un enregistrement spécifie une ressource telle qu'un serveur web qui n'est pas disponible, un navigateur renvoie l'erreur « Server not found ». Nous vous recommandons de vérifier l'état de la ressource vers laquelle vous acheminez le trafic.

Je ne peux pas acheminer le trafic vers un compartiment Amazon S3 qui est configuré pour l'hébergement de site web

Lorsque vous configurez un compartiment Amazon S3 pour l'hébergement de site web, vous devez donner à ce compartiment un nom identique à celui de l'enregistrement que vous souhaitez utiliser pour acheminer le trafic vers le compartiment. Par exemple, si vous souhaitez acheminer le trafic d'example.com vers un compartiment S3 qui est configuré pour l'hébergement de site web, le nom du compartiment doit être example.com.

Si vous souhaitez acheminer le trafic vers un compartiment S3 configuré pour l'hébergement de sites Web mais que le nom du compartiment n'apparaît pas dans la liste des cibles d'alias de la console Amazon Route 53, ou si vous essayez de créer un enregistrement d'alias par programmation et que vous recevez une InvalidInput erreur de l'API Route 53, l'un des AWS SDKs, ou AWS CLI AWS Tools for Windows PowerShell, vérifiez les points suivants :

- Le nom du compartiment correspond exactement au nom de l'enregistrement, par exemple, example.com ou www.example.com.
- Le compartiment S3 est correctement configuré pour l'hébergement de site web. Pour de plus amples informations, veuillez consulter la section Hébergement d'un site web statique sur Amazon S3 dans le Guide de l'utilisateur Amazon Simple Storage Service.

J'ai été facturé deux fois pour la même zone hébergée

Nous ne vous facturons pas si vous supprimez une zone hébergée au cours de 12 hours suivant sa création. Une fois ce délai passé, nous facturons immédiatement un coût mensuel standard pour la zone hébergée. Le coût mensuel d'une zone hébergée n'est pas calculé au prorata des mois partiels. (Le même coût s'applique à la zone hébergée que nous créons automatiquement lorsque vous enregistrez un domaine.)

Si vous créez une zone hébergée le dernier jour du mois (par exemple, le 31 janvier), le coût du mois de janvier peut apparaître sur la facture de février, ainsi que le coût de février. Notez qu'Amazon Route 53 utilise l'heure UTC (temps universel coordonné) comme fuseau horaire pour déterminer à quel moment une zone hébergée a été créée.

Plusieurs factures m'ont été facturées pour mon domaine

Lorsque vous souscrivez à un abonnement, que vous payez des frais d'inscription, des frais de transfert ou des frais de renouvellement avec un coût initial, une facture unique est générée. Cette facture reste sur la console de facturation, même si la transaction de paiement échoue. L'élément de ligne de facturation correspondant est indiqué sous la forme [x] Quantité dans la sous-section Registrar-Global de l'onglet Détails de la facture par service de la console de facturation.

Pour consulter les factures annulées, procédez comme suit :

Pour consulter les factures annulées sur la console de facturation

1. Connectez-vous à la AWS Billing and Cost Management console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/costmanagement/.
2. Dans le volet de navigation, choisissez Factures.
3. Choisissez Factures pour voir les détails des factures annulées.

Pour consulter les paiements et remboursements réussis sur la console de facturation, procédez comme suit :

Pour confirmer les paiements ou les remboursements qui ont été traités avec succès

1. Dans le panneau de navigation, choisissez Payments (Paiements).
2. Choisissez l'onglet Transactions pour afficher le tableau des transactions pour toutes les transactions effectuées avec AWS.

Mon AWS compte est fermé ou définitivement, et mon domaine est enregistré auprès de Route 53

Si vous fermez votre AWS compte, ou si votre compte est fermé ou définitivement, vos domaines seront soumis à un processus de suppression :

1. Nous vous informerons que votre compte est fermé et que votre domaine sera suspendu quotidiennement dans les 5 prochains jours.
2. Une fois votre domaine suspendu, les événements suivants se produiront :

- Si votre bureau d'enregistrement est Amazon Registrar, nous vous informerons que nous supprimerons votre domaine dans les 30 jours. Pour de plus amples informations, veuillez consulter Trouver votre bureau d'enregistrement et d'autres informations concernant votre domaine.
- Si votre bureau d'enregistrement est Gandi, nous vous informerons que nous céderons votre domaine à Gandi lorsque votre compte sera définitivement fermé.

3. Après 30 jours d'attente, nous supprimerons tous les domaines enregistrés auprès d'Amazon Registrar dans le compte et nous vous enverrons une mise à jour.
4. Lorsque votre compte sera définitivement fermé, nous transférerons à Gandi tous les domaines enregistrés auprès de Gandi dans le compte.

Si vous rouvrez votre compte pendant la période pendant laquelle vos domaines peuvent être récupérés, nous annulerons la suspension de vos domaines ou vous informerons que vos domaines ont été supprimés mais qu'ils pourront peut-être être restaurés. Pour de plus amples informations, veuillez consulter Domaines que vous pouvez enregistrer avec Amazon Route 53.

> **Note**
>
> Une fois que 90 jours se sont écoulés depuis la fermeture de votre compte, vous ne pouvez plus le rouvrir. Pour plus d'informations, consultez la section Fermeture d'un compte dans le guide de gestion des AWS comptes.

Pour de plus amples informations, veuillez consulter Contacter le AWS Support à propos de problèmes d'enregistrement de domaine.

Plages d'adresses IP de serveurs Amazon Route 53

Amazon Web Services (AWS) publie ses plages d'adresses IP actuelles au format JSON. Si votre pare-feu ou des groupes de sécurité limitent le trafic entrant en fonction des adresses IP source, vérifiez que votre configuration permet le trafic de la nouvelle plage d'adresses IP applicable.

Pour afficher les plages d'adresses IP actuelles pour Route 53, téléchargez ip-ranges.json et recherchez les valeurs suivantes dans le fichier :

- `"service": "ROUTE53"`
- `"service": "ROUTE53_HEALTHCHECKS"`
- `"service": "ROUTE53_HEALTHCHECKS_PUBLISHING"`

Pour plus d'informations sur les adresses IP des AWS ressources, consultez la section Plages d'adresses AWS IP dans le Référence générale d'Amazon Web Services.

Plages d'adresses IP de serveurs de noms Route 53

`"service": "ROUTE53"` : ces plages d'adresses IP sont utilisées par les serveurs de noms Route 53. Ajoutez ces plages à la liste des plages d'adresses IP autorisées si vous employez Route 53 comme service DNS pour un ou plusieurs domaines et que vous souhaitez pouvoir utiliser les commandes `dig` ou `nslookup` pour interroger des serveurs de noms Route 53.

> **Note**
>
> La modification des adresses IP de serveurs de noms est rare. Si nous avons besoin de modifier des adresses IP, vous serez averti à l'avance.

Plages d'adresses IP utilisées par les surveillances de l'état de Route 53

`"service": "ROUTE53_HEALTHCHECKS"` : ces plages d'adresses IP sont utilisées par les outils de surveillance de l'état de Route 53. Ajoutez ces plages à la liste des plages d'adresses IP autorisées si vous utilisez la fonctionnalité de surveillance de l'état Route 53 pour vérifier l'intégrité des ressources de votre réseau.

> **Note**
>
> Nous modifions rarement les plages d'adresses IP des contrôleurs de santé ; si nous devons modifier les plages d'adresses IP, nous vous en informerons à l'avance.

Pour plus d'informations sur les adresses IP pour les surveillances de l'état, consultez Configuration des règles de pare-feu et de routeur pour les surveillances de l'état Amazon Route 53.

Référencement de listes de préfixes

Une liste de préfixes est un ensemble d'une ou de plusieurs entrées de bloc CIDR que vous pouvez utiliser pour configurer des groupes de sécurité. Votre routeur et votre pare-feu pour les règles de l' EC2instance Amazon doivent autoriser le trafic entrant provenant des adresses IP utilisées par les vérificateurs de santé de Route 53. Une référence à une liste de préfixes vous permet de simplifier la gestion des blocs d'adresse CIDR dans vos règles. Si vous utilisez fréquemment le même code pour CIDRs plusieurs règles, vous pouvez les gérer CIDRs dans une seule liste de préfixes, au lieu de les référencer à plusieurs reprises CIDRs dans chaque règle. Si vous devez supprimer un bloc d'adresse CIDR, vous pouvez supprimer son entrée de la liste des préfixes au lieu de supprimer le CIDR de chaque règle concernée. Pour de plus amples informations sur les listes de préfixes en général, consultez Grouper des blocs d'adresse CIDR à l'aide de listes de préfixes gérées dans le Guide de l'utilisateur Amazon VPC.

AWS-les listes de préfixes gérées sont des ensembles de plages d'adresses IP pour les AWS services. AWS-les listes de préfixes gérées sont créées et maintenues par AWS et peuvent être utilisées par toute personne possédant un AWS compte. Vous ne pouvez pas créer, modifier, partager ou supprimer une liste de AWS préfixes gérée.

Pour plus d'informations sur les listes de AWS préfixes gérées par -managées, consultez la section Travailler avec des listes de AWS préfixes -gérées dans le guide de l'utilisateur Amazon VPC.

Plages d'adresses IP internes utilisées par les surveillances de l'état de Route 53

`"service": "ROUTE53_HEALTHCHECKS_PUBLISHING"` : Route 53 utilise ces plages d'adresses IP uniquement en interne. Vous n'avez pas besoin d'ajouter ces plages à la liste des plages autorisées.

Balisage des ressources Amazon Route 53

Une étiquette est une étiquette que vous attribuez à une AWS ressource. Chaque balise est constituée d'une clé et d'une valeur que vous définissez toutes deux. Par exemple, vous pouvez choisir la clé « domaine » et la valeur « exemple.com ». Vous pouvez utiliser les balises pour atteindre plusieurs objectifs. Elles sont couramment utilisées pour classer vos coûts Amazon Route 53 par catégorie et en effectuer le suivi. Lorsque vous appliquez des balises aux zones hébergées par Route 53, aux domaines et aux bilans de santé, vous AWS générez un rapport de répartition des coûts sous forme de fichier CSV (valeurs séparées par des virgules) avec votre utilisation et vos coûts agrégés par vos balises. Vous pouvez appliquer des balises associées à des catégories métier (telles que les centres de coûts, les noms d'applications ou les propriétaires) pour organiser les coûts relatifs à divers services. Pour en savoir plus sur l'utilisation des identifications pour la répartition des coûts, consultez Utilisation des identifications de répartition des coûts dans le Guide de l'utilisateur AWS Billing.

Pour faciliter l'utilisation et obtenir de meilleurs résultats, utilisez l'éditeur de balises dans le AWS Management Console, qui fournit un moyen centralisé et unifié de créer et de gérer vos balises. Pour de plus amples informations, veuillez consulter Utilisation de Tag Editor dans le Guide de démarrage de la AWS Management Console. Vous pouvez également utiliser la console Route 53 pour appliquer des balises pour certaines ressources :

- Surveillances de l'état : pour plus d'informations, consultez Attribution de noms et balisage des surveillances de l'état.
- Points de terminaison entrants du Route 53 Resolver : pour plus d'informations, consultez Valeurs à spécifier lors de la création ou de la modification de points de terminaison entrants.
- Points de terminaison sortants Resolver : pour plus d'informations, consultez Valeurs à spécifier lors de la création ou de la modification de points de terminaison sortants.
- Règles Resolver : pour plus d'informations, consultez Valeurs à spécifier lors de la création ou de la modification de règles.
- Zones hébergées – Pour plus d'informations, consultez Utilisation de zones hébergées.

> **Note**
>
> Les frais pour les points de terminaison du résolveur sont alloués par interface réseau du résolveur. Comme il n'est actuellement pas possible de baliser les interfaces réseau du

résolveur, la répartition des coûts basée sur les balises n'est actuellement pas prise en charge pour les points de terminaison du résolveur. Pour plus d'informations sur la tarification pour Resolver, consultez Tarification Amazon Route 53.

Vous pouvez également appliquer des balises aux ressources à l'aide de l'API Route 53. Pour plus d'informations, consultez les actions liées aux balises dans la rubrique Actions d'API Route 53 par fonction dans le document Référence d'API Amazon Route 53.

Didacticiels

Cette section couvre les didacticiels suivants :

Utilisation de Route 53 comme service DNS pour les sous-domaines

Découvrez comment utiliser Route 53 comme service DNS pour un sous-domaine nouveau ou existant tout en utilisant un autre service DNS pour le domaine parent.

Transition vers le routage basé sur la latence

Découvrez comment passer progressivement du routage standard au routage basé sur la latence dans Route 53, en dirigeant les utilisateurs vers le point de terminaison le plus faible AWS disponible.

Combinez les enregistrements pondérés et les enregistrements de latence pour une transition fluide et peu risquée avec un contrôle total et une capacité de restauration.

Ajouter une autre région au routage basé sur la latence

Élargissez votre configuration de routage basée sur la latence en ajoutant une nouvelle AWS région et en transférant progressivement le trafic vers la nouvelle région.

Acheminement du trafic vers plusieurs EC2 instances Amazon dans une région

Utilisez une combinaison de latence et d'enregistrements pondérés pour acheminer le trafic vers plusieurs EC2 instances Amazon au sein d'une instance spécifique Région AWS.

Gestion de plus de 100 enregistrements pondérés

Découvrez comment diriger le trafic vers plus de 100 points de terminaison en créant une arborescence d'enregistrements d'alias pondérés et d'enregistrements pondérés.

Pondération des réponses à plusieurs enregistrements tolérantes aux pannes

Découvrez comment pondérer les réponses DNS contenant plusieurs enregistrements, en garantissant la tolérance aux pannes et en équilibrant la charge sur plusieurs points de terminaison.

Ces didacticiels couvrent différents cas d'utilisation et scénarios et vous aident à tirer parti efficacement des politiques de routage, des enregistrements pondérés et du routage basé sur la latence de Route 53 afin d'optimiser la gestion de votre DNS et le routage du trafic.

Rubriques

- Utilisation d'Amazon Route 53 comme service DNS pour des sous-domaines sans migration du domaine parent
- Transition vers le routage basé sur la latence dans Amazon Route 53
- Ajout d'une autre région à votre routage basé sur la latence dans Amazon Route 53
- Utilisation de la latence et des enregistrements pondérés dans Amazon Route 53 pour acheminer le trafic vers plusieurs EC2 instances Amazon dans une région
- Gestion de plus de 100 enregistrements pondérés dans Amazon Route 53
- Pondération des réponses pour la tolérance aux pannes pour plusieurs enregistrements dans Amazon Route 53

Utilisation d'Amazon Route 53 comme service DNS pour des sous-domaines sans migration du domaine parent

Amazon Route 53 offre de la flexibilité dans la gestion du DNS pour les sous-domaines, ce qui vous permet de tirer parti de ses fonctionnalités sans avoir à migrer l'intégralité du domaine parent.

Vous pouvez créer un nouveau sous-domaine ou migrer un sous-domaine existant vers Route 53, tout en conservant le domaine parent hébergé chez un autre fournisseur de services DNS.

Création d'un nouveau sous-domaine avec Route 53 :

1. Créez une zone hébergée pour le nouveau sous-domaine.
2. Ajoutez les enregistrements DNS souhaités (par exemple, A, CNAME, MX) pour le sous-domaine à la zone hébergée.
3. Obtenez les serveurs de noms Route 53 assignés à la zone hébergée.
4. Mettez à jour la configuration DNS du domaine parent en ajoutant des enregistrements NS (serveur de noms) pour le sous-domaine, en pointant vers les serveurs de noms Route 53.

Migration d'un sous-domaine existant vers Route 53 :

1. Créez une zone hébergée pour le sous-domaine.
2. Obtenez la configuration DNS actuelle pour le sous-domaine auprès de votre fournisseur de services DNS existant.

3. Ajoutez les enregistrements DNS correspondants à la zone hébergée.
4. Obtenez les serveurs de noms Route 53 assignés à la zone hébergée.
5. Mettez à jour la configuration DNS du domaine parent en ajoutant des enregistrements NS pour le sous-domaine, en pointant vers les serveurs de noms Route 53.

En suivant ces étapes, vous pouvez tirer parti des fonctionnalités avancées de Route 53, telles que les contrôles de santé, les politiques de routage et la gestion du flux de trafic, pour vos sous-domaines tout en conservant la configuration DNS du domaine parent auprès de votre fournisseur actuel.

Rubriques

- Création d'un sous-domaine qui utilise Amazon Route 53 en tant que service DNS sans migration du domaine parent
- Migration d'un service DNS pour un sous-domaine vers Amazon Route 53 sans migration du domaine parent

Création d'un sous-domaine qui utilise Amazon Route 53 en tant que service DNS sans migration du domaine parent

Vous pouvez créer un sous-domaine qui utilise Amazon Route 53 en tant que service DNS sans migrer le domaine parent depuis un autre service DNS.

Le processus comporte les étapes de base suivantes :

1. Déterminez si cette procédure est adaptée à votre situation.
2. Créez une zone hébergée Route 53 pour le sous-domaine.
3. Ajoutez des enregistrements pour le nouveau sous-domaine à votre zone hébergée Route 53.
4. API uniquement : confirmez que vos modifications ont été répercutées à tous les serveurs DNS de Route 53.

> **Note**
>
> Actuellement, le seul moyen de vérifier que les modifications se sont propagées est d'utiliser l'action GetChangeAPI. Les changements se propagent généralement sur tous les serveurs de Route 53 en 60 secondes.

5. Mettez à jour le service DNS pour le domaine parent en ajoutant des enregistrements de serveur de noms pour le sous-domaine.

Choisir les procédures à utiliser pour créer un sous-domaine

Les procédures de cette rubrique expliquent comment effectuer une opération rare. Si vous utilisez déjà Route 53 comme service DNS pour votre domaine et que vous souhaitez simplement acheminer le trafic d'un sous-domaine, tel que www.example.com, vers vos ressources, telles qu'un serveur Web exécuté sur une EC2 instance, consultez. Acheminement du trafic pour les sous-domaines

N'utilisez cette procédure que si vous utilisez un autre service DNS pour un domaine, par exemple exemple.com, et que vous voulez commencer à utiliser Route 53 en tant que service DNS pour un nouveau sous-domaine de ce domaine, par exemple www.exemple.com.

Création d'une zone hébergée pour le nouveau sous-domaine

Lorsque vous souhaitez utiliser Amazon Route 53 en tant que service DNS pour un nouveau sous-domaine sans migrer le domaine parent, vous commencez par créer une zone hébergée pour le sous-domaine. Route 53 stocke des informations sur votre sous-domaine dans la zone hébergée.

Pour plus d'informations sur la façon de créer une zone hébergée à l'aide de la console Route 53, consultez Création d'une zone hébergée publique.

Création d'enregistrements

Vous pouvez créer des enregistrements à l'aide de la console Amazon Route 53 ou de l'API Route 53. Les enregistrement que vous créez dans Route 53 deviennent les enregistrements qu'utilise DNS une fois que vous déléguez la responsabilité du sous-domaine à Route 53, comme expliqué dans Mise à jour de votre service DNS avec les enregistrements de serveur de noms pour le sous-domaine, ultérieurement dans le processus.

> **Important**
>
> Ne créez pas d'autre enregistrement NS ou SOA dans la zone hébergée Route 53 et ne supprimez pas les enregistrements NS et SOA existants.

Pour créer des enregistrements à l'aide de la console Route 53, consultez Utilisation des enregistrements. Pour créer des enregistrements à l'aide de l'API Route 53, consultez

`ChangeResourceRecordSets`. Pour plus d'informations, consultez ChangeResourceRecordSetsle manuel Amazon Route 53 API Reference.

Vérification du statut de vos modifications (API uniquement)

La création d'une nouvelle zone hébergée et la modification des enregistrements prennent du temps pour se propager sur les serveurs DNS Route 53. Si vous avez créé vos enregistrements, vous pouvez utiliser cette `GetChange` action pour déterminer si vos modifications se sont propagées. ChangeResourceRecordSets (`ChangeResourceRecordSets`renvoie une valeur que vous pouvez inclure dans une `GetChange` demande ultérieure. `ChangeId` `ChangeId`n'est pas disponible si vous avez créé les enregistrements à l'aide de la console.) Pour plus d'informations, consultez GET GetChange dans le manuel Amazon Route 53 API Reference.

> **Note**
>
> Les changements se propagent généralement sur tous les serveurs de Route 53 en 60 secondes.

Mise à jour de votre service DNS avec les enregistrements de serveur de noms pour le sous-domaine

Lorsque les modifications apportées aux enregistrements Amazon Route 53 ont été répercutées (voir Vérification du statut de vos modifications (API uniquement)), mettez à jour le service DNS pour le domaine parent en ajoutant des enregistrements NS pour le sous-domaine. Cette méthode consiste à déléguer la responsabilité pour un sous-domaine à Route 53. Par exemple, si le domaine parent example.com est hébergé avec un autre service DNS et que vous avez créé le sous-domaine test.example.com dans Route 53, vous devez mettre à jour le service DNS de example.com avec les nouveaux enregistrements NS de test.example.com.

Utilisez la procédure suivante.

1. Utilisez la méthode fournie par votre service DNS pour sauvegarder le fichier de zone pour le domaine parent.
2. Dans la console Route 53, récupérez les serveurs de noms pour votre zone hébergée Route 53 :
   a. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
   b. Dans le panneau de navigation, choisissez Hosted zones (Zones hébergées).

c. Sur la page Hosted zones (Zones hébergées), choisissez la case d'option (pas le nom) de la zone hébergée, puis View details (Afficher les détails).

d. Sur la page des détails de la zone hébergée, choisissez Hosted zone details (Détails de la zone hébergée).

e. Notez les quatre serveurs répertoriés dans Name servers (Serveurs de noms).

Vous pouvez également utiliser l'action `GetHostedZone`. Pour plus d'informations, consultez GetHostedZonele manuel Amazon Route 53 API Reference.

3. Utilisez la méthode fournie par le service DNS du domaine parent pour ajouter des enregistrements NS pour le sous-domaine dans le fichier de zone pour le domaine parent. Dans ces enregistrements NS, spécifiez les quatre serveurs de noms Route 53 qui sont associés à la zone hébergée que vous avez créée à l'étape 1.

> **Important**
>
> N'ajoutez pas d'enregistrement SOA au fichier de zone du domaine parent. Étant donné que le sous-domaine utilisera Route 53, le service DNS du domaine parent n'est pas le service de référence pour le sous-domaine.
> Si votre service DNS a automatiquement ajouté un enregistrement SOA pour le sous-domaine, supprimez-le pour le sous-domaine, en veillant à ne pas le supprimer pour le domaine parent.

Migration d'un service DNS pour un sous-domaine vers Amazon Route 53 sans migration du domaine parent

Vous pouvez migrer un sous-domaine afin d'utiliser Amazon Route 53 en tant que service DNS sans migrer le domaine parent à partir d'un autre service DNS.

Le processus comporte les étapes de base suivantes :

1. Déterminez si cette procédure est adaptée à votre situation.
2. Créez une zone hébergée Route 53 pour le sous-domaine.
3. Obtenez la configuration DNS actuelle auprès du fournisseur de services DNS actuel pour le domaine parent.

4. Ajoutez des enregistrements pour le sous-domaine à votre zone hébergée Route 53.
5. API uniquement : confirmez que vos modifications ont été répercutées à tous les serveurs DNS de Route 53.

> **Note**
>
> À l'heure actuelle, le seul moyen de vérifier que les modifications se sont propagées consiste à utiliser l'action GetChangeAPI. Les changements se propagent généralement sur tous les serveurs Route 53 en 60 secondes.

6. Mettez à jour la configuration DNS avec le fournisseur de services DNS pour le domaine parent en ajoutant des enregistrements de serveur de noms pour le sous-domaine.

Choisir les procédures à utiliser pour créer un sous-domaine

Les procédures de cette rubrique expliquent comment effectuer une opération rare. Si vous utilisez déjà Route 53 comme service DNS pour votre domaine et que vous souhaitez simplement acheminer le trafic d'un sous-domaine, tel que www.example.com, vers vos ressources, telles qu'un serveur Web exécuté sur une EC2 instance, consultez. Acheminement du trafic pour les sous-domaines

N'utilisez cette procédure que si vous utilisez un autre service DNS pour un domaine, par exemple exemple.com, et que vous voulez commencer à utiliser Route 53 en tant que service DNS pour un sous-domaine existant de ce domaine, par exemple www.exemple.com.

Création d'une zone hébergée pour le sous-domaine

Si vous souhaitez effectuer la migration d'un sous-domaine d'un autre service DNS vers Amazon Route 53 sans effectuer la migration du domaine parent, commencez par créer une zone hébergée pour le sous-domaine. Route 53 stocke des informations sur votre sous-domaine dans la zone hébergée.

Pour plus d'informations sur la façon de créer une zone hébergée à l'aide de la console Route 53, consultez Création d'une zone hébergée publique.

Obtention de la configuration DNS actuelle auprès du fournisseur de services DNS

Pour simplifier le processus de migration d'un sous-domaine existant vers Route 53, obtenez la configuration DNS actuelle du domaine auprès du fournisseur de services DNS actuellement en

charge du domaine. Vous pouvez utiliser ces informations comme base pour configurer Route 53 en tant que service DNS pour le sous-domaine.

Les informations que vous demandez et le format dans lequel vous les recevez dépend de votre fournisseur de services DNS actuel. Dans l'idéal, vous recevez un fichier de zone, qui contient les informations relatives à tous les enregistrements de votre configuration actuelle. (Les enregistrements indiquent au DNS comment vous souhaitez que le trafic soit acheminé pour vos domaines et sous-domaines. Par exemple, lorsque quelqu'un saisit votre nom de domaine dans un navigateur Web, souhaitez-vous que le trafic soit acheminé vers un serveur Web de votre centre de données, vers une EC2 instance Amazon, vers une CloudFront distribution ou vers un autre emplacement ?) Si vous pouvez obtenir un fichier de zone de la part de votre fournisseur de services DNS actuel, vous pouvez le modifier pour supprimer les enregistrements que vous ne souhaitez pas migrer vers Amazon Route 53. Ensuite, vous pouvez importer les enregistrements restants vers votre zone hébergée Route 53, ce qui simplifie considérablement le processus. Demandez au service client de votre fournisseur de services DNS actuel comment obtenir un fichier de zone ou une liste d'enregistrements.

Création d'enregistrements

Utilisez les enregistrements que vous avez reçus de votre fournisseur de services DNS actuel comme point de départ pour créer les enregistrements correspondants dans la zone hébergée Amazon Route 53 créée pour le sous-domaine. Les enregistrement que vous créez dans Route 53 deviennent les enregistrements qu'utilise DNS une fois que vous déléguez la responsabilité du sous-domaine à Route 53, comme expliqué dans Mise à jour de votre service DNS avec les enregistrements de serveur de noms pour le sous-domaine, ultérieurement dans le processus.

> **Important**
>
> Ne créez pas d'autre enregistrement NS ou SOA dans la zone hébergée Route 53 et ne supprimez pas les enregistrements NS et SOA existants.

Pour créer des enregistrements à l'aide de la console Route 53, consultez Utilisation des enregistrements. Pour créer des enregistrements à l'aide de l'API Route 53, consultez `ChangeResourceRecordSets`. Pour plus d'informations, consultez ChangeResourceRecordSetsle manuel Amazon Route 53 API Reference.

Vérification du statut de vos modifications (API uniquement)

La création d'une nouvelle zone hébergée et la modification des enregistrements prennent du temps pour se propager sur les serveurs DNS Route 53. Si vous avez créé vos enregistrements, vous pouvez utiliser cette `GetChange` action pour déterminer si vos modifications se sont propagées. ChangeResourceRecordSets (`ChangeResourceRecordSets`renvoie une valeur que vous pouvez inclure dans une `GetChange` demande ultérieure. `ChangeId` `ChangeIdn`'est pas disponible si vous avez créé les enregistrements à l'aide de la console.) Pour plus d'informations, consultez GET GetChange dans le manuel Amazon Route 53 API Reference.

> **Note**
>
> Les changements se propagent généralement sur tous les serveurs de Route 53 en 60 secondes.

Mise à jour de votre service DNS avec les enregistrements de serveur de noms pour le sous-domaine

Lorsque les modifications apportées aux enregistrements Amazon Route 53 ont été répercutées (voir Vérification du statut de vos modifications (API uniquement)), mettez à jour le service DNS pour le domaine parent en ajoutant des enregistrements NS pour le sous-domaine. Cette méthode consiste à déléguer la responsabilité pour un sous-domaine à Route 53. Supposons par exemple que le domaine parent example.com est hébergé par un autre service DNS et que vous migrez le sous-domaine test.example.com vers Route 53. Vous devez créer une zone hébergée pour test.example.com et mettre à jour le service DNS pour example.com avec les enregistrements NS que Route 53 a assigné à la nouvelle zone hébergée pour test.example.com.

Utilisez la procédure suivante.

1. Utilisez la méthode fournie par votre service DNS pour sauvegarder le fichier de zone pour le domaine parent.
2. Si l'ancien fournisseur de services DNS pour le domaine propose une méthode pour modifier les paramètres de durée de vie pour leurs serveurs de noms, nous vous recommandons de modifier ces paramètres à 900 secondes. Cela vous permet de limiter la durée pendant laquelle les demandes client tenteront de résoudre des noms de domaine à l'aide de serveurs de noms obsolètes. Si la valeur actuelle de la durée de vie est 172 800 secondes (deux jours), valeur par défaut couramment utilisée pour ce paramètre, vous devez attendre deux jours pour que

les résolveurs et les clients arrêtent de mettre en cache des enregistrements DNS à l'aide de la valeur de la durée de vie précédente. Après expiration des paramètres de la durée de vie, vous pouvez supprimer en toute sécurité les enregistrements qui sont stockés chez l'ancien fournisseur et apporter des modifications uniquement dans Route 53.

3. Dans la console Route 53, récupérez les serveurs de noms pour votre zone hébergée Route 53 :

   a. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.

   b. Dans le panneau de navigation, choisissez Hosted zones (Zones hébergées).

   c. Sur la page Hosted zones (Zones hébergées), choisissez la case d'option (pas le nom) de la zone hébergée, puis View details (Afficher les détails).

   d. Sur la page des détails de la zone hébergée, choisissez Hosted zone details (Détails de la zone hébergée).

   e. Notez les quatre serveurs répertoriés dans Name servers (Serveurs de noms).

   Vous pouvez également utiliser l'action `GetHostedZone`. Pour plus d'informations, consultez GetHostedZonele manuel Amazon Route 53 API Reference.

4. Utilisez la méthode fournie par le service DNS du domaine parent pour ajouter des enregistrements NS pour le sous-domaine dans le fichier de zone pour le domaine parent. Attribuez aux enregistrements NS le même nom que celui du sous-domaine. Pour les valeurs des enregistrements NS, spécifiez les quatre serveurs de noms Route 53 qui sont associés à la zone hébergée que vous avez créée à l'étape 2. Notez que les différents services de DNS utilisent une terminologie différente. Vous pouvez être amené à contacter le support technique de votre service DNS pour effectuer cette étape.

   > **Important**
   >
   > N'ajoutez pas d'enregistrement SOA au fichier de zone du domaine parent. Étant donné que le sous-domaine utilisera Route 53, le service DNS du domaine parent n'est pas le service de référence pour le sous-domaine.
   > Si votre service DNS a automatiquement ajouté un enregistrement SOA pour le sous-domaine, supprimez-le pour le sous-domaine, en veillant à ne pas le supprimer pour le domaine parent.

En fonction des paramètres de la durée de vie des serveurs de noms du domaine parent, la propagation de vos modifications aux résolveurs DNS peut prendre 48 heures ou plus. Durant cette période, les résolveurs DNS peuvent toujours répondre aux demandes avec les serveurs de noms du service DNS du domaine parent. En outre, les ordinateurs clients peuvent continuer à utiliser les serveurs de noms précédents pour le sous-domaine dans leur cache.

5. Une fois que les paramètres de la durée de vie du bureau d'enregistrement du domaine expirent (voir l'étape 2), supprimez les enregistrements suivants du fichier de zone pour le domaine parent :

   - Les enregistrements que vous avez ajoutés à Route 53 comme décrit dans Création d'enregistrements.
   - Les enregistrements NS de votre service DNS. Lorsque vous avez terminé de supprimer des enregistrements NS, les seuls enregistrements NS du fichier de zone seront ceux que vous avez créés à l'étape 4.

Transition vers le routage basé sur la latence dans Amazon Route 53

Grâce au routage basé sur la latence, Amazon Route 53 peut diriger vos utilisateurs vers le point de terminaison à latence la plus faible AWS disponible. Par exemple, vous pouvez associer un nom DNS à un ELB Classic, Application ou Network Load Balancer, ou à des instances EC2 Amazon ou à des adresses IP Elastic hébergées dans les régions USA Est (Ohio) et Europe (Irlande). `www.example.com` Les serveurs DNS Route 53 décident, en fonction des conditions du réseau au cours des deux semaines précédentes, quelles instances dans quelles régions doivent servir des utilisateurs spécifiques. Un utilisateur basé à Londres sera probablement dirigé vers l'instance Europe (Irlande), un utilisateur basé à Chicago sera probablement dirigé vers l'instance USA Est (Ohio), et ainsi de suite. Route 53 prend en charge le routage basé sur la latence pour les enregistrements A, AAAA, TXT et CNAME, ainsi que les alias pour les enregistrements A et AAAA.

> **Note**
>
> Les données relatives à la latence entre les utilisateurs et vos ressources sont entièrement basées sur le trafic entre les utilisateurs et les centres de AWS données. Si vous n'utilisez pas de ressources dans une AWS région, la latence réelle entre vos utilisateurs et vos

ressources peut varier considérablement en fonction des données de AWS latence. Cela est vrai même si vos ressources sont situées dans la même ville qu'une AWS région.

Pour profiter d'une transition en douceur et présentant un faible risque, vous pouvez associer des enregistrements de latence et pondérés pour migrer progressivement d'un routage standard à un routage basé sur la latence, en exerçant un contrôle total et en ayant la possibilité de revenir en arrière à chaque étape. Prenons un exemple dans lequel elle `www.example.com` est actuellement hébergée sur une EC2 instance Amazon dans la région USA Est (Ohio). L'instance a l'adresse IP Elastic `W.W.W.W`. Supposons que vous souhaitiez continuer à acheminer le trafic vers la région USA Est (Ohio), le cas échéant, tout en dirigeant les utilisateurs vers des EC2 instances Amazon supplémentaires dans la région USA Ouest (Californie du Nord) (Elastic IP`X.X.X.X`) et dans la région Europe (Irlande) (Elastic `Y.Y.Y.Y` IP). La zone hébergée Route 53 pour `example.com` a déjà un enregistrement pour `www.example.com`, dont la valeur de Type est A et celle de Valeur (une adresse IP) est `W.W.W.W`.

Lorsque l'exemple suivant est terminé, vous disposez de deux enregistrements d'alias pondérés :

- Vous allez convertir votre enregistrement existant pour `www.example.com` en un enregistrement alias pondéré qui continue à diriger la majeure partie de votre trafic vers votre EC2 instance Amazon existante dans la région USA Est (Ohio).
- Vous allez créer un autre enregistrement d'alias pondéré qui, au départ, dirige seulement une petite partie de votre trafic vers vos enregistrements de latence, qui acheminent le trafic vers les trois régions.

En mettant à jour les pondérations dans ces enregistrements d'alias pondérés, vous pouvez progressivement passer du routage du trafic uniquement vers la région USA Est (Ohio) à l'acheminement du trafic vers les trois régions dans lesquelles vous possédez des EC2 instances Amazon.

Pour effectuer la transition vers le routage basé sur la latence

1. Faites une copie de l'enregistrement pour `www.example.com`, mais utilisez un nouveau nom de domaine, par exemple `copy-www.example.com`. Attribuez au nouvel enregistrement les mêmes valeurs Type (A) et Value (`W.W.W.W`) que celles de l'enregistrement pour `www.example.com`.

2. Mettez à jour l'enregistrement A existant pour `www.example.com` afin qu'il devienne l'enregistrement d'alias pondéré :

   - Pour Value/Route traffic to (Valeur/acheminer le trafic vers), choisissez Alias to another record in this hosted zone (Alias vers un autre enregistrement de cette zone hébergée), et spécifiez `copy-www.example.com`.
   - Pour Weight (Poids), spécifiez 100.

   Lorsque vous avez terminé la mise à jour, Route 53 continue à utiliser cet enregistrement pour acheminer l'ensemble du trafic vers la ressource dont l'adresse IP est `W.W.W.W`.

3. Créez un enregistrement de latence pour chacune de vos EC2 instances Amazon, par exemple :

   - USA Est (Ohio), adresse IP Elastic `W.W.W.W`
   - USA Ouest (Californie du Nord), adresse IP Elastic `X.X.X.X`
   - Europe (Irlande), adresse IP Elastic `Y.Y.Y.Y`

   Attribuez à tous les enregistrements de latence le même nom de domaine, par exemple `www-lbr.example.com`, et le même type, A.

   Lorsque vous avez terminé de créer des enregistrements de latence, Route 53 continue à acheminer le trafic à l'aide de l'enregistrement mis à jour à l'étape 2.

   Vous pouvez utiliser `www-lbr.example.com` pour les tests de validation, par exemple pour vous assurer que chaque point de terminaison peut accepter des demandes.

4. Ajoutons maintenant l'enregistrement de `www-lbr.example.com` latence à l'enregistrement `www.example.com` pondéré et commençons à acheminer le trafic limité vers les EC2 instances Amazon correspondantes. Cela signifie que l' EC2 instance Amazon de la région de l'est des États-Unis (Ohio) recevra du trafic provenant des deux enregistrements pondérés.

   Créer un autre enregistrement d'alias pondéré pour `www.example.com` :

   - Pour Value/Route traffic to (Valeur/acheminer le trafic vers), choisissez Alias to another record in this hosted zone (Alias vers un autre enregistrement de cette zone hébergée), et spécifiez `www-lbr.example.com.`
   - Pour Weight (Poids), spécifiez 1.

Lorsque vous aurez terminé et que vos modifications seront synchronisées avec les serveurs Route 53, Route 53 commencera à acheminer une infime fraction de votre trafic (1/101) vers les EC2 instances Amazon pour lesquelles vous avez créé des enregistrements de latence à l'étape 3.

5. Au fur et à mesure que vous avez l'assurance que vos points de terminaison sont correctement dimensionnés pour le trafic entrant, ajustez les pondérations en conséquence. Par exemple, si vous souhaitez que 10 % de vos demandes soient basées sur le routage basé sur la latence, modifiez respectivement les pondérations par 90 et 10.

Pour plus d'informations sur la création des enregistrements de latence, consultez Création d'enregistrements à l'aide de la console Amazon Route 53.

Ajout d'une autre région à votre routage basé sur la latence dans Amazon Route 53

Si vous utilisez le routage basé sur la latence et si vous souhaitez ajouter une instance dans une nouvelle région, vous pouvez diriger progressivement le trafic vers la nouvelle région de la même manière que vous avez progressivement passé le trafic au routage basé sur la latence dans Transition vers le routage basé sur la latence dans Amazon Route 53.

Par exemple, supposons que vous utilisiez un routage basé sur la latence pour `www.example.com` acheminer le trafic et que vous souhaitiez ajouter une EC2 instance Amazon en Asie-Pacifique (Tokyo) à vos instances situées dans l'est des États-Unis (Ohio), dans l'ouest des États-Unis (Californie du Nord) et en Europe (Irlande). L'exemple de procédure suivant explique une façon d'ajouter une instance dans une autre région.

Dans le cadre de cet exemple, la zone hébergée Amazon Route 53 pour `example.com` a déjà un enregistrement d'alias pondéré pour `www.example.com` qui achemine le trafic vers les enregistrements basés sur la latence pour `www-lbr.example.com` :

- USA Est (Ohio), adresse IP Elastic `W.W.W.W`
- USA Ouest (Californie du Nord), adresse IP Elastic `X.X.X.X`
- Europe (Irlande), adresse IP Elastic `Y.Y.Y.Y`

La pondération de l'enregistrement d'alias pondéré est 100. Une fois que vous effectuez la transition vers le routage basé sur la latence, supposez que vous avez supprimé l'autre enregistrement pondéré que vous avez utilisé pour la transition.

Pour ajouter une autre région à votre routage basé sur la latence dans Route 53

1. Créez quatre nouveaux enregistrements basés sur la latence qui incluent les trois régions d'origine, ainsi que la nouvelle région pour laquelle vous voulez commencer à acheminer le trafic.

   - USA Est (Ohio), adresse IP Elastic `W.W.W.W`
   - USA Ouest (Californie du Nord), adresse IP Elastic `X.X.X.X`
   - Europe (Irlande), adresse IP Elastic `Y.Y.Y.Y`
   - Adresse IP Elastic `Z.Z.Z.Z`

   Attribuez à tous les enregistrements de latence le même nouveau nom de domaine, par exemple `www-lbr-2012-04-30.example.com`, et le même type, A.

   Lorsque vous avez terminé de créer les enregistrements de latence, Route 53 continue d'acheminer le trafic à l'aide de l'enregistrement d'alias pondéré (`www.example.com`) et des enregistrements de latence (`www-lbr.example.com`) d'origine.

   Vous pouvez utiliser les enregistrements `www-lbr-2012-04-30.example.com` pour les tests de validation, par exemple pour vous assurer que chaque point de terminaison peut accepter des demandes.
2. Créer un enregistrement d'alias pondéré pour les nouveaux enregistrements de latence :

   - Pour le nom de domaine, spécifiez le nom de l'enregistrement d'alias pondéré existant, `www.example.com`.
   - Pour Value/Route traffic to (Valeur/acheminer le trafic vers), choisissez Alias to another record in this hosted zone (Alias vers un autre enregistrement de cette zone hébergée), et spécifiez `www-lbr-2012-04-30.example.com`.
   - Pour Weight (Poids), spécifiez 1.

   Lorsque vous aurez terminé, Route 53 commencera à acheminer une infime fraction de votre trafic (1/101) vers les EC2 instances Amazon pour lesquelles vous avez créé les enregistrements de `www-lbr-2012-04-30.example.com` latence à l'étape 1. Le reste du trafic continuera

d'être acheminé vers les enregistrements de `www-lbr.example.com` latence, qui n'incluent pas l' EC2 instance Amazon dans la région Asie-Pacifique (Tokyo).

3. Au fur et à mesure que vous avez l'assurance que vos points de terminaison sont correctement dimensionnés pour le trafic entrant, ajustez les pondérations en conséquence. Par exemple, si vous souhaitez que 10 % de vos demandes soient acheminées vers les enregistrements de latence qui comprennent la région de Tokyo, modifiez la pondération de `www-lbr.example.com` de 100 à 90 et la pondération de `www-lbr-2012-04-30.example.com` de 1 à 10.

Pour plus d'informations sur la création d'enregistrements, consultez Création d'enregistrements à l'aide de la console Amazon Route 53.

Utilisation de la latence et des enregistrements pondérés dans Amazon Route 53 pour acheminer le trafic vers plusieurs EC2 instances Amazon dans une région

Si votre application s'exécute sur des EC2 instances Amazon dans au moins deux EC2 régions Amazon, et si vous avez plusieurs EC2 instances Amazon dans une ou plusieurs régions, vous pouvez utiliser le routage basé sur la latence pour acheminer le trafic vers la bonne région, puis utiliser des enregistrements pondérés pour acheminer le trafic vers les instances de la région en fonction des poids que vous spécifiez.

Supposons, par exemple, que vous disposiez de trois EC2 instances Amazon dotées d'adresses IP élastiques dans la région USA Est (Ohio) et que vous souhaitiez répartir les demandes sur les trois de IPs manière égale pour les utilisateurs pour lesquels la région USA Est (Ohio) est la région appropriée. Une seule EC2 instance Amazon est suffisante dans les autres régions, mais vous pouvez appliquer la même technique à plusieurs régions à la fois.

Pour utiliser la latence et les enregistrements pondérés dans Amazon Route 53 pour acheminer le trafic vers plusieurs EC2 instances Amazon dans une région

1. Créez un groupe d'enregistrements pondérés pour les EC2 instances Amazon de la région. Remarques :

   - Attribuez à chaque enregistrement pondéré la même valeur pour Record name (Nom de l'enregistrement (par exemple, `us-east.example.com`) et Record type (Type d'enregistrement).

- Pour Value/Route traffic to (Valeur/Acheminer le trafic vers), choisissez IP address or another value depending on the record type (Adresse IP ou une autre valeur en fonction du type d'enregistrement) et spécifiez la valeur d'une adresse IP Elastic.
- Si vous souhaitez pondérer les EC2 instances Amazon de manière égale, spécifiez la même valeur pour Weight.
- Spécifiez une valeur unique pour Set ID pour chaque enregistrement.

Pour plus d'informations sur les enregistrements pondérés, veuillez consulter la section Weighted routing (Routage pondéré).

2. Si vous avez plusieurs EC2 instances Amazon dans d'autres régions, répétez l'étape 1 pour les autres régions. Spécifiez une valeur différente pour Name (Nom) dans chaque région.
3. Pour chaque région dans laquelle vous possédez plusieurs EC2 instances Amazon (par exemple, USA East (Ohio)), créez un enregistrement d'alias de latence. Pour Value/Route traffic to (Valeur/Routage du trafic vers), choisissez Alias to another record in this hosted zone (Alias vers un autre enregistrement de cette zone hébergée) et spécifiez la valeur du champ Record name (Nom de l'enregistrement) (par exemple, `us-east.example.com`) que vous avez affecté aux enregistrements pondérés dans cette région.
4. Pour chaque région dans laquelle vous possédez une EC2 instance Amazon, créez un enregistrement de latence. Pour la valeur de Record name (Nom de l'enregistrement), spécifiez la même valeur que celle spécifiée pour les enregistrements d'alias de latence créés à l'étape 3. Pour Valuer/Router le trafic vers, choisissez l'adresse IP ou une autre valeur en fonction du type d'enregistrement, puis spécifiez l'adresse IP élastique de l' EC2 instance Amazon dans cette région.

   Pour plus d'informations sur l'ajout d'enregistrements d'alias aux EC2 instances Amazon, consultez Acheminement du trafic vers une EC2 instance Amazon

Pour plus d'informations sur la création d'enregistrements, consultez Création d'enregistrements à l'aide de la console Amazon Route 53.

Gestion de plus de 100 enregistrements pondérés dans Amazon Route 53

Amazon Route 53 vous permet de configurer des enregistrements pondérés. Pour un nom et un type donnés (par exemple, `www.example.com`, type A), vous pouvez configurer jusqu'à 100 réponses

alternatives, chacune ayant sa propre pondération. Lorsque les serveurs DNS Route 53 répondent aux demandes pour `www.example.com`, ils sélectionnent une réponse aléatoire pondérée qui sera renvoyée aux résolveurs DNS. La valeur d'un enregistrement pondéré dont la pondération est 2 est renvoyée en moyenne deux fois plus souvent que la valeur d'un enregistrement pondéré dont la pondération est 1.

Si vous avez besoin de diriger le trafic vers plus de 100 points de terminaison, vous pouvez utiliser une arborescence d'enregistrements d'alias pondérés et d'enregistrements pondérés. Par exemple, le premier « niveau » de l'arborescence comporter jusqu'à 100 enregistrements d'alias pondérés, chacun pouvant, tour à tour, pointer vers 100 enregistrements pondérés au maximum. Route 53 permet jusqu'à trois niveaux de récursivité, ce qui vous permet de gérer jusqu'à 1 000 000 points de terminaison pondérés uniques.

Une arborescence à deux niveaux simple peut ressembler à ceci :

Enregistrements d'alias pondérés

- Alias `www.example.com` à `www-a.example.com` avec une pondération de 1
- Alias `www.example.com` à `www-b.example.com` avec une pondération de 1

Enregistrements pondérés

- `www-a.example.com`, type A, valeur 192.0.2.1, pondération 1
- `www-a.example.com`, type A, valeur 192.0.2.2, pondération 1

- `www-b.example.com`, type A, valeur 192.0.2.3, pondération 1
- `www-b.example.com`, type A, valeur 192.0.2.4, pondération 1

Pour plus d'informations sur la création d'enregistrements, consultez Utilisation des enregistrements.

Pondération des réponses pour la tolérance aux pannes pour plusieurs enregistrements dans Amazon Route 53

> **Note**
>
> Les enregistrements utilisant une règle de routage de réponse multivaleur se comportent assez similairement à la configuration figurant dans ce didacticiel. La principale différence

est que la configuration du didacticiel vous permet de spécifier des pondérations, ce qui peut être utile lorsque vos points de terminaison ont des capacités distinctes. Pour de plus amples informations, veuillez consulter Multivalue answer routing (Routage de réponse multivaleur).

Un enregistrement pondéré Amazon Route 53 ne peut être associé qu'à un enregistrement, c'est-à-dire à une combinaison d'un nom (par exemple, `example.com`) et d'un type d'enregistrement (par exemple, A). Mais il est souvent préférable de pondérer les réponses DNS contenant plusieurs enregistrements.

Par exemple, vous pouvez avoir huit EC2 instances Amazon ou points de terminaison IP Elastic pour un service. Si les clients de ce service prennent en charge les nouvelles tentatives de connexion (à l'instar de tous les navigateurs courants), alors le fait de fournir plusieurs adresses IP dans les réponses DNS fournit à ces clients des points de terminaison alternatifs, en cas de défaillance d'un point de terminaison. Vous pouvez même vous protéger contre la défaillance d'une zone de disponibilité si vous configurez les réponses de manière à ce qu'elles soient IPs hébergées dans au moins deux zones de disponibilité.

Les réponses impliquant plusieurs enregistrements sont également utiles lorsqu'un grand nombre de clients (par exemple, des applications web mobiles) partage un petit ensemble de caches DNS. Dans ce cas, les réponses impliquant plusieurs enregistrements permettent aux clients de diriger les demandes vers plusieurs points de terminaison même s'ils reçoivent une réponse DNS commune du cache partagé.

Ces types de réponses pondérées impliquant plusieurs enregistrements peuvent être obtenus grâce à une combinaison d'enregistrements et d'enregistrements d'alias pondérés. Vous pouvez regrouper huit points de terminaison dans deux jeux d'enregistrements distincts, chacun contenant quatre adresses IP :

`endpoint-a.example.com`, type A, avec les valeurs suivantes :

- 192.0.2.1
- 192.0.2.2
- 192.0.2.128
- 192.0.2.129

`endpoint-b.example.com`, type A, avec les valeurs suivantes :

- 192.0.2.3
- 192.0.2.4
- 192.0.2.130
- 192.0.2.131

Vous pouvez ensuite créer un enregistrement d'alias pondéré qui pointe vers chaque groupe :

- alias `www.example.com` à `endpoint-a.example.com`, type A, pondération 1
- alias `www.example.com` à `endpoint-b.example.com`, type A, pondération 1

Pour plus d'informations sur la création d'enregistrements, consultez Utilisation des enregistrements.

Bonnes pratiques relatives à Amazon Route 53

Cette section présente les meilleures pratiques relatives aux différents composants d'Amazon Route 53, notamment :

1. Bonnes pratiques en matière de DNS :
   - Comprenez les compromis entre les valeurs de durée de vie (TTL) et la réactivité par rapport à la fiabilité.
   - Utilisez des enregistrements alias plutôt que des enregistrements CNAME lorsque cela est possible pour améliorer les performances et réduire les coûts.
   - Configurez les politiques de routage par défaut pour garantir que tous les clients reçoivent une réponse.
   - Tirez parti du routage basé sur la latence pour minimiser la latence des applications et du routage par géolocalisation/géoproximité pour plus de stabilité et de prévisibilité.
   - Vérifiez la propagation des modifications à l'aide de l'`GetChange`API pour les flux de travail automatisés.
   - Déléguez les sous-domaines de la zone parent pour un routage cohérent.
   - Évitez les réponses uniques volumineuses en utilisant le routage des réponses à valeurs multiples.
2. Meilleures pratiques en matière de résolution :
   - Empêchez les boucles de routage en évitant d'associer le même VPC à la fois à une règle de résolution et à son point de terminaison entrant.
   - Mettez en œuvre des règles de groupe de sécurité afin de réduire les frais de suivi des connexions et d'optimiser le débit des requêtes.
   - Configurez les points de terminaison entrants avec des adresses IP dans plusieurs zones de disponibilité à des fins de redondance.
   - Soyez conscient des attaques potentielles basées sur les zones DNS et contactez le AWS Support si vos terminaux subissent un ralentissement.
3. Bonnes pratiques en matière de bilans de santé :
   - Suivez les recommandations pour optimiser les bilans de santé d'Amazon Route 53 afin de garantir une surveillance fiable de vos ressources

En adhérant à ces meilleures pratiques, vous pouvez optimiser les performances, la fiabilité et la sécurité de votre infrastructure DNS, en garantissant un routage efficace du trafic vers vos applications et services

Rubriques

- Bonnes pratiques relatives à Amazon Route 53 DNS
- Bonnes pratiques relatives à Resolver
- Bonnes pratiques relatives aux vérifications de l'état d'Amazon Route 53

Bonnes pratiques relatives à Amazon Route 53 DNS

Suivez ces bonnes pratiques pour obtenir les meilleurs résultats lorsque vous utilisez le service DNS Amazon Route 53.

Utilisation des fonctions de plan de données pour le basculement DNS et la récupération d'applications

Les plans de données pour Route 53, y compris les bilans de santé, et le contrôle de routage d'Amazon Application Recovery Controller (ARC) sont distribués dans le monde entier et sont conçus pour garantir une disponibilité et des fonctionnalités à 100 %, même en cas d'événements graves. Ils s'intègrent les uns aux autres et ne dépendent pas de la fonctionnalité du plan de contrôle. Bien que les plans de contrôle de ces services, y compris leurs consoles, soient généralement très fiables, ils sont conçus de manière plus centralisée et privilégient la durabilité et la cohérence plutôt que la haute disponibilité. Pour les scénarios tels que le basculement pendant la reprise après sinistre, nous vous recommandons d'utiliser des fonctionnalités telles que les contrôles de santé de Route 53 et le contrôle du routage ARC qui s'appuient sur les fonctionnalités du plan de données pour mettre à jour le DNS. Pour plus d'informations, consultez Concepts de plan de données et contrôle et Blog : Création de mécanismes de reprise après sinistre avec Amazon Route 53.

Choix des valeurs TTL pour les registres DNS

La TTL de DNS est la valeur numérique (en secondes) que les résolveurs DNS utilisent pour décider pendant combien de temps un registre peut être mis en cache sans effectuer une autre requête à Route 53. Tous les registres DNS doivent avoir une TTL spécifiée. La plage recommandée pour les valeurs de TTL est comprise entre 60 et 172 800 secondes.

Le choix d'une TTL est un compromis entre la latence et la fiabilité, et la réactivité au changement. Avec un enregistrement plus court TTLs , les résolveurs DNS constatent les mises à jour de l'enregistrement plus rapidement car ils doivent effectuer des requêtes plus fréquemment. Cela augmente le volume (et le coût) de la requête. Lorsque vous augmentez la TTL, les résolveurs DNS répondent plus souvent aux requêtes du cache, ce qui est généralement plus rapide, moins coûteux et, dans certains cas, plus fiable, car cela évite les requêtes sur Internet. Il n'y a pas de valeur correcte, mais il vaut la peine de réfléchir à la question de savoir si la réactivité ou la fiabilité est plus importante pour vous.

Points à prendre en compte lors de la définition des valeurs de la TTL :

- Définissez un enregistrement DNS TTLs pour la durée que vous pouvez vous permettre d'attendre avant qu'une modification prenne effet. Cela est particulièrement vrai pour les délégations (ensembles de registres NS) ou d'autres registres qui changent rarement, par exemple les registres MX. Pour ces enregistrements, une durée plus longue TTLs est recommandée. Une valeur comprise entre une heure (3 600 s) et un jour (86 400 s) est un choix courant.
- Pour les enregistrements qui doivent être modifiés dans le cadre d'un mécanisme de basculement rapide (en particulier les enregistrements dont l'état de santé est vérifié), une valeur inférieure TTLs est appropriée. La définition d'une TTL de 60 ou 120 secondes est un choix courant pour ce scénario.
- Lorsque vous souhaitez apporter des modifications à des entrées DNS critiques, nous vous recommandons de raccourcir temporairement le TTLs. Vous pouvez ensuite effectuer les modifications, les observer et procéder rapidement à une restauration, si nécessaire. Lorsque les modifications sont finalisées et fonctionnent comme prévu, vous pouvez augmenter les TTL.

Pour plus d'informations, consultez TTL (secondes).

Enregistrements CNAME

Les registres CNAME DNS permettent de pointer un nom de domaine vers un autre. Si un résolveur DNS résout le domaine 1.exemple.com et trouve un CNAME pointant vers domain-2.example.com, le résolveur DNS doit procéder à la résolution domain-2.example.com avant qu'il ne puisse répondre. Ces registres sont utiles dans de nombreuses situations, par exemple pour garantir la cohérence lorsqu'un site Web possède plusieurs noms de domaine.

Cependant, les résolveurs DNS doivent effectuer davantage de requêtes pour y répondre CNAMEs, ce qui augmente le temps de latence et les coûts. Dans la mesure du possible, une

alternative plus rapide et moins coûteuse consiste à utiliser un registre Route 53 alias. Les enregistrements d'alias permettent à Route 53 de répondre directement aux AWS ressources (par exemple, un équilibreur de charge) et aux autres domaines de la même zone hébergée.

Pour de plus amples informations, veuillez consulter Acheminement du trafic Internet vers vos AWS ressources.

Routage DNS avancé

- Lorsque vous utilisez la géolocalisation, la géoproximité ou le routage basé sur la latence, définissez toujours une valeur par défaut, sauf si vous souhaitez que certains clients reçoivent des réponses Aucune réponse.
- Pour réduire la latence des applications, utilisez le routage basé sur la latence. Ce type de données de routage peut changer fréquemment.
- Pour assurer la stabilité et la prévisibilité du routage, utilisez la géolocalisation ou le routage de géoproximité.

Pour plus d'informations, consultez Routage de géolocalisation, Routage par géoproximité et Routage basé sur la latence.

Propagation de la modification du DNS

Lorsque vous créez ou mettez à jour un registre ou une zone hébergée à l'aide de la console ou de l'API Route 53, il faut un certain temps avant que la modification soit reflétée sur Internet. C'est ce qu'on appelle propagation du changement. Bien que la propagation dure généralement moins d'une minute, il arrive parfois qu'une modification soit retardée, par exemple, en raison de problèmes de synchronisation avec un emplacement ou, dans de rares cas, de problèmes du plan de contrôle central. Si vous créez des flux de travail de provisionnement automatisés et qu'il est important d'attendre que la propagation des modifications soit terminée avant de passer à l'étape suivante du flux de travail, utilisez l'GetChangeAPI pour vérifier que vos modifications DNS sont entrées en vigueur (`Status =INSYNC`).

Délégation DNS

Lorsque vous déléguez plusieurs niveaux de sous-domaines dans DNS, il est important de toujours déléguer à partir de la zone parente. Par exemple, si vous déléguez www.dept.example.com, vous devez le faire à partir du dept.example.com zone, pas depuis le example.com zone. Les délégations à partir d'un grand-parent vers une zone enfant peuvent ne pas fonctionner du tout ou fonctionner de manière incohérente. Pour de plus amples informations, veuillez consulter Acheminement du trafic pour les sous-domaines.

Taille de la réponse DNS

Évitez de créer des réponses uniques volumineuses. Si les réponses dépassent les 512 octets, de nombreux résolveurs DNS doivent réessayer sur TCP plutôt que sur UDP, ce qui peut entraîner une fiabilité réduite et des réponses plus lentes. Nous vous recommandons d'utiliser le routage de réponse multivaleur qui choisit huit adresses IP surveillées et aléatoires pour conserver les réponses dans la limite de 512 octets.

Pour plus d'informations, consultez Multivalue answer routing (Routage de réponse multivaleur) et DNS Reply Size Test Server (Serveur de test de taille de réponse DNS).

Bonnes pratiques relatives à Resolver

Cette section fournit les meilleures pratiques pour optimiser Amazon Route 53 Resolver, en abordant les sujets suivants :

1. Éviter les configurations de boucle avec les points de terminaison du résolveur :
   - Empêchez les boucles de routage en vous assurant que le même VPC n'est pas associé à la fois à une règle de résolution et à son point de terminaison entrant.
   - AWS RAM À utiliser pour partager VPCs entre comptes tout en conservant des configurations de routage appropriées.

   Pour de plus amples informations, consultez Évitez les configurations de boucle avec les points de terminaison Resolver..
2. Dimensionnement des points de terminaison du résolveur :
   - Mettez en œuvre des règles de groupe de sécurité qui autorisent le trafic en fonction de l'état de la connexion afin de réduire les frais de suivi des connexions
   - Suivez les règles de groupe de sécurité recommandées pour les points de terminaison du résolveur entrants et sortants afin d'optimiser le débit des requêtes.
   - Surveillez les combinaisons d'adresses IP et de ports uniques générant du trafic DNS afin d'éviter les limitations de capacité.

   Pour de plus amples informations, consultez Mise à l'échelle du point de terminaison Resolver.
3. Haute disponibilité pour les terminaux Resolver :
   - Créez des points de terminaison entrants avec des adresses IP dans au moins deux zones de disponibilité à des fins de redondance.

- Fournir des interfaces réseau supplémentaires pour garantir la disponibilité pendant la maintenance ou les pics de trafic

  Pour de plus amples informations, consultez Haute disponibilité pour les points de terminaison Resolver .

4. Prévention des attaques basées sur les zones DNS :
   - Soyez conscient des attaques potentielles basées sur les zones DNS, dans le cadre desquelles les attaquants tentent de récupérer tout le contenu des zones DNS signées par le protocole DNSSEC.
   - Si vos terminaux subissent un ralentissement en raison d'une suspicion de franchissement de zone, contactez le AWS Support pour obtenir de l'aide.

   Pour de plus amples informations, consultez Parcours de zone DNS .

En suivant ces meilleures pratiques, vous pouvez optimiser les performances, l'évolutivité et la sécurité de vos déploiements de résolveurs Route 53, en garantissant une résolution DNS fiable et efficace pour vos applications et ressources.

Évitez les configurations de boucle avec les points de terminaison Resolver.

N'associez pas le même VPC à une règle Resolver et à son point de terminaison entrant (qu'il s'agisse d'une cible directe du point de terminaison ou via un serveur DNS local). Lorsque le point de terminaison sortant d'une règle Resolver pointe vers un point de terminaison entrant qui partage un VPC avec la règle, il peut provoquer une boucle dans laquelle la requête est continuellement transmise entre les points de terminaison entrants et sortants.

La règle de transfert peut toujours être associée à d'autres VPCs règles partagées avec d'autres comptes en utilisant AWS Resource Access Manager (AWS RAM). Les zones hébergées privées associées au hub, ou à un VPC central, sont toujours résolues à partir des requêtes vers les points de terminaison entrants car une règle de réacheminement de résolveur ne modifie pas cette résolution.

Mise à l'échelle du point de terminaison Resolver

Les groupes de sécurité du point de terminaison Resolver utilisent le suivi de connexion pour collecter des informations sur le trafic en provenance ou à destination des points de terminaison. Chaque interface de point de terminaison dispose d'un nombre maximal de connexions qui peuvent

être suivies, et un volume élevé de requêtes DNS peut dépasser les connexions et provoquer une limitation et une perte de requête. Le suivi des connexions AWS est le comportement par défaut pour surveiller l'état du trafic passant par les groupes de sécurité (SGs). L'utilisation du suivi des SGs connexions permet de réduire le débit du trafic, mais vous pouvez implémenter des connexions non suivies pour réduire les frais généraux et améliorer les performances. Pour plus d'informations, voir Connexions non suivies.

Si le suivi des connexions est appliqué en utilisant des règles de groupe de sécurité restrictives ou si les requêtes sont acheminées via Network Load Balancer (voir Connexions suivies automatiquement), le nombre maximum de requêtes par seconde et par adresse IP pour un point de terminaison peut être inférieur à 1 500.

Recommandations relatives aux règles du groupe de sécurité d'entrée et de sortie pour le point de terminaison entrant du résolveur

Règles d'entrée		
Type de protocole	Numéro de port	IP Source
TCP	53	0.0.0.0/0
UDP	53	0.0.0.0/0
Règles de sortie		
Type de protocole	Numéro de port	IP de destination
TCP	Tous	0.0.0.0/0
UDP	Tous	0.0.0.0/0

Recommandations relatives aux règles des groupes de sécurité d'entrée et de sortie pour le point de terminaison Resolver sortant

Règles d'entrée		
Type de protocole	Numéro de port	IP Source
TCP	Tous	0.0.0.0/0

UDP	Tous	0.0.0.0/0
Règles de sortie		
Type de protocole	Numéro de port	IP de destination
TCP	Tous	0.0.0.0/0
UDP	Tous	0.0.0.0/0

Points de terminaison Resolver

Pour les clients utilisant un point de terminaison de résolveur entrant, la capacité de l'elastic network interface sera affectée si vous avez plus de 40 000 combinaisons d'adresses IP et de ports uniques générant le trafic DNS.

Haute disponibilité pour les points de terminaison Resolver

Lorsque vous créez vos points de terminaison entrants Route 53 Resolver, Route 53 exige que vous créiez au moins deux adresses IP auxquelles les résolveurs DNS de votre réseau transmettront les requêtes. Vous devez également spécifier les adresses IP dans au moins deux zones de disponibilité pour la redondance.

Si vous avez besoin que plus d'un point de terminaison d'Interface réseau Elastic soit disponible à tout moment, nous vous recommandons de créer au moins une interface réseau de plus que nécessaire, afin de vous assurer que vous disposez d'une capacité supplémentaire pour gérer d'éventuelles surtensions de trafic. L'interface réseau supplémentaire assure également la disponibilité pendant les opérations de service, telles que la maintenance ou les mises à niveau.

Pour plus d'informations, consultez cet article de blog détaillé : Comment atteindre la haute disponibilité du DNS avec les points de terminaison Route 53 Resolver et. Valeurs à spécifier lors de la création ou de la modification de points de terminaison entrants

Parcours de zone DNS

Le parcours de zone est une attaque visant à récupérer tous le contenu signé par DNSSEC. Si l'équipe Route 53 Resolver détecte un modèle de trafic correspondant à ceux générés lorsque les zones DNS sont parcourues sur votre point de terminaison, elle limitera le trafic sur ce dernier. Par conséquent, vous pouvez observer un pourcentage élevé de vos requêtes DNS expirer.

Si vous constatez une réduction de la capacité de vos terminaux et que vous pensez que le terminal a été limité par erreur, rendez-vous https://console.aws.amazon.com/support/ sur home#/ pour créer un dossier d'assistance.

Bonnes pratiques relatives aux vérifications de l'état d'Amazon Route 53

Une configuration efficace des bilans de santé est essentielle pour maintenir une infrastructure hautement disponible et résiliente. Voici quelques bonnes pratiques à prendre en compte lors de la configuration et de la gestion des bilans de santé d'Amazon Route 53 :

1. Utilisez des adresses IP élastiques pour les points de terminaison de contrôle de l'état :
   - Utilisez des adresses IP élastiques pour vos points de terminaison de contrôle de santé afin de garantir une surveillance cohérente.
   - Si vous n'utilisez plus d' EC2 instance Amazon, pensez à supprimer tous les bilans de santé associés afin d'éviter tout risque de sécurité ou toute compromission des données.

   Pour plus d'informations, voirValeurs que vous spécifiez lors de la création ou de la mise à jour de surveillances de l'état.
2. Configurez les intervalles de contrôle de santé appropriés :
   - Définissez des intervalles de contrôle de santé en fonction des exigences de votre application et de la criticité des ressources surveillées.
   - Des intervalles plus courts permettent de détecter plus rapidement les défaillances, mais peuvent augmenter les coûts de la Route 53 et alourdir vos ressources.
   - Des intervalles plus longs réduisent les coûts et la charge de ressources, mais peuvent retarder la détection des défaillances.

   Pour plus d'informations, voirConfiguration avancée (option « Monitor an endpoint » uniquement).
3. Implémenter les notifications d'alarme :
   - Configurez Amazon CloudWatchalarms pour recevoir des notifications lorsque les tests de santé échouent ou se rétablissent.
   - Définissez des seuils d'alarme appropriés en fonction des exigences de votre application et du comportement attendu de vos ressources.
   - Intégrez les notifications à vos processus de surveillance et de réponse aux incidents.

Pour plus d'informations, voirSurveillance des bilans de santé à l'aide CloudWatch.

4. Utilisez les régions de bilan de santé de manière stratégique :
   - Choisissez les régions de contrôle de santé en fonction de la répartition géographique de vos utilisateurs et de vos ressources.
   - Envisagez d'utiliser plusieurs régions de contrôle de santé pour les ressources critiques afin d'améliorer la fiabilité et de réduire l'impact des pannes régionales.
5. Surveillez les journaux et les indicateurs des bilans de santé :
   - Consultez régulièrement les journaux et CloudWatch indicateurs des bilans de santé de Route 53 pour identifier les problèmes potentiels ou les goulots d'étranglement liés aux performances
   - Analysez les raisons de l'échec du bilan de santé et prenez les mesures appropriées pour résoudre les problèmes sous-jacents.
6. Mettez en œuvre des stratégies de basculement et de retour en arrière :
   - Tirez parti des politiques de routage en cas de basculement de Route 53 pour acheminer automatiquement le trafic vers des ressources saines en cas de panne.
   - Planifiez et testez les processus de basculement et de reprise afin de garantir une transition fluide en cas de panne et de reprise.

   Pour plus d'informations, voirConfiguration du basculement DNS.
7. Passez régulièrement en revue et mettez à jour les bilans de santé :
   - Mettez à jour les points de terminaison, les intervalles et les seuils d'alarme du bilan de santé selon les besoins afin de maintenir une surveillance et des performances optimales.

En suivant ces bonnes pratiques, vous pouvez exploiter efficacement les bilans de santé d'Amazon Route 53 pour surveiller l'état et la disponibilité de vos ressources, garantissant ainsi une infrastructure fiable et performante pour vos applications et services.

Quotas

Les demandes d'API Amazon Route 53 et les entités sont assujetties aux quotas suivants (anciennement appelés « limites »).

Rubriques

- Utilisation de Service Quotas pour afficher et gérer les quotas
- Quotas applicables aux entités
- Quotas maximums pour les demandes d'API

Utilisation de Service Quotas pour afficher et gérer les quotas

Vous pouvez utiliser le service Service Quotas pour afficher les quotas et demander des augmentations de quota pour de nombreux services AWS . Pour plus d'informations, consultez le Guide de l'utilisateur Service Quotas. (Vous pouvez actuellement utiliser Service Quotas pour consulter et gérer les quotas de domaines, Route 53 et Route 53 Resolver.)

> **Note**
>
> Pour consulter les quotas et demander leur augmentation pour Route 53, vous devez remplacer la région par USA Est (Virginie du Nord). Pour consulter les quotas et demander leur augmentation pour Resolver, spécifiez la région applicable.

Quotas applicables aux entités

Les entités Amazon Route 53 sont soumises aux quotas suivants.

Pour plus d'informations sur les quotas actuels (anciennement appelés « limites »), consultez les actions Route 53 suivantes :

- GetAccountLimit— Obtient des quotas sur les bilans de santé, les zones hébergées, les ensembles de délégation réutilisables, les politiques de flux de trafic et les enregistrements de politiques de flux de trafic
- GetHostedZoneLimit— Obtient des quotas sur les enregistrements d'une zone hébergée et sur Amazon VPCs que vous pouvez associer à une zone hébergée privée

- GetReusableDelegationSetLimit— Obtient le quota du nombre de zones hébergées que vous pouvez associer à un ensemble de délégations réutilisable

Rubriques

- Quotas applicables aux domaines
- Quotas applicables aux zones hébergées
- Quotas applicables aux enregistrements
- Quotas sur Route 53 Resolver
- Quotas applicables aux surveillances de l'état
- Quotas applicables aux configurations de journalisation des requêtes
- Quotas applicables aux stratégies de flux de trafic et d'enregistrements de stratégies
- Quotas applicables aux ensembles de délégations réutilisables
- Quotas sur les profils de la Route 53

Quotas applicables aux domaines

Entité	Quota
Domaines	20* par compte AWS Demander l'augmentation du quota

*La limite s'élève à 20 pour les nouveaux clients à partir de mars 2021.

Si vous avez un compte existant et que votre limite par défaut s'élève désormais à 50, celle-ci reste à 50.

Quotas applicables aux zones hébergées

Entité	Quota
Zones hébergées	Quota initial de 500 par AWS compte, mais vous pouvez demander un quota plus élevé si nécessaire.

Entité	Quota
	Demander l'augmentation du quota
Zones hébergées pouvant utiliser le même ensemble de délégations réutilisables	100 Demander l'augmentation du quota
Amazon VPCs que vous pouvez associer à une zone hébergée privée par zone hébergée	300 Si vous souhaitez plus de 300 associations, nous vous recommandons d'utiliser les profils Route 53. Pour de plus amples informations, veuillez consulter Que sont les profils Amazon Route 53 ?.
Zones hébergées privées auxquelles vous pouvez associer un VPC	Pas de quota *
Autorisations que vous pouvez créer afin de pouvoir associer VPCs celles créées par un compte à une zone hébergée créée par un autre compte	1 000
Nombre de clés de signature principales (KSK) que vous pouvez créer par zone hébergée	2

* Vous pouvez associer un VPC à une ou à toutes les zones hébergées privées que vous contrôlez via vos AWS comptes. Supposons, par exemple, que vous disposiez de trois AWS comptes et que le quota par défaut de 500 zones hébergées soit atteint pour tous les trois. Si vous créez 500 zones hébergées privées pour les trois comptes, vous pouvez associer un VPC à l'ensemble des 1 500 zones hébergées privées.

Quotas applicables aux enregistrements

Entité	Quota
Enregistrements	10 000 par zone hébergée Demander l'augmentation du quota Pour un quota supérieur à 10 000 registres dans une zone hébergée, des frais supplémentaires sont facturés. Pour plus d'informations, consultez Amazon Route 53 Pricing (Facturation Amazon Route 53).
Enregistrement dans un ensemble d'enregistrements	400 par ensemble d'enregistrements
Enregistrements de géolocalisation, de latence, de réponse à valeurs multiples, pondérés et basés sur IP	100 enregistrements ayant le même nom et le même type
Enregistrements de proximité géographique	30 enregistrements ayant le même nom et le même type
Collections CIDR	5 par Compte AWS. Demander l'augmentation du quota
Blocs CIDR	1000 par collection CIDR. Demander l'augmentation du quota

Quotas sur Route 53 Resolver

Cette section inclut tous les quotas Route 53 Resolver

Quotas sur Route 53 Resolver

Utilisez la procédure suivante pour augmenter les quotas pour Route 53 Resolver.

Pour augmenter les quotas Resolver

1. Ouvrez la console Service Quotas sur https://console.aws.amazon.com/servicequotas/home/services/route53resolver/quotas.
2. Accédez à la région où vous souhaitez augmenter la limite.
3. Sélectionnez le Quota name (Nom du quota) Route 53 Resolver que vous souhaitez augmenter.
4. Sélectionnez Request quota increase (Demander une augmentation de quota), entrez la valeur du quota, puis sélectionnez Request (Demander).

Quotas sur les points de terminaison Route 53 Resolver

Entité	Quota
Points de terminaison par région AWS	4 par AWS compte Demander l'augmentation du quota
Adresses IP par point de terminaison	6 Demander l'augmentation du quota
Adresses IP par règle	6
Règles par AWS région	1000 par AWS compte Demander l'augmentation du quota
Associations entre les règles et VPCs par AWS région	2000 par AWS compte Demander l'augmentation du quota

Entité	Quota
Requêtes UDP par seconde et par adresse IP sur un point de terminaison	10 000*

* Chaque adresse IP d'un point de terminaison peut traiter jusqu'à 10 000 requêtes DNS UDP par seconde (QPS). Le nombre de requêtes DNS par seconde varie en fonction du type de requête, de la taille de la réponse, de l'état des serveurs de noms cibles, des temps de réponse aux requêtes, de la latence de l'aller-retour, et du protocole en cours d'utilisation. Par exemple, les requêtes adressées à un serveur de noms cible qui est lent à répondre peuvent réduire considérablement la capacité de l'interface réseau. En outre, pour garantir une haute disponibilité, Route 53 Resolver génère des requêtes sortantes redondantes pour chaque requête DNS qu'il reçoit. Par conséquent, le nombre de requêtes par seconde de chaque interface réseau sortante ne correspond pas au nombre de requêtes par seconde envoyé à Route 53 Resolver. Utilisez CloudWatch des métriques pour mesurer le nombre de requêtes envoyées à chaque interface réseau. Pour de plus amples informations, veuillez consulter Métriques pour les adresses IP Resolver. Si votre taux de requête maximal dépasse 50 % de la capacité d'une interface réseau du point de terminaison, vous pouvez ajouter d'autres interfaces réseau pour augmenter la capacité du point de terminaison.

Les connexions établies via des applications telles que Network Load Balancer et AWS Lambda (pour une liste complète, voir Connexions suivies automatiquement) sont automatiquement suivies, même si la configuration du groupe de sécurité ne nécessite pas de suivi par ailleurs.

Si le suivi des connexions est appliqué en utilisant des règles de groupe de sécurité restrictives ou si les requêtes sont acheminées via Network Load Balancer, le nombre maximum de requêtes par seconde et par adresse IP pour un point de terminaison entrant peut être inférieur à 1 500.

Quotas sur les journaux de requête Route 53 Resolver

Entité	Quota
Configurations du journal des requêtes par AWS région	20
	100

Entité	Quota
Associations VPC des configurations de journal de requête par région AWS *	
Associations VPC des configurations de journal de requête par compte par région AWS (partagées avec RAM) pour le compte avec lequel la configuration a été partagée.	100

* Il s'agit d'une limite stricte. Vous pouvez créer une autre configuration de journal des requêtes dans la même configuration Région AWS et y VPCs associer 100 autres.

Quotas sur le pare-feu DNS Route 53 Resolver

Entité	Quota
Nombre de groupes de règles associés à un VPC pour un seul compte par région AWS	5
Nombre de domaines de pare-feu DNS dans un seul fichier Amazon S3 pour un seul compte par AWS région	250 000 Demander l'augmentation du quota
Nombre de groupes de règles de pare-feu DNS pour un seul compte par AWS région	1 000 Demander l'augmentation du quota
Nombre de règles au sein d'un groupe de règles pour un seul compte par AWS région	100 Demander l'augmentation du quota

Entité	Quota
Nombre de listes de domaines pour un seul compte par AWS région	1 000 Demander l'augmentation du quota
Le nombre maximum de domaines que vous pouvez spécifier dans toutes les listes de domaines pour un seul compte par AWS région	100 000 Demander l'augmentation du quota

Quotas sur le résolveur sur Outpost

Entité	Quota
Limite d'instances du résolveur sur Outpost	6 (avec un minimum de 4 requis)

Les types d'instances Resolver on Outpost et le nombre de requêtes DNS par seconde que chaque type d'instance peut prendre en charge :

Type d’instance	Requêtes par seconde
c5.large	Jusqu'à 7 000
c5.xlarge	Jusqu'à 12 000
c5.2xlarge	Jusqu'à 24 000
c5.4xlarge	Jusqu'à 56 000
c5d.large	Jusqu'à 7 000
c5d.xlarge	Jusqu'à 12 000

Type d’instance	Requêtes par seconde
c5d.2xlarge	Jusqu'à 24 000
c5d.4xlarge	Jusqu'à 56 000
m5.large	Jusqu'à 7 000
m5.xlarge	Jusqu'à 12 000
m5.2xlarge	Jusqu'à 24 000
m5.4xlarge	Jusqu'à 56 000
m5d.large	Jusqu'à 7 000
m5d.xlarge	Jusqu'à 12 000
m5d.2xlarge	Jusqu'à 24 000
m5d.4xlarge	Jusqu'à 56 000
r5.large	Jusqu'à 7 000
r5.xlarge	Jusqu'à 12 000
r5.2xlarge	Jusqu'à 24 000
r5.4xlarge	Jusqu'à 56 000

Type d’instance	Requêtes par seconde
r5d.large	Jusqu'à 7 000
r5d.xlarge	Jusqu'à 12 000
r5d.2xlarge	Jusqu'à 24 000
r5d.4xlarge	Jusqu'à 56 000

Types d'instances de point de terminaison Resolver on Outpost et nombre de requêtes DNS par seconde que chaque type d'instance peut prendre en charge :

Type d’instance	Requêtes par seconde
c5.large	Jusqu'à 5 000
c5.xlarge	Jusqu'à 10 000
c5.2xlarge	Jusqu'à 18 000
c5.4xlarge	Jusqu'à 30 000
c5d.large	Jusqu'à 5 000
c5d.xlarge	Jusqu'à 10 000
c5d.2xlarge	Jusqu'à 18 000
c5d.4xlarge	Jusqu'à 30 000
m5.large	Jusqu'à 5 000

Type d’instance	Requêtes par seconde
m5.xlarge	Jusqu'à 10 000
m5.2xlarge	Jusqu'à 18 000
m5.4xlarge	Jusqu'à 30 000
m5d.large	Jusqu'à 5 000
m5d.xlarge	Jusqu'à 10 000
m5d.2xlarge	Jusqu'à 18 000
m5d.4xlarge	Jusqu'à 30 000
r5.large	Jusqu'à 5 000
r5.xlarge	Jusqu'à 10 000
r5.2xlarge	Jusqu'à 18 000
r5.4xlarge	Jusqu'à 30 000
r5d.large	Jusqu'à 5 000
r5d.xlarge	Jusqu'à 10 000
r5d.2xlarge	Jusqu'à 18 000

Type d'instance	Requêtes par seconde
r5d.4xlarge	Jusqu'à 30 000

Quotas applicables aux surveillances de l'état

Entité	Quota
Surveillance de l'état	200 bilans de santé actifs par AWS compte Demander l'augmentation du quota
Vérifications de l'état enfants qu'une surveillance de l'état calculée peut surveiller	255
Longueur totale maximale des en-têtes dans la réponse adressée à une demande de surveillance de l'état	16 384 octets (16 K)

Quotas applicables aux configurations de journalisation des requêtes

Entité	Quota
Configurations de journalisation des requêtes	1 par zone hébergée

Quotas applicables aux stratégies de flux de trafic et d'enregistrements de stratégies

Entité	Quota
Stratégies de trafic Pour plus d'informations sur le flux de trafic Route 53, consultez Utiliser Traffic Flow pour acheminer le trafic DNS.	50 par AWS compte Demander l'augmentation du quota
Versions de stratégie de trafic	1 000 par stratégie de trafic
Enregistrements de politique de trafic (appelés « instances de politique » dans l'API Route 53 AWS SDKs, AWS Command Line Interface, et AWS Tools for Windows PowerShell)	5 par AWS compte Demander l'augmentation du quota

Quotas applicables aux ensembles de délégations réutilisables

Entité	Quota
Ensembles de délégations réutilisables	100 par AWS compte Demander l'augmentation du quota

Quotas sur les profils de la Route 53

Entité	Quota

Entité	Quota
Nombre de profils Route 53 par Compte AWS région	5 Demander l'augmentation du quota
Numéro VPCs pouvant être associé à un profil	1 000 Demander l'augmentation du quota
Nombre de groupes de règles de pare-feu DNS par profil	5
Nombre de règles de résolution par profil	1 000 Demander l'augmentation du quota
Nombre de zones hébergées privées par profil	1 000 Demander l'augmentation du quota

Quotas maximums pour les demandes d'API

Les demandes d'API Amazon Route 53 sont soumises aux quotas suivants.

Rubriques

- Nombre d'éléments et de caractères dans les demandes ChangeResourceRecordSets
- Fréquence des demandes d'API Amazon Route 53
- Fréquence des demandes d'API Route 53 Resolver

Nombre d'éléments et de caractères dans les demandes `ChangeResourceRecordSets`

`ResourceRecord` éléments

Une requête ne peut pas contenir plus de 1 000 `ResourceRecord` éléments (y compris les registres d'alias). Lorsque la valeur de l'élément `Action` est `UPSERT`, chaque élément `ResourceRecord` est comptabilisé deux fois.

Nombre maximum de caractères

La somme des caractères (y compris les espaces) dans tous les éléments `Value` d'une demande ne peut pas dépasser 32 000 caractères. Lorsque la valeur de l'élément `Action` est `UPSERT`, chaque caractère dans un élément `Value` est comptabilisé deux fois.

Fréquence des demandes d'API Amazon Route 53

Toutes les requêtes d'API Amazon Route 53

Pour l'Amazon Route 53, APIs cinq demandes par seconde et par AWS compte. Si vous envoyez plus de cinq demandes par seconde, Amazon Route 53 renvoie une erreur HTTP 400 (`Bad request`). L'en-tête de réponse inclut également un élément `Code` avec une valeur `Throttling` et un élément `Message` avec une valeur `Rate exceeded`.

> **Note**
>
> Si votre application dépasse cette limite, nous vous recommandons d'implémenter une interruption exponentielle pour les nouvelles tentatives. Pour plus d'informations, consultez Tentatives sur l'erreur et backoff exponentiel AWS dans la Référence générale d'Amazon Web Services.

`ChangeResourceRecordSets` requêtes

Si Route 53 ne peut pas traiter une demande avant l'arrivée de la suivante, il rejette les demandes suivantes relatives à la même zone hébergée et renvoie une erreur HTTP 400 (`Bad request`). L'en-tête de réponse inclut également un élément `Code` avec une valeur `PriorRequestNotComplete` et un élément `Message` avec une valeur `The request was rejected because Route 53 was still processing a prior request.`

`CreateHealthCheck` requêtes

Vous pouvez envoyer une `CreateHealthCheck` demande toutes les 2 secondes par Compte AWS.

Fréquence des demandes d'API Route 53 Resolver

Toutes les demandes

Cinq demandes par seconde, par AWS compte et par région. Si vous envoyez plus de cinq requêtes par seconde dans une région, Resolver renvoie une erreur HTTP 400 (`Bad request`). L'en-tête de réponse inclut également un élément `Code` avec une valeur `Throttling` et un élément `Message` avec une valeur `Rate exceeded`.

> **Note**
>
> Si votre application dépasse cette limite, nous vous recommandons d'implémenter une interruption exponentielle pour les nouvelles tentatives. Pour plus d'informations, consultez Error Retries and Exponential Backoff in AWS(Tentatives sur l'erreur et backoff exponentiel)) dans Référence générale d'Amazon Web Services.

Informations connexes

Les ressources connexes suivantes peuvent s'avérer utiles lors de l'utilisation de ce service.

Rubriques

- AWS ressources
- Bibliothèques et outils tiers
- Interfaces utilisateur graphiques

AWS ressources

Plusieurs guides, forums et autres ressources utiles sont disponibles à partir d'Amazon Web Services.

- Référence API Amazon Route 53 : un guide de référence qui comprend l'emplacement du schéma, les descriptions complètes des actions d'API, des paramètres et des types de données, ainsi que la liste des erreurs que le service renvoie.
- AWS::Route53::RecordSet Tapez le guide de AWS CloudFormation l'utilisateur : propriété permettant d'utiliser Amazon Route 53 AWS CloudFormation afin de créer des noms DNS personnalisés pour vos AWS CloudFormation piles.
- Forums de discussion : un forum communautaire qui permet aux développeurs d'échanger à propos de questions techniques liées à Route 53.
- AWS Support Center — Ce site rassemble des informations sur vos récents cas d'assistance et les résultats des AWS bilans de santé et fournit des liens vers des forums de discussion, des informations techniques FAQs, le tableau de bord de santé des services et des informations sur les plans de AWS support.
- AWS Informations sur le support Premium : page Web principale contenant des informations sur le support AWS Premium one-on-one, un canal d'assistance rapide destiné à vous aider à créer et à exécuter des applications sur les services AWS d'infrastructure.
- Contactez-nous – Liens pour les questions sur votre compte ou votre facturation. Pour les questions techniques, veuillez utiliser les forums de discussion ou les liens de support ci-dessus.
- Informations sur le produit Route 53 : la page web principale pour toutes les informations sur Route 53, y compris les fonctions, la tarification, etc.

- Cours et ateliers — Liens vers des cours spécialisés et basés sur des rôles, ainsi que des ateliers à votre rythme pour vous aider à perfectionner vos AWS compétences et à acquérir une expérience pratique.
- AWS Centre pour développeurs : découvrez les didacticiels, téléchargez des outils et découvrez les événements AWS destinés aux développeurs.
- AWS Outils de développement : liens vers des outils de développement SDKs, des boîtes à outils IDE et des outils de ligne de commande pour le développement et la gestion d' AWS applications.
- Centre de ressources pour la mise en route : découvrez comment configurer votre application Compte AWS, rejoindre la AWS communauté et lancer votre première application.
- Tutoriels pratiques — Suivez les step-by-step didacticiels pour lancer votre première application sur AWS.
- AWS Livres blancs : liens vers une liste complète de livres AWS blancs techniques, traitant de sujets tels que l'architecture, la sécurité et l'économie, rédigés par des architectes de AWS solutions ou d'autres experts techniques.
- AWS Support Centre — Le centre de création et de gestion de vos AWS Support dossiers. Comprend également des liens vers d'autres ressources utiles, telles que des forums, des informations techniques FAQs, l'état de santé des services et AWS Trusted Advisor.
- Support— La principale page Web contenant des informations sur Support un one-on-one canal d'assistance à réponse rapide pour vous aider à créer et à exécuter des applications dans le cloud.
- Contactez-nous : point de contact central pour toute question relative à la facturation AWS , à votre compte, aux événements, à des abus ou à d'autres problèmes.
- AWS Conditions du site — Informations détaillées sur nos droits d'auteur et notre marque commerciale ; votre compte, votre licence et l'accès au site ; et d'autres sujets.

Bibliothèques et outils tiers

Outre les AWS ressources, vous pouvez trouver une variété d'outils et de bibliothèques tiers compatibles avec Amazon Route 53.

- AmazonRoute53 AppsScript (via Webos-Goodies)

  Gestion des feuilles de calcul Google d'Amazon Route 53.
- AWS Composant pour .NET (via SprightlySoft)

SprightlySoft Composant .NET pour Amazon Web Services prenant en charge les opérations REST et Route 53.

- Téléchargement de l'API Boto (via github)

  Interface Python Boto Python pour Amazon web Services.

- cli53 (via github)

  Interface de ligne de commande pour Route 53.

- API Cloud Dasein

  API basée sur Java.

- R53.py (via github)

  Gère une version canonique de vos configurations DNS sous le contrôle de code source et calcule les modifications minimales requises pour procéder à un changement de configuration.

- route53d

  Serveur frontal DNS pour l'API Route 53 (active le transfert de zone incrémentiel [IXFR]).

- Route53Manager (via github)

  Interface basée sur le web.

- Ruby Fog (via github)

  Bibliothèque des services de cloud Ruby.

- WebService: :Amazon : :Route53 (via le CPAN)

  Interface Perl pour l'API Amazon Route 53.

Interfaces utilisateur graphiques

Les outils tiers suivants fournissent des interfaces utilisateur graphiques (GUIs) permettant de travailler avec Amazon Route 53 :

- R53 Fox
- Ylastic

Historique du document

Les entrées ci-après décrivent les modifications importantes apportées à chaque version de la documentation Route 53. Pour recevoir les notifications de mise à jour de cette documentation, abonnez-vous à un flux RSS.

Rubriques

- Sorties en 2025
- 2024 sorties
- Versions de 2023
- Publications de 2022
- Versions de 2021
- Versions de 2020
- Versions 2018
- Versions 2017
- Versions 2016
- Versions 2015
- Versions 2014
- Versions 2013
- Version 2012
- Versions 2011
- Version 2010

Sorties en 2025

26 juin 2025

Ajouté `ResolverEndpointCapacityStatus` à l'espace de `AWS/Route53Resolver` noms. Pour de plus amples informations, veuillez consulter Métriques pour les points de terminaison Resolver.

25 juin 2025

Amazon Route 53 prend désormais en charge les enregistrements d'alias pour les points de terminaison de domaine personnalisés du service VPC Lattice. Pour de plus amples informations, veuillez consulter Acheminement du trafic vers le point de terminaison du domaine du service Amazon VPC Lattice.

24 juin 2025

Vous pouvez désormais utiliser la délégation entrante et sortante avec Route 53 Resolver. Pour de plus amples informations, veuillez consulter Comment les résolveurs DNS de votre réseau réacheminent les requêtes DNS vers les points de terminaison Route 53 Resolver.

01 juin 2025

Autorisations ajoutées pour `cloudwatch:GetMetricDatatag:GetResources`,`es:ListDomainNames`,`es:DescribeDomains`, `cloudfront:GetConnectionGroup` et`lightsail:GetContainerServices`. Ces autorisations vous permettent de récupérer jusqu'à 500 indicateurs de CloudWatch santé, jusqu'à 100 noms de bilans de santé, d'obtenir la configuration du domaine pour les domaines Amazon OpenSearch Service spécifiés et de répertorier les noms de tous les domaines Amazon OpenSearch Service détenus par l'utilisateur actuel dans la région active, de récupérer les distributions CloudFront multi-locataires et d'obtenir les services de conteneur Lightsail. Pour de plus amples informations, veuillez consulter AWS politique gérée : AmazonRoute 53 FullAccess.

28 avril 2025

Vous pouvez désormais associer les points de terminaison VPC de l'interface aux profils Route 53. Pour de plus amples informations, veuillez consulter Associer les points de terminaison VPC de l'interface à un profil Route 53.

28 avril 2025

Vous pouvez désormais ajouter un enregistrement d'alias à un locataire CloudFront de distribution. Pour de plus amples informations, veuillez consulter Acheminement du trafic vers une CloudFront distribution Amazon à l'aide de votre nom de domaine.

27 février 2025

Mise à jour du guide Route 53 avec la nouvelle expérience de console pour Traffic Flow. Pour plus d’informations, consultez Création et gestion des stratégies de trafic et Création et gestion des enregistrements de stratégie.

14 janvier 2025

Amazon Route 53 prend désormais en charge les enregistrements d'alias pour les points de terminaison de domaine personnalisés du OpenSearch Service. Pour de plus amples informations, veuillez consulter Acheminement du trafic vers le point de terminaison du domaine Amazon OpenSearch Service.

13 janvier 2025

Les résultats du pare-feu DNS Route 53 Resolver ont été ajoutés au Security Hub. Pour de plus amples informations, veuillez consulter Envoi des résultats depuis le pare-feu DNS Route 53 Resolver vers Security Hub.

2024 sorties

15 novembre 2024

Ajout de Route 53 Resolver DNS Firewall Advanced, un nouvel ensemble de fonctionnalités du pare-feu DNS Route 53 Resolver qui vous permet d'identifier et de bloquer le trafic DNS associé à des menaces DNS avancées, telles que le tunneling DNS et les menaces basées sur l'algorithme de génération de domaines (DGA). Pour de plus amples informations, veuillez consulter Route 53 Resolver DNS Firewall Advanced.

29 octobre 2024

Ajout de la prise en charge des types d'enregistrement DNS HTTPS, SSHFP, SVCB et TLSA. Pour de plus amples informations, veuillez consulter Types d'enregistrements DNS pris en charge.

3 octobre 2024

Ajout de la prise en charge de l'indication du nom de service (SNI) pour les points de terminaison DoH sortants du résolveur. Pour de plus amples informations, veuillez consulter Valeurs à spécifier lors de la création ou de la modification de règles.

3 septembre 2024

Vous pouvez désormais utiliser la condition `route53:VPCs` de politique pour accorder un accès détaillé à la gestion des associations de zones hébergées à. VPCs Pour de plus amples informations, veuillez consulter Utilisation de conditions de politique IAM pour un contrôle d’accès précis.

27 août 2024

`AmazonRoute53ProfilesFullAccess`autorisations ajoutées pour `GetProfilePolicy` et`PutProfilePolicy`. Il s'agit d'actions IAM avec autorisation uniquement. Si ces autorisations ne sont pas accordées à un principal IAM, une erreur se produira lors de la tentative de partage du profil à l'aide du AWS RAM service. Pour de plus amples informations, veuillez consulter AWS politique gérée : AmazonRoute 53 ProfilesFullAccess.

27 août 2024

`AmazonRoute53ProfilesReadOnlyAccess`autorisation ajoutée pour`GetProfilePolicy`. Il s'agit d'une action IAM avec autorisation uniquement. Si cette autorisation n'est pas accordée à un principal IAM, une erreur se produira lors de la tentative d'accès à la politique du profil à l'aide du AWS RAM service. Pour de plus amples informations, veuillez consulter AWS politique gérée : AmazonRoute 53 ProfilesReadOnlyAccess.

5 août 2024

Ajout d'un identifiant de déclaration (Sid) pour identifier de manière unique la politique géréeAmazonRoute53ResolverFullAccess. Pour de plus amples informations, veuillez consulter AWS politique gérée : AmazonRoute 53 ResolverFullAccess.

5 août 2024

Ajout d'un identifiant de déclaration (Sid) pour identifier de manière unique la politique géréeAmazonRoute53ResolverReadOnlyAccess. Pour de plus amples informations, veuillez consulter AWS politique gérée : AmazonRoute 53 ResolverReadOnlyAccess.

18 juillet 2024

Mise à jour de l'intégralité du guide Route 53 avec la nouvelle interface de console pour les bilans de santé. Pour de plus amples informations, veuillez consulter Création, mise à jour et suppression de surveillances de l'état.

30 avril 2024

Vous pouvez désormais décider si une règle de pare-feu DNS inspectera (par défaut) ou fera confiance à la chaîne de redirection DNS. Pour plus d'informations, consultez Composants et paramètres de Route 53 Resolver DNS Firewall et Paramètres de règles dans le pare-feu DNS.

22 avril 2024

Vous pouvez désormais utiliser les profils Route 53 pour partager des configurations spécifiques au DNS avec de nombreuses personnes VPCs et avec AWS des comptes. Pour de plus amples informations, veuillez consulter Que sont les profils Amazon Route 53 ?.

22 avril 2024

Ajout des politiques gérées `AmazonRoute53ProfilesReadOnlyAccess` et de l'octroi `AmazonRoute53ProfilesFullAccess` d'un accès complet et en lecture seule aux profils Amazon Route 53. Pour de plus amples informations, veuillez consulter AWS politiques gérées pour Amazon Route 53.

5 février 2024

Vous pouvez désormais utiliser Amazon EventBridge pour les alertes en temps réel grâce au pare-feu DNS. Pour de plus amples informations, veuillez consulter Gestion des événements du pare-feu DNS Route 53 Resolver à l'aide de Amazon EventBridge.

9 janvier 2024

Vous pouvez désormais utiliser le type de requête DNS comme valeur facultative pour la règle de pare-feu DNS afin de différencier la réponse de la règle pour un type de requête DNS spécifique. Pour plus d'informations, consultez Composants et paramètres de Route 53 Resolver DNS Firewall et Paramètres de règles dans le pare-feu DNS.

9 janvier 2024

Vous pouvez désormais utiliser l'enregistrement rapide ou l'assistant de création d'enregistrement pour créer des enregistrements de routage de géoproximité. Pour plus d'informations, consultez Routage par géoproximité, Valeurs spécifiques aux enregistrements de géoproximité et Valeurs spécifiques aux enregistrements d'alias de géoproximité.

Versions de 2023

20 décembre 2023

Vous pouvez désormais utiliser le DNS via HTTPS avec les points de terminaison Route 53 Resolver. Pour de plus amples informations, veuillez consulter Choisir des protocoles pour les points de terminaison.

20 juillet 2023

Amazon Route 53 on Outposts est désormais disponible sur AWS Outposts racks. Cela inclut un résolveur qui met en cache toutes les requêtes DNS provenant de AWS Outposts. Vous pouvez également configurer une connectivité hybride entre un résolveur Outpost et un résolveur DNS sur site lorsque vous déployez des points de terminaison entrants et sortants. Pour de plus amples informations, veuillez consulter Qu'est-ce que Amazon Route 53 sur Outposts ?.

19 juillet 2023

Vous pouvez désormais utiliser les zones locales avec un routage de proximité géographique (flux de trafic uniquement) une fois que vous les avez activées. Pour plus d'informations, voir Routage par géoproximité et Format du document de la stratégie de trafic.

22 mars 2023

Mise à jour de l'intégralité du guide Route 53 avec la nouvelle console pour les domaines. Vous pouvez également utiliser la nouvelle expérience de console pour transférer un domaine d'un domaine Compte AWS à un autre Compte AWS. Pour plus d'informations, consultez Enregistrement d'un nouveau domaine et Transfert de domaines.

10 mars 2023

Vous pouvez désormais vous connecter à vos ressources en utilisant ou en utilisant IPv4 des IPv6 points de terminaison à double pile avec. Amazon Route 53 Resolver Pour plus d'informations, consultez Valeurs à spécifier lors de la création ou de la modification de points de terminaison entrants et Valeurs à spécifier lors de la création ou de la modification de points de terminaison sortants.

Publications de 2022

21 septembre 2022

Vous pouvez désormais utiliser des conditions de politique pour donner aux utilisateurs un accès précis à la mise à jour des ensembles d'enregistrements de ressources dans Amazon Route 53. Pour de plus amples informations, veuillez consulter Utilisation de conditions de politique IAM pour un contrôle d'accès précis.

30 août 2022

Amazon Route 53 prend désormais en charge les enregistrements d'alias pour les AWS App Runner services créés après le 1er août 2022. Pour de plus amples informations, veuillez consulter Acheminement du trafic vers un AWS App Runner service.

1 juin 2022

L'option de routage basé sur IP est désormais disponible dans Amazon Route 53. Pour de plus amples informations, veuillez consulter Routage basé sur IP.

16 mars 2022

Les options de routage basées sur la géolocalisation et la latence sont désormais prises en charge pour les zones hébergées privées dans Amazon Route 53. Pour de plus amples informations, veuillez consulter Remarques sur l'utilisation des zones hébergées privées.

25 janvier 2022

Le processus de changement de propriétaire pour .com.au et .net.au TLDs a été simplifié pour inclure la réponse à deux e-mails (envoyés par les anciens et les nouveaux inscrits) et n'inclut pas le remplissage de formulaires. Pour plus d'informations, consultez .com.au (Australie) et .net.au (Australie).

Versions de 2021

26 octobre 2021

Ajout de la prise en charge de la désactivation des règles DNS inverses par défaut avec Amazon Route 53. Vous pouvez désormais désactiver la création de ces règles et transférer des requêtes pour les espaces de noms DNS inverses vers des serveurs externes comme vous le souhaitez. Pour de plus amples informations, veuillez consulter Règles de transfert pour les requêtes DNS inverses dans Resolver.

1er septembre 2021

Ajout d'une nouvelle rubrique de démarrage qui explique comment créer des CloudFront distributions Amazon pour un site Web statique. Pour de plus amples informations, veuillez consulter Utiliser une CloudFront distribution Amazon pour diffuser un site Web statique.

14 juillet 2021

J'ai commencé AWS à suivre les politiques gérées pour Amazon Route 53. Pour de plus amples informations, veuillez consulter AWS politiques gérées pour Amazon Route 53.

31 mars 2021

Ajout du pare-feu DNS Route 53 Resolver. Avec le pare-feu DNS, vous pouvez protéger les requêtes DNS sortantes provenant de votre VPCs. Pour de plus amples informations, veuillez consulter Utilisation du pare-feu DNS pour filtrer le trafic DNS sortant.

Versions de 2020

17 décembre 2020

Ajout du support pour la signature DNSSEC pour Route 53 Resolver. Pour de plus amples informations, veuillez consulter Configuration de la signature DNSSEC dans Amazon Route 53.

Ajout du support pour la validation DNSSEC pour Route 53 Resolver. Pour de plus amples informations, veuillez consulter Activation de la validation DNSSEC dans Amazon Route 53.

23 septembre 2020

Mise à jour de l'intégralité du guide Route 53 avec la nouvelle console. Pour de plus amples informations, veuillez consulter Qu'est-ce qu'Amazon Route 53 ?.

1 septembre 2020

Ajout du support des journaux de requête Resolver. Pour de plus amples informations, veuillez consulter Journalisation des requêtes Resolver.

Versions 2018

20 décembre 2018

Vous pouvez créer des enregistrements d'alias Route 53 qui acheminent le trafic vers API Gateway APIs ou vers les points de terminaison de l'interface Amazon VPC. Pour de plus amples informations, veuillez consulter Valeur/acheminer le trafic vers.

28 novembre 2018

Route 53 Auto Naming (également connu sous le nom de Service Discovery) est désormais un service distinct AWS Cloud Map. Pour plus d'informations, consultez le Manuel du développeur AWS Cloud Map.

19 novembre 2018

Vous pouvez également utiliser le Resolver Route 53 pour configurer la résolution DNS entre votre VPC et votre réseau via une connexion VPN ou Direct Connect. (Resolver est le nouveau nom pour le service DNS récursif qui est fourni à tous les clients par défaut dans Amazon Virtual Private Cloud [Amazon VPC].) Cela vous permet de transférer des requêtes DNS depuis les résolveurs sur votre réseau vers Route 53 Resolver. Resolver vous permet également de transférer des requêtes pour certains noms de domaine (example.com) et noms de sous-domaines (api.example.com) depuis un VPC vers les résolveurs sur votre réseau. Pour de plus amples informations, veuillez consulter Qu'est-ce que c'est Amazon Route 53 Resolver ?.

7 novembre 2018

Lorsque vous utilisez Route 53 Traffic Flow et le routage de proximité géographique, vous pouvez utiliser une carte interactive pour visualiser la façon dont vos utilisateurs finaux seront acheminés vers vos points de terminaison à travers le monde. Pour de plus amples informations, veuillez consulter Affichage d'une carte montrant l'effet des paramètres de proximité géographique.

18 octobre 2018

Vous pouvez utiliser l'API et la console Route 53 pour désactiver temporairement une surveillance de l'état Route 53. Cela vous permet de facilement suspendre la surveillance d'un point de terminaison, tel qu'un serveur web, pour pouvoir y effectuer sa maintenance sans déclencher d'alarmes ou produire de journaux ou de messages de statut inutiles. Pour plus d'informations, consultez « Désactivé » dans la rubrique Valeurs que vous spécifiez lors de la création ou de la mise à jour de surveillances de l'état. Cette fonctionnalité est disponible pour les trois types de bilans de santé de Route 53 : les bilans de santé qui surveillent un terminal, les bilans de santé qui surveillent les autres bilans de santé et les bilans de santé qui surveillent une CloudWatch alarme.

13 mars 2018

Si vous utilisez la dénomination automatique, vous pouvez désormais utiliser un outil de surveillance de l'état tiers pour évaluer l'état de vos ressources. Cela s'avère utile lorsqu'une ressource n'est pas disponible sur Internet, par exemple, parce que l'instance est dans un VPC

Amazon. Pour plus d'informations, consultez HealthCheckCustomConfigle manuel Amazon Route 53 API Reference.

9 mars 2018

IAM comprend désormais des stratégies gérées pour la dénomination automatique. Pour de plus amples informations, veuillez consulter AWS politiques gérées pour Amazon Route 53.

6 février 2018

Vous pouvez désormais configurer la dénomination automatique pour créer des enregistrements d'alias qui acheminent le trafic vers des équilibreurs de charge ELB ou pour créer des enregistrements CNAME. Pour plus d'informations, consultez la section Attributs de la documentation de l'RegisterInstanceAPI dans le manuel Amazon Route 53 API Reference.

Versions 2017

5 décembre 2017

Vous pouvez désormais utiliser l'API de dénomination automatique Route 53 pour allouer des instances pour des microservices. La dénomination automatique vous permet de créer automatiquement des enregistrements DNS et, éventuellement, des surveillances de l'état basées sur un modèle que vous définissez. Pour plus d'informations, consultez Qu'est-ce que AWS Cloud Map ? dans le Guide AWS Cloud Map du développeur.

16 novembre 2017

Vous pouvez désormais obtenir par programme les quotas actuels applicables aux ressources Route 53 telles que les zones hébergées et les surveillances d'état, mais également le nombre de chacune des ressources que vous utilisez actuellement. Pour plus d'informations, consultez GetAccountLimitGetHostedZoneLimit, et GetReusableDelegationSetLimitdans le manuel Amazon Route 53 API Reference.

3 octobre 2017

Route 53 est désormais un service éligible HIPAA. Pour de plus amples informations, veuillez consulter Validation de la conformité pour Amazon Route 53.

29 septembre 2017

Vous pouvez désormais vérifier par programme si un domaine peut être transféré vers Route 53. Pour plus d'informations, consultez CheckDomainTransferabilityle manuel Amazon Route 53 API Reference.

11 septembre 2017

Vous pouvez désormais créer des registres d'alias Route 53 qui acheminent le trafic Internet vers des dispositifs d'équilibrage de charge réseau Elastic Load Balancing. Pour plus d'informations sur les enregistrements d'alias, consultez Choix entre des enregistrements avec ou sans alias.

7 septembre 2017

Si vous utilisez Route 53 en tant que service DNS public faisant autorité, vous pouvez désormais journaliser des requêtes DNS que Route 53 reçoit. Pour de plus amples informations, veuillez consulter Journalisation des requêtes DNS publiques.

1 septembre 2017

Si vous utilisez le flux de trafic Route 53, vous pouvez désormais utiliser le routage de proximité géographique, ce qui vous permet d'acheminer le trafic en fonction de la distance physique entre vos utilisateurs et vos ressources. Vous pouvez également acheminer un trafic plus ou moins important pour chaque ressource en spécifiant une valeur d'écart positive ou négative. Pour de plus amples informations, veuillez consulter Routage par géoproximité.

le 21 août 2017

Vous pouvez désormais utiliser Route 53 pour créer des registres d'autorisation d'autorité de certification (CAA), ce qui vous permet de spécifier les autorités de certification qui peuvent émettre des certificats pour vos domaines et sous-domaines. Pour de plus amples informations, veuillez consulter Type d'enregistrement CAA.

18 août 2017

Vous pouvez désormais transférer un grand nombre de domaines vers Route 53 à l'aide de la console Route 53. Pour de plus amples informations, veuillez consulter Transfert d'un enregistrement de domaine vers Amazon Route 53.

4 août 2017

Lorsque vous enregistrez un domaine, les registres de certains domaines de premier niveau (TLDs) vous demandent de vérifier que vous avez indiqué une adresse e-mail valide pour le contact du titulaire. Vous pouvez désormais envoyer l'e-mail de vérification et obtenir la confirmation que vous avez vérifié avec succès l'adresse e-mail pendant le processus d'inscription du domaine. Pour de plus amples informations, veuillez consulter Enregistrement d'un nouveau domaine.

21 juin 2017

Si vous souhaitez acheminer le trafic approximativement de manière aléatoire vers plusieurs ressources, comme des serveurs web, vous pouvez désormais créer un registre de réponse multivaleur pour chaque ressource et, facultativement, associer une surveillance d'état Route 53 à chaque registre. Route 53 répond aux requêtes DNS avec jusqu'à huit registres sains par réponse à chaque requête DNS, et fournit des réponses distinctes aux différents résolveurs DNS. Pour de plus amples informations, veuillez consulter Multivalue answer routing (Routage de réponse multivaleur).

10 avril 2017

Lorsque vous utilisez la console Route 53 pour transférer un enregistrement de domaine vers Route 53, vous pouvez désormais choisir l'une des options suivantes afin d'associer les serveurs de noms pour le service DNS pour le domaine avec l'enregistrement de domaine transféré :

- Utilisation des serveurs de noms pour une zone hébergée Route 53 que vous choisissez
- Utiliser les serveurs de noms pour le service DNS actuel pour le domaine
- Utiliser les serveurs de noms que vous spécifiez

Route 53 associe automatiquement ces serveurs de noms à l'enregistrement de domaine transféré.

Versions 2016

21 novembre 2016

Vous pouvez désormais créer des bilans de santé qui utilisent IPv6 des adresses pour vérifier l'état des terminaux. Pour de plus amples informations, veuillez consulter Création et mise à jour de surveillances de l'état.

15 novembre 2016

Vous pouvez désormais utiliser une action d'API Route 53 pour associer un VPC Amazon que vous avez créé à l'aide d'un compte avec une zone hébergée privée que vous avez créée à l'aide d'un autre compte. Pour de plus amples informations, veuillez consulter Associer un Amazon VPC et une zone hébergée privée que vous avez créée avec différents comptes AWS.

30 août 2016

Cette version de Route 53 introduit les nouvelles fonctions suivantes :

- Registres de pointeur d'autorité de nom (NAPTR) – Vous pouvez désormais créer des registres NAPTR, qui sont utilisés par les applications DDDS (Dynamic Delegation Discovery System) pour convertir une valeur en une autre ou remplacer une valeur par une autre. Par exemple, une utilisation courante consiste à convertir des numéros de téléphone en SIP URIs. Pour de plus amples informations, veuillez consulter Type d'enregistrement NAPTR.
- Outil de test de requête DNS – Vous pouvez désormais simuler des requêtes DNS pour un registre et déterminer la valeur renvoyée par Route 53. Pour les enregistrements de géolocalisation et de latence, vous pouvez également simuler des requêtes provenant d'une adresse IP de and/or client de résolution DNS particulière afin de savoir quelle réponse Route 53 renverrait à un client possédant cette adresse IP de résolveur and/or . Pour de plus amples informations, veuillez consulter Vérification des réponses DNS à partir de Route 53.

11 août 2016

Avec cette version, vous pouvez créer des enregistrements d'alias qui acheminent le trafic vers des équilibreurs Application Load Balancers ELB. Le processus est le même que pour les équilibreurs de charges classiques. Pour de plus amples informations, veuillez consulter Valeur/acheminer le trafic vers.

9 août 2016

Cette version de Route 53 prend désormais en charge DNSSEC pour l'enregistrement de domaine. Le protocole DNSSEC vous permet de protéger votre domaine contre les attaques par usurpation du DNS, également appelées attaques. man-in-the-middle Pour de plus amples informations, veuillez consulter Configuration du protocole DNSSEC pour un domaine.

7 juillet 2016

Vous pouvez désormais étendre manuellement la période d'enregistrement de domaine et enregistrer un domaine avec une période d'enregistrement initiale plus longue que la période d'enregistrement minimum indiquée par le registre. Pour de plus amples informations, veuillez consulter Extension de la période d'enregistrement pour un domaine.

6 juillet 2016

Si vous êtes un client AISPL avec une adresse de contact en Inde, vous pouvez désormais utiliser Route 53 pour enregistrer des domaines. Pour plus d'informations, consultez la page Gestion de votre compte en Inde.

26 mai 2016

Cette version de Route 53 introduit les nouvelles fonctions suivantes :

- Rapport de facturation de domaine – Vous pouvez désormais télécharger un rapport qui répertorie tous les frais d'enregistrement de domaine, par domaine, pour une durée déterminée. Le rapport inclut toutes les opérations d'enregistrement de domaines payantes, y compris l'enregistrement de domaines, le transfert de domaines vers Route 53, le renouvellement de l'enregistrement de domaines et (pour certaines TLDs) le changement de propriétaire d'un domaine. Pour plus d'informations, consultez la documentation de suivante :
  - Console Route 53 – Consultez Téléchargement d'un rapport de facturation de domaine
  - API Route 53 — Voir ViewBillingla référence de l'API Amazon Route 53.
- Nouveau TLDs — Vous pouvez désormais enregistrer les domaines suivants TLDs : .college, .consulting, .host, .name, .online, .republican, .rocks, .sucks, .trade, .website et .uk. Pour de plus amples informations, veuillez consulter Domaines que vous pouvez enregistrer avec Amazon Route 53.
- Nouveau APIs pour l'enregistrement de domaine : pour les opérations nécessitant la confirmation de la validité de l'adresse e-mail du contact du titulaire, telles que l'enregistrement d'un nouveau domaine, vous pouvez désormais déterminer par programme si le contact du titulaire a cliqué sur le lien contenu dans l'e-mail de confirmation et, dans le cas contraire, si le lien est toujours valide. Vous pouvez également demander par programmation l'envoi d'un nouvel e-mail de confirmation. Pour plus d'informations, consultez la documentation suivante dans le document Référence de l'API Amazon Route 53 :
  - GetContactReachabilityStatus
  - ResendContactReachabilityEmail

5 avril 2016

Cette version de Route 53 introduit les nouvelles fonctions suivantes :

- Contrôles de santé basés sur CloudWatch des métriques — Vous pouvez désormais créer des bilans de santé basés sur l'état d'alarme de n'importe quelle CloudWatch métrique. Cela permet de vérifier l'état des points de terminaison qui ne peuvent pas être vérifiés à l'aide d'une surveillance d'état Route 53 standard, comme les instances au sein d'un Amazon Virtual Private Cloud (VPC) qui n'ont que des adresses IP privées. Pour plus d'informations, consultez la documentation de suivante :
  - Console Route 53 – Consultez Surveillance d'une alarme CloudWatch dans la rubrique « Valeurs que vous spécifiez lors de la création ou de la mise à jour des surveillances d'état ».
  - API Route 53 — Voir CreateHealthChecket UpdateHealthCheckdans le manuel Amazon Route 53 API Reference.

- Emplacements de surveillance d'état configurables – Vous pouvez désormais choisir les régions de surveillance d'état Route 53 qui vérifient l'état de vos ressources, ce qui réduit la charge des surveillances d'état sur le point de terminaison. Cette fonction est utile si vos clients sont concentrés dans une région géographique, ou dans un petit nombre de régions. Pour plus d'informations, consultez la documentation de suivante :
  - Console Route 53 – Consultez Configuration avancée (option « Monitor an endpoint » uniquement) dans la rubrique « Valeurs que vous spécifiez lors de la création ou de la mise à jour des surveillances d'état ».
  - API Route 53 — Consultez l'`Regions`élément pour CreateHealthChecket UpdateHealthCheckdans le manuel de référence de l'API Amazon Route 53.
- Basculement dans des zones hébergées privées – Vous pouvez désormais créer des registres de basculement et d'alias de basculement dans une zone hébergée privée. Lorsque vous associez cette fonction aux surveillances d'état basées sur les métriques, vous pouvez configurer le basculement DNS même pour les points de terminaison qui ont uniquement des adresses IP privées et qui ne peuvent pas être vérifiés à l'aide des surveillances d'état Route 53 standard. Pour plus d'informations, consultez la documentation de suivante :
  - Console Route 53 – Consultez Configuration du basculement dans une zone hébergée privée.
  - API Route 53 — Voir ChangeResourceRecordSetsla référence de l'API Amazon Route 53.
- Registres d'alias dans les zones hébergées privées – Jusqu'à maintenant, vous pouviez uniquement créer des registres d'alias qui acheminaient les requêtes DNS uniquement vers d'autres registres Route 53 de la même zone hébergée. Cette version vous permet également de créer des registres d'alias qui acheminent les requêtes DNS vers des environnements Elastic Beanstalk qui ont des sous-domaines régionalisés, des équilibreurs de charge Elastic Load Balancing et des compartiments Amazon S3. (Vous ne pouvez toujours pas créer d'enregistrements d'alias qui acheminent les requêtes DNS vers une CloudFront distribution.) Pour plus d'informations, consultez la documentation de suivante :
  - Console Route 53 – Consultez Choix entre des enregistrements avec ou sans alias.
  - API Route 53 — Voir ChangeResourceRecordSetsla référence de l'API Amazon Route 53.

23 février 2016

Lorsque vous créez ou mettez à jour des surveillances d'état HTTPS, vous pouvez désormais configurer Route 53 pour envoyer le nom d'hôte au point de terminaison lors de la négociation TLS. Cela permet au point de terminaison de répondre à la demande HTTPS avec le SSL/TLS certificat applicable. Pour plus d'informations, consultez la description du SNI dans le

Configuration avancée (option « Monitor an endpoint » uniquement) champ « Valeurs que vous spécifiez lorsque vous créez ou mettez à jour des bilans de santé ». Pour plus d'informations sur la façon d'activer le SNI lorsque vous utilisez l'API pour créer ou mettre à jour un bilan de santé, consultez CreateHealthChecket UpdateHealthCheckdans le manuel Amazon Route 53 API Reference.

27 janvier 2016

Vous pouvez désormais enregistrer des domaines pour plus de 100 domaines de premier niveau supplémentaires (TLDs) tels que .accountants, .band et .city. Pour obtenir la liste complète des produits pris en charge TLDs, consultezDomaines que vous pouvez enregistrer avec Amazon Route 53.

19 janvier 2016

Vous pouvez désormais créer des registres d'alias qui acheminent le trafic vers des environnements Elastic Beanstalk. Pour plus d'informations sur la création de registres à l'aide de la console Route 53, consultez Création d'enregistrements à l'aide de la console Amazon Route 53. Pour plus d'informations sur l'utilisation de l'API pour créer des enregistrements, consultez ChangeResourceRecordSetsle manuel Amazon Route 53 API Reference.

Versions 2015

3 décembre 2015

La console Route 53 inclut désormais un éditeur visuel qui vous permet de créer rapidement des configurations de routage complexes qui utilisent une combinaison de politiques de routage pondéré, de latence, de basculement et de géolocalisation Route 53. Vous pouvez ensuite associer la configuration avec un ou plusieurs noms de domaine (par exemple, example.com) ou noms de sous-domaine (par exemple, www.example.com), dans la même zone hébergée ou dans plusieurs zones hébergées. En outre, vous pouvez restaurer les mises à jour si la nouvelle configuration ne fonctionne pas comme vous l'aviez prévu. La même fonctionnalité est disponible en utilisant l'API Route 53 AWS SDKs, le AWS CLI, et AWS Tools for Windows PowerShell. Pour plus d'informations sur l'utilisation de l'éditeur visuel, consultez Utiliser Traffic Flow pour acheminer le trafic DNS. Pour plus d'informations sur l'utilisation de l'API pour créer des configurations de flux de trafic, consultez le document Référence de l'API Amazon Route 53.

19 octobre 2015

Cette version de Route 53 introduit les nouvelles fonctions suivantes :

- Enregistrement de domaines pour les domaines .com et .net par Amazon Registrar, Inc. — Amazon est désormais un bureau d'enregistrement accrédité par l'ICANN pour les domaines de premier niveau .com et .net () TLDs via Amazon Registrar, Inc. Lorsque vous utilisez Route 53 pour enregistrer un domaine .com ou .net, Amazon Registrar sera le bureau d'enregistrement officiel et sera répertorié comme le « bureau d'enregistrement sponsor » dans les résultats de votre requête Whois. Pour plus d'informations sur l'utilisation de Route 53 pour enregistrer des domaines, consultez Enregistrement et gestion des domaines à l'aide d'Amazon Route 53.
- Protection de la confidentialité des domaines .com et .net – Lorsque vous enregistrez un domaine .com ou .net avec Route 53, toutes vos informations personnelles, y compris le nom et le prénom, sont désormais masquées. Le prénom et le nom ne sont pas masqués pour les autres domaines que vous enregistrez avec Route 53. Pour plus d'informations sur la protection de la confidentialité, consultez Activation ou désactivation de la protection de la confidentialité pour les informations de contact pour un domaine.

15 septembre 2015

Cette version de Route 53 introduit les nouvelles fonctions suivantes :

- Surveillances d'état calculées – Vous pouvez désormais créer des surveillances d'état dont le statut est déterminé par le statut de l'état d'autres surveillances d'état. Pour de plus amples informations, veuillez consulter Création et mise à jour de surveillances de l'état. Consultez également le manuel CreateHealthCheckde référence des API Amazon Route 53.
- Mesures de la latence des surveillances d'état – Vous pouvez désormais configurer Route 53 pour mesurer la latence entre les outils de surveillance d'état et votre point de terminaison. Les données de latence apparaissent dans CloudWatch les graphiques Amazon de la console Route 53. Pour activer les mesures de la latence pour les nouvelles surveillances de l'état, consultez le paramètre Latency measurements dans la section Configuration avancée (option « Monitor an endpoint » uniquement) de la rubrique Valeurs que vous spécifiez lors de la création ou de la mise à jour de surveillances de l'état. (Vous ne pouvez pas activer les mesures de la latence pour des surveillances de l'état existantes.) Consultez MeasureLatencyégalement la rubrique du manuel CreateHealthCheckAmazon Route 53 API Reference.
- Mises à jour du tableau de bord des bilans de santé dans la console Route 53 — Le tableau de bord de surveillance des bilans de santé a été amélioré de différentes manières, notamment CloudWatch des graphiques pour surveiller le temps de latence entre les vérificateurs de santé Route 53 et vos terminaux. Pour de plus amples informations, veuillez consulter Surveillance du statut de la vérification de l'état et obtention de notifications.

3 mars 2015

Le Guide du développeur Amazon Route 53 explique désormais comment configurer des serveurs de noms en marque blanche pour les zones hébergées Route 53. Pour de plus amples informations, veuillez consulter Configuration de serveurs de noms en marque blanche.

26 février 2015

Vous pouvez désormais utiliser l'API Route 53 pour répertorier les zones hébergées associées à un AWS compte par ordre alphabétique de nom. Vous pouvez également obtenir le nombre de zones hébergées associées à un compte. Pour plus d'informations, consultez ListHostedZonesByNameet consultez GetHostedZoneCountle manuel Amazon Route 53 API Reference.

11 février 2015

Cette version de Route 53 introduit les nouvelles fonctions suivantes :

- Statut de surveillance d'état – La page relative aux surveillances d'état dans la console Route 53 comprend désormais une colonne Status (Statut) qui vous permet d'afficher le statut général de l'ensemble de vos surveillances d'état. Pour de plus amples informations, veuillez consulter Affichage du statut des vérifications de l'état et motifs des échecs de vérifications de l'état.
- Intégration avec AWS CloudTrail — Route 53 fonctionne désormais CloudTrail pour capturer des informations sur chaque demande que votre AWS compte envoie à l'API Route 53. L'intégration de Route 53 vous CloudTrail permet de déterminer quelles demandes ont été adressées à l'API Route 53, l'adresse IP source à partir de laquelle chaque demande a été faite, qui a fait la demande, quand elle a été faite, etc. Pour de plus amples informations, veuillez consulter Journalisation des appels d'API Amazon Route 53 avec AWS CloudTrail.
- Alarmes rapides pour les bilans de santé : lorsque vous créez un bilan de santé à l'aide de la console Route 53, vous pouvez désormais créer simultanément une CloudWatch alarme Amazon pour le bilan de santé et spécifier qui avertir lorsque Route 53 considère que le terminal est en mauvais état pendant une minute. Pour de plus amples informations, veuillez consulter Création et mise à jour de surveillances de l'état.
- Balisage pour les zones hébergées et les domaines – Vous pouvez désormais affecter des balises, couramment utilisées pour l'allocation de coûts, aux zones hébergées et domaines Route 53. Pour de plus amples informations, veuillez consulter Balisage des ressources Amazon Route 53.

5 février 2015

Vous pouvez désormais utiliser la console Route 53 pour mettre à jour les informations de contact pour un domaine. Pour de plus amples informations, veuillez consulter Valeurs que vous spécifiez lorsque vous enregistrez ou transférez un domaine.

22 janvier 2015

Vous pouvez désormais spécifier des noms de domaine internationaux lorsque vous enregistrez un nouveau nom de domaine avec Route 53. (Route 53 prenait déjà en charge les noms de domaine internationaux pour les zones hébergées et les registres.) Pour de plus amples informations, veuillez consulter Format de nom de domaine DNS.

Versions 2014

25 novembre 2014

Avec cette version, vous pouvez désormais modifier le commentaire que vous avez spécifié pour une zone hébergée à sa création. Dans la console, il vous suffit de cliquer sur l'icône en forme de crayon en regard du champ Comment et d'entrer une nouvelle valeur. Pour plus d'informations sur la modification du commentaire à l'aide de l'API Route 53, consultez UpdateHostedZoneCommentla référence de l'API Amazon Route 53.

5 novembre 2014

Cette version de Route 53 introduit les nouvelles fonctions suivantes :

- DNS privé VPCs créé à l'aide du service Amazon Virtual Private Cloud — Vous pouvez désormais utiliser Route 53 pour gérer vos noms de domaine internes VPCs sans exposer les données DNS à l'Internet public. Pour de plus amples informations, veuillez consulter Utilisation des zones hébergées privées.
- Motifs d'échec des surveillances d'état – Vous pouvez désormais voir le statut actuel d'une surveillance d'état sélectionnée, ainsi que des détails sur les raisons de l'échec de la surveillance d'état, comme indiqué par chacun des outils de surveillance d'état Route 53. Le statut inclut le code de statut HTTP, et les motifs d'échec incluent des informations sur les nombreux types d'échec, par exemple les échecs de correspondance de chaînes et les délais de réponse. Pour de plus amples informations, veuillez consulter Affichage du statut des vérifications de l'état et motifs des échecs de vérifications de l'état.
- Ensembles de délégations réutilisables – Vous pouvez désormais appliquer le même ensemble de quatre serveurs de noms faisant autorité, appelés collectivement « ensemble de

délégations », à plusieurs zones hébergées qui correspondent à différents noms de domaine. Cette fonction simplifie considérablement le processus de migration des services DNS vers Route 53 et la gestion d'un grand nombre de zones hébergées. Pour utiliser des ensembles de délégations réutilisables, vous devez actuellement utiliser l'API Route 53 ou un kit SDK AWS . Pour plus d'informations, consultez la référence d'API Amazon Route 53.

- Routage de géolocalisation amélioré — Nous avons encore amélioré la précision du routage de géolocalisation en ajoutant la prise en charge de l' edns-client-subnetextension d'EDNS0. Pour de plus amples informations, veuillez consulter Routage de géolocalisation.
- Support de signature v4 – Vous pouvez désormais signer toutes les demandes d'API Route 53 à l'aide de la version 4 de la Signature. Pour plus d'informations, consultez Signature des demandes d'API Route 53 dans le document Référence de l'API Amazon Route 53.

31 juillet 2014

Avec cette version, vous pouvez désormais effectuer les opérations suivantes :

- Enregistrez des noms de domaine avec Route 53. Pour de plus amples informations, veuillez consulter Enregistrement et gestion des domaines à l'aide d'Amazon Route 53.
- Configurez Route 53 pour répondre aux requêtes DNS en fonction de l'emplacement géographique d'origine des requêtes. Pour de plus amples informations, veuillez consulter Routage de géolocalisation.

2 juillet 2014

Avec cette version, vous pouvez désormais effectuer les opérations suivantes :

- Modifier la plupart des valeurs des surveillances de l'état. Pour de plus amples informations, veuillez consulter Création, mise à jour et suppression de surveillances de l'état.
- Utilisez l'API Route 53 pour obtenir une liste des plages d'adresses IP que les outils de surveillance d'état Route 53 utilisent pour vérifier l'état de vos ressources. Vous pouvez utiliser ces adresses IP pour configurer vos règles de routeur et de pare-feu afin de permettre aux outils de surveillance de l'état de vérifier l'état de vos ressources. Pour plus d'informations, consultez GetCheckerIpRangesle manuel Amazon Route 53 API Reference.
- Attribuer des balises d'allocation de coûts pour les surveillances de l'état, ce qui vous permet également de leur attribuer un nom. Pour de plus amples informations, veuillez consulter Attribution de noms et balisage des surveillances de l'état.
- Utilisez l'API Route 53 pour connaître le nombre de bilans de santé associés à votre AWS compte. Pour plus d'informations, consultez GetHealthCheckCountle manuel Amazon Route 53 API Reference.

30 avril 2014

Avec cette version, vous pouvez désormais créer des surveillances de l'état et utiliser un nom de domaine au lieu d'une adresse IP pour spécifier le point de terminaison. Cela est utile lorsque l'adresse IP d'un point de terminaison n'est pas fixe ou est desservie par plusieurs instances IPs, telles que des instances Amazon EC2 ou Amazon RDS. Pour de plus amples informations, veuillez consulter Création et mise à jour de surveillances de l'état.

En outre, certaines informations concernant l'utilisation de l'API Route 53 anciennement incluses dans le Guide du développeur Amazon Route 53 ont été déplacées. Désormais, l'intégralité de la documentation relative à l'API figure dans le document Référence de l'API Amazon Route 53.

18 avril 2014

Avec cette version, Route 53 transmet une valeur différente dans l'en-tête `Host` lorsque la valeur Port de la surveillance d'état est 443 et que la valeur Protocol (Protocole) est HTTPS. Au cours d'une surveillance d'état, Route 53 transmet désormais au point de terminaison un en-tête `Host` qui contient la valeur du champ Host Name (Nom d'hôte). Si vous avez créé la surveillance de l'état à l'aide de l'action d'API `CreateHealthCheck`, il s'agit de la valeur de l'élément `FullyQualifiedDomainName`.

Pour de plus amples informations, veuillez consulter Création, mise à jour et suppression de surveillances de l'état.

9 avril 2014

Avec cette version, vous pouvez désormais afficher le pourcentage d'outils de surveillance d'état Route 53 qui indiquent actuellement qu'un point de terminaison est sain.

En outre, le comportement de la métrique Health Check Status sur Amazon indique CloudWatch désormais uniquement zéro (si votre terminal était en mauvais état pendant une période donnée) ou un (si le point de terminaison était en bon état pendant cette période). La métrique n'affiche plus de valeurs entre 0 et 1, ce qui reflétait la part des surveillances d'état Route 53 signalant le point de terminaison comme sain.

Pour de plus amples informations, veuillez consulter Surveillance des bilans de santé à l'aide CloudWatch.

18 février 2014

Cette version de Route 53 introduit les fonctions suivantes :

- Seuil de basculement de surveillance d'état : vous pouvez désormais spécifier le nombre de surveillances d'état consécutives pour lesquelles un point de terminaison doit échouer pour que Route 53 considère le point de terminaison comme non sain. Vous devez affecter une valeur entre 1 et 10. Un point de terminaison non sain doit réussir le même nombre de vérifications pour être considéré comme sain. Pour de plus amples informations, veuillez consulter Comment Amazon Route 53 détermine si une surveillance de l'état est saine.
- Intervalle de demande de surveillance d'état : vous pouvez désormais spécifier la fréquence à laquelle Route 53 envoie des requêtes à un point de terminaison pour déterminer si le point de terminaison est sain. Les valeurs valides sont 10 secondes et 30 secondes. Pour de plus amples informations, veuillez consulter Comment Amazon Route 53 détermine si une surveillance de l'état est saine.

30 janvier 2014

Cette version de Route 53 introduit les fonctions suivantes :

- Surveillances d'état de la correspondance de chaîne HTTP et HTTPS : Route 53 prend désormais en charge les surveillances d'état qui déterminent l'état d'un point de terminaison en fonction de l'aspect d'une chaîne spécifiée dans le corps de la réponse. Pour de plus amples informations, veuillez consulter Comment Amazon Route 53 détermine si une surveillance de l'état est saine.
- Surveillances d'état HTTPS : Route 53 prend désormais en charge les surveillances d'état pour les sites web sécurisés n'utilisant que SSL. Pour de plus amples informations, veuillez consulter Comment Amazon Route 53 détermine si une surveillance de l'état est saine.
- **`UPSERT`** pour l'action d'API **`ChangeResourceRecordSets`** : lors de la création ou de la modification d'enregistrements à l'aide de l'action d'API `ChangeResourceRecordSets`, vous pouvez désormais utiliser l'action `UPSERT` pour créer un nouvel enregistrement s'il n'en existe aucun avec un nom et un type donnés, ou mettre à jour un enregistrement existant. Pour plus d'informations, consultez ChangeResourceRecordSetsle manuel Amazon Route 53 API Reference.

7 janvier 2014

Avec cette version, Route 53 prend désormais en charge les surveillances d'état qui déterminent l'état d'un point de terminaison en fonction de la présence ou de l'absence d'une chaîne spécifiée dans le corps de la réponse. Pour de plus amples informations, veuillez consulter Comment Amazon Route 53 détermine si une surveillance de l'état est saine.

Versions 2013

14 août 2013

Avec cette version, Route 53 prend désormais en charge la création de registres en important un fichier de zone au format BIND. Pour de plus amples informations, veuillez consulter Création d'enregistrements par importation d'un fichier de zone.

En outre, CloudWatch les mesures relatives aux bilans de santé de Route 53 ont été intégrées à la console Route 53 et rationalisées. Pour de plus amples informations, veuillez consulter Surveillance des bilans de santé à l'aide CloudWatch.

26 juin 2013

Dans cette version, Route 53 prend en charge l'intégration des contrôles de santé aux CloudWatch métriques afin que vous puissiez effectuer les opérations suivantes :

- Vérifier qu'une surveillance de l'état est correctement configurée.
- Passer en revue l'état d'un point de terminaison sur une période donnée.
- Configurez CloudWatch pour envoyer une alerte Amazon Simple Notification Service (Amazon SNS) lorsque tous les vérificateurs de santé de Route 53 considèrent que le point de terminaison que vous avez spécifié n'est pas sain.

Pour de plus amples informations, veuillez consulter Surveillance des bilans de santé à l'aide CloudWatch.

11 juin 2013

Avec cette version, Route 53 prend en charge la création d'enregistrements d'alias qui acheminent les requêtes DNS vers des noms de domaine alternatifs pour les CloudFront distributions Amazon. Vous pouvez utiliser cette fonction pour les noms de domaine alternatifs de la zone apex (example.com) et les noms de domaine alternatifs pour les sous-domaines (www.example.com). Pour de plus amples informations, veuillez consulter Acheminement du trafic vers une CloudFront distribution Amazon à l'aide de votre nom de domaine.

30 mai 2013

Avec cette version, Route 53 prend en charge l'évaluation de l'état des équilibreurs de charge ELB et des instances Amazon EC2 associées. Pour de plus amples informations, veuillez consulter Création de bilans de santé pour Amazon Route 53 .

28 mars 2013

La documentation relative aux surveillances de l'état et au basculement a été réécrite afin d'en améliorer l'utilisation. Pour de plus amples informations, veuillez consulter Création de bilans de santé pour Amazon Route 53 .

11 février 2013

Avec cette version, Route 53 prend désormais en charge le basculement et les surveillances d'état. Pour de plus amples informations, veuillez consulter Création de bilans de santé pour Amazon Route 53 .

Version 2012

21 mars 2012

Avec cette version, Route 53 vous permet de créer des registres de latence. Pour de plus amples informations, veuillez consulter Routage basé sur la latence.

Versions 2011

21 décembre 2011

Dans cette version, la console Route 53 vous AWS Management Console permet de créer un enregistrement d'alias en choisissant un Elastic Load Balancer dans une liste au lieu de saisir manuellement l'ID de zone hébergée et le nom DNS de l'équilibreur de charge. La nouvelle fonctionnalité est documentée dans le Guide du développeur Amazon Route 53.

16 novembre 2011

Dans cette version, vous pouvez utiliser la console Route 53 AWS Management Console pour créer et supprimer des zones hébergées, ainsi que pour créer, modifier et supprimer des enregistrements. Cette nouvelle fonctionnalité est documentée dans le Guide du développeur Amazon Route 53, le cas échéant.

18 octobre 2011

Le Guide de mise en route Amazon Route 53 a été intégré dans le Guide du développeur Amazon Route 53, et le Guide du développeur a été réorganisé pour améliorer la facilité d'utilisation.

24 mai 2011

Cette version d'Amazon Route 53 introduit les registres d'alias, qui vous permettent de créer des alias pour la zone apex), les registres pondérés, une nouvelle API (2011-05-05) et un contrat de niveau de service. En outre, après six mois en version bêta, Route 53 est désormais mis à la disposition générale. Pour plus d'informations, consultez la page du produit Amazon Route 53 et Choix entre des enregistrements avec ou sans alias dans le Guide du développeur Amazon Route 53.

Version 2010

5 décembre 2010

Ce document est la première version du Guide du développeur Amazon Route 53.

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.