aws

Guide du développeur

Application Recovery Controller Amazon Route 53

Application Recovery Controller Amazon Route 53: Guide du développeur

Table of Contents

Qu'est-ce qu'Amazon Route 53 Application Recovery Controller ?

Amazon Route 53 Application Recovery Controller (Route 53 ARC) vous aide à préparer et à effectuer une restauration plus rapide pour les applications qui s'exécutent sur ce dernier AWS. Route 53 ARC fournit deux ensembles de fonctionnalités : la restauration par zones à disponibilité multiple (AZ), qui inclut le décalage zonal et le décalage automatique zonal, et la restauration multirégionale, qui inclut le contrôle du routage et le contrôle de préparation. Avec Route 53 ARC, vous pouvez tirer parti d'outils de restauration hautement disponibles pour atténuer rapidement les défaillances qui ont un impact sur vos applications multirégionales ou multi-AZ. Vous pouvez également utiliser le contrôle du niveau de préparation pour savoir si vos applications et ressources sont prêtes à être restaurées.

L'infrastructure cloud AWS mondiale assure la tolérance aux pannes et la résilience, chacune étant Région AWS composée de plusieurs zones de disponibilité entièrement isolées. Route 53 ARC fonctionne au sein de cette AWS structure pour aider vos applications à être résilientes.

Restauration multi-AZ

Si vous avez des applications conçues pour tirer parti des zones de disponibilité AWS, vous pouvez rapidement isoler et corriger les défaillances de l'AZ en utilisant le changement de zone. Le changement de zone vous permet de remédier aux défaillances d'une zone de disponibilité (AZ), en déplaçant temporairement le trafic vers une ressource prise en charge hors d'une zone de disponibilité (AZ) vers des zones de disponibilité saines dans le. Région AWS Le lancement d'un changement de zone permet à votre application de se rétablir rapidement, par exemple après un déploiement de code incorrect par un développeur ou une défaillance AWS dans une seule zone de disponibilité. En éloignant le trafic, vous réduisez l'impact sur les clients qui utilisent votre application en cas de problème dans une zone de zones géographiques.

Vous pouvez commencer un changement de zone pour n'importe quelle ressource prise en charge sur votre compte dans une région. AWS les services enregistrent automatiquement AWS les ressources prises en charge avec le décalage de zone dans Route 53 ARC, afin que vous puissiez commencer un changement de zone à tout moment.

L'autoshift zonal est une fonctionnalité de Route 53 ARC que vous pouvez activer pour autoriser AWS le transfert du trafic d'une AZ pour les ressources prises en charge, en votre nom, vers une AZ saine dans le. Région AWS AWS lance un changement automatique lorsque la télémétrie interne

indique la présence d'une anomalie dans un AZ d'une région susceptible d'avoir un impact sur les clients. La télémétrie interne intègre des métriques provenant de plusieurs sources, notamment le AWS réseau et les services Amazon EC2 et Elastic Load Balancing.

Les changements de zone et les changements automatiques sont temporaires. Lorsque vous commencez un changement de zone manuel, vous devez spécifier une date d'expiration (extensible), d'une durée initiale maximale de trois jours. Si vous souhaitez continuer à éloigner le trafic d'un AZ, vous pouvez mettre à jour le décalage de zone et définir une nouvelle date d'expiration. Avec l'autoshift zonal, AWS met fin à un changement automatique lorsque les indicateurs indiquent qu'il n'y a plus de problème ou de problème potentiel.

Pour en savoir plus sur ces fonctionnalités, consultez les chapitres suivants :

- Changement de zone dans Amazon Route 53 Application Recovery Controller
- Autoshift zonal dans le contrôleur de restauration d'applications Amazon Route 53

Restauration multirégionale

Si vous avez une application que vous avez conçue pour fonctionner à partir d'une autre Région AWS afin de poursuivre les opérations, vous pouvez utiliser le contrôle du routage pour le basculement. Le contrôle du routage vous permet de transférer le trafic de l'un Région AWS à l'autre en cas de problème, afin de garantir la disponibilité de votre application. Le contrôle du routage inclut des règles de sécurité, qui vous aident à vous protéger contre les conséquences imprévues, en imposant des garde-corps que vous définissez vous-même. À l'aide de ces règles, vous pouvez vous assurer, par exemple, qu'une seule des répliques de vos applications, active ou en veille, est activée et utilisée à la fois.

Pour une restauration multirégionale, Route 53 ARC peut vous aider à contourner le trafic DNS. Régions AWS Les contrôles de routage extrêmement fiables de Route 53 ARC vous permettent de récupérer votre application en redirigeant le trafic d'une région handicapée vers une région saine.

Grâce au contrôle de disponibilité, Route 53 ARC surveille en permanence les quotas de AWS ressources, la capacité et les politiques de routage réseau, et peut vous informer des modifications susceptibles d'affecter votre capacité à basculer vers une réplique et à effectuer une restauration. Les contrôles de disponibilité continus permettent de s'assurer, en permanence, que vous pouvez maintenir vos applications multirégionales dans un état adapté et configuré pour gérer le trafic de basculement. La vérification de l'état de préparation est utile lorsque vous configurez Route 53 ARC pour la première fois et pendant le fonctionnement normal de l'application. Le contrôle de préparation n'est pas destiné à être utilisé sur le chemin critique du basculement lors d'un événement.

Pour en savoir plus sur ces fonctionnalités, consultez les chapitres suivants :

- Contrôle du routage dans Amazon Route 53 Application Recovery Controller
- Vérification de l'état de préparation dans Amazon Route 53 Application Recovery Controller

Comparez les fonctionnalités de restauration multi-AZ et multirégionales d'Amazon Route 53 Application Recovery Controller

Le changement de zone, le changement automatique de zone et le contrôle du routage dans Amazon Route 53 Application Recovery Controller peuvent tous permettre une restauration rapide et vous aider à garantir la résilience de vos applications. AWS Ces options sont hautement disponibles et permettent de prendre en charge la restauration dans les scénarios où votre application connaît une latence accrue ou une disponibilité réduite. Ces options permettent de restaurer rapidement les applications en éloignant le trafic des déficiences isolées, ce qui limite l'impact et le temps perdu en raison des déficiences.

Le contrôle du routage est principalement axé sur AWS les applications situées dans plusieurs AWS régions (multirégions), tandis que le décalage de zone et le décalage automatique de zone ne prennent en charge le transfert de trafic que pour les équilibreurs de charge dotés d'applications multi-AZ. Il existe également d'autres différences, comme décrit dans cette section.

Les informations du tableau suivant incluent certaines des principales fonctionnalités du changement de zone, du changement automatique de zone et du contrôle du routage, ainsi que la comparaison des options entre elles. Ces descriptions peuvent vous aider à mieux comprendre comment une option spécifique peut être la meilleure solution pour les besoins de reprise après sinistre de votre organisation.

Contrôle du routage	Changement de zone	Autoshift zonal
Régional	Zonal	Zonal
Réachemine le trafic d'une AWS région à une autre (principalement) Peut également être utilisé pour rediriger le routage entre les zones de disponibilité	Éloigne le trafic d'une zone de disponibilité Le trafic est dirigé vers d'autres zones de disponibilité de la région, et non vers une cible spécifique	Éloigne le trafic d'une zone de disponibilité Le trafic est dirigé vers d'autres zones de disponibilité de la région, et non vers une cible spécifique
Nécessite une configuration	Disponible sans configuration	Nécessite une installation d'entraînement

Contrôle du routage	Changement de zone	Autoshift zonal
Nécessite une configuration et un paramétrage	Activé automatiquement par les services pris en charge (actuellement Network Load Balancer et Application Load Balancer)	Disponible pour les services pris en charge (actuellement Network Load Balancer et Application Load Balancer)
Initié par le client Le client détermine à quel moment il doit réacheminer le trafic	Initié par le client Le client détermine à quel moment il doit commencer un changement de zone	AWS-initié AWS déplace le trafic des applications vers un AZ en votre nom
Basé sur des frais Nécessite des frais distincts pour le contrôle du routage	Inclus avec les services La création de décalages de zone pour éloigner le trafic des AZ est incluse pour les équilibreurs de charge pris en charge	Inclus avec les services Le démarrage des transferts automatiques pour déplacer le trafic hors de AZ en votre nom est inclus pour les équilibreurs de charge pris en charge
N'expire pas Le trafic peut être redirigé indéfiniment vers une réplique	Temporaire Tous les décalages de zone doivent être définis pour expirer	Temporaire AWS démarre et arrête les changements automatiques

Pour en savoir plus sur chacune de ces fonctionnalités, consultez les chapitres suivants :

- Changement de zone dans Amazon Route 53 Application Recovery Controller
- Autoshift zonal dans le contrôleur de restauration d'applications Amazon Route 53
- Contrôle du routage dans Amazon Route 53 Application Recovery Controller

Utilisez le décalage de zone et le décalage automatique de zone pour restaurer les applications dans Amazon Route 53 Application Recovery Controller

Cette section explique comment utiliser les fonctionnalités d'Amazon Route 53 Application Recovery Controller pour restaurer de manière fiable votre AWS application en cas de problème dans une zone de disponibilité (AZ). Ces fonctionnalités, le changement de zone et le décalage automatique de zone, éloignent temporairement le trafic d'une zone AZ pour une ressource Elastic Load Balancing, afin de réduire le temps de restauration de vos applications.

La principale différence entre le changement de zone et le changement automatique de zone réside dans le fait que l'un est un changement de circulation manuel que vous contrôlez, tandis que l'autre déplace automatiquement le trafic en votre nom pour éviter toute entrave.

- Avec le changement de zone, vous déplacez manuellement le trafic d'une ressource Elastic Load Balancing gérée vers et Région AWS hors d'une zone de disponibilité.
- Grâce à l'autoshift zonal, le trafic Elastic Load Balancing est automatiquement transféré d'une zone de zone de zone endommagée vers une zone de zone saine d'une région lors d'événements, en votre nom.

Les rubriques suivantes décrivent les fonctionnalités de changement de zone et de décalage automatique de zone, ainsi que leur utilisation.

Rubriques

Changement de zone dans Amazon Route 53 Application Recovery Controller

Grâce au changement de zone dans Amazon Route 53 Application Recovery Controller, vous pouvez déplacer le trafic d'une ressource Elastic Load Balancing hors d'une zone de disponibilité dans un Région AWS, afin de pallier rapidement un problème et de restaurer rapidement votre application.

Notez que l'équilibrage de charge entre zones des ressources Elastic Load Balancing doit être désactivé pour utiliser cette fonctionnalité.

Lorsque vous déployez et exécutez AWS des applications sur des équilibreurs de charge dans plusieurs zones (généralement trois) d'une région, vous pouvez rapidement récupérer une application dans une zone de zone altérée en commençant un changement de zone. Le transfert du trafic de vos applications vers des zones de zone de disponibilité permet de réduire la durée et la gravité de l'impact causé par les pannes de courant ou les problèmes matériels ou logiciels dans une zone de zone de disponibilité.

Vous pouvez choisir de transférer le trafic, par exemple, parce qu'un mauvais déploiement entraîne des problèmes de latence ou parce que la zone de disponibilité est altérée. Un changement de zone ne nécessite aucune étape de configuration préalable, mais votre AWS configuration doit prendre en charge la charge de votre clientèle sans la zone de disponibilité dont vous vous éloignez. Les ressources d'équilibreur de charge prises en charge sont automatiquement enregistrées auprès d'Amazon Route 53 Application Recovery Controller pour vous, afin que vous puissiez simplement commencer un changement de zone pour l'équilibreur de charge en cas de besoin.

Le démarrage d'un changement de zone ne nécessite aucune installation ni configuration. Après avoir vérifié que vous disposez d'une capacité suffisante pour déplacer le trafic hors d'une zone de disponibilité, choisissez la zone de disponibilité à quitter et la ressource vers laquelle transférer le trafic, puis lancez le changement de zone. Vous pouvez annuler le quart de travail à tout moment pour que le trafic commence à revenir dans la zone de disponibilité.

Tous les changements de zone sont des mesures d'atténuation temporaires. Vous définissez une date d'expiration initiale lorsque vous commencez un changement de zone, d'une heure à trois jours (72 heures), que vous pouvez prolonger si vous devez poursuivre le changement de trafic.

Sachez que, dans certains scénarios spécifiques, le changement de zone ne déplace pas le trafic depuis l'AZ. Pour plus d'informations sur la prise en charge du décalage zonal, consultezRessources prises en charge pour le changement de zone et le décalage automatique de zone.

Comment fonctionne un changement de zone

Lorsque vous commencez un changement de zone pour une ressource d'équilibrage de charge, le trafic de cette ressource est déplacé hors de la zone de disponibilité que vous avez spécifiée. Pour commencer le changement, Amazon Route 53 Application Recovery Controller demande que le bilan de santé de l'équilibreur de charge soit défini sur « non fonctionnel » pour que le bilan de santé de la zone de disponibilité échoue. En cas de mauvais état de santé, Amazon Route 53 retire

automatiquement du DNS les adresses IP correspondantes à la ressource, de sorte que le trafic est redirigé depuis la zone de disponibilité. Les nouvelles connexions sont désormais routées vers d'autres zones de disponibilité Région AWS .

Il est important de noter que le changement de zone n'utilise pas de tests de santé de la manière habituelle, lorsqu'un bilan de santé surveille l'état sous-jacent des équilibreurs de charge ou des applications. Route 53 ARC utilise plutôt des contrôles de santé comme mécanisme pour éloigner le trafic d'une zone de disponibilité. Le mécanisme demande qu'un bilan de santé soit explicitement défini sur « non sain », puis sur « sain » à nouveau, afin de modifier le flux de trafic.

Le trafic commence à changer - Lorsque vous commencez un changement de zone sur la Route 53 ARC, en raison des étapes liées à la circulation, il se peut que vous ne voyiez pas le trafic quitter immédiatement la zone de disponibilité. L'établissement des connexions existantes en cours dans la zone de disponibilité peut également prendre un certain temps, en fonction du comportement du client et de la réutilisation des connexions. En fonction de vos paramètres DNS et d'autres facteurs, les connexions existantes peuvent être établies en quelques minutes ou prendre plus de temps. Pour plus d'informations, consultez la section Veiller à ce que les changements de trafic se terminent rapidement.

Fin du changement de zone - Lorsqu'un changement de zone expire ou que vous l'annulez, Route 53 ARC prend des mesures pour arrêter le changement de trafic. Il inverse le processus de démarrage d'un changement de trafic et demande que les bilans de santé de la Route 53 soient remis en état de fonctionnement. Des bilans de santé sains permettent de restaurer les adresses IP zonales d'origine. Désormais, la zone de disponibilité récupérée est à nouveau incluse dans le routage de l'équilibreur de charge et le trafic recommence à circuler vers l'AZ.

Vous devez configurer tous les décalages de zone pour qu'ils expirent lorsque vous commencez les changements de zone. Vous pouvez initialement définir un décalage de zone pour qu'il expire dans un délai maximum de trois jours (72 heures). Vous pouvez toutefois mettre à jour un décalage de zone pour définir une nouvelle date d'expiration à tout moment. Vous pouvez également annuler un changement de zone avant son expiration, si vous êtes prêt à rétablir le trafic vers la zone de disponibilité.

Quand le trafic ne s'éloigne pas

Dans certains scénarios spécifiques, un changement de zone ne déplace pas le trafic depuis l'AZ. Par exemple, si les groupes cibles de l'équilibreur de charge dans les AZ ne possèdent aucune instance, ou si toutes les instances ne fonctionnent pas correctement, l'équilibreur de charge est dans un état ouvert en cas de défaillance. Si vous commencez un changement de zone pour un

équilibreur de charge dans ce scénario, le décalage de zone ne change pas les AZ que l'équilibreur de charge utilise, car celui-ci est déjà dans un état ouvert en cas de défaillance. Ce comportement est normal. Le changement de zone ne peut pas forcer une zone à être insalubre et déplacer le trafic vers les autres zones d'une région si toutes les zones ne sont pas ouvertes (mauvaises conditions). Un deuxième scénario est celui où vous entamez un changement de zone pour un Application Load Balancer qui est le point de terminaison d'un accélérateur dans. AWS Global Accelerator Le changement de zone n'est pas pris en charge pour les équilibreurs de charge d'application qui sont les points de terminaison des accélérateurs dans Global Accelerator.

Pour plus d'informations sur la prise en charge du décalage zonal, consultezRessources prises en charge pour le changement de zone et le décalage automatique de zone.

Région AWS disponibilité pour le changement de zone

Pour obtenir des informations détaillées sur le support régional et les points de terminaison de service pour Amazon Route 53 Application Recovery Controller, consultez la section Points de terminaison et quotas Amazon Route 53 Application Recovery Controller dans le manuel Amazon Web Services General Reference.

Le changement de zone est actuellement disponible dans la Régions AWS liste ci-dessous. Le changement de zone est également disponible dans les régions chinoises, c'est-à-dire dans les régions de Chine (Pékin) et de Chine (Ningxia).

Nom de la région	Région	Point de terminaison	Protocole	
US East (Ohio)	us-east-2	arc-zonal-shift.us-east-2.amazonaws.com	HTTPS	
US East (N. Virginia)	us-east-1	arc-zonal-shift.us-east-1.amazonaws.com	HTTPS	
USA Ouest (Californie du Nord)	us-west-1	arc-zonal-shift.us-west-1.amazonaws.com	HTTPS	

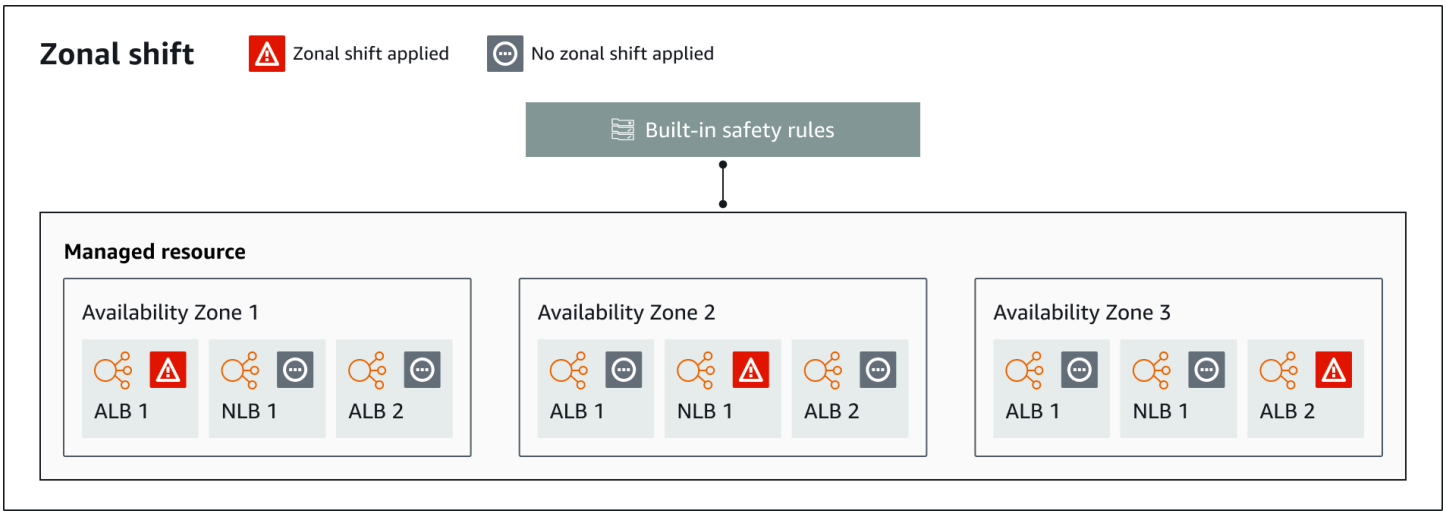
Nom de la région	Région	Point de terminaison	Protocole	
US West (Oregon)	us-west-2	arc-zonal-shift.us-west-2.amazonaws.com	HTTPS	
Afrique (Le Cap)	af-south-1	arc-zonal-shift.af-south-1.amazonaws.com	HTTPS	
Asie-Pacifique (Hong Kong)	ap-east-1	arc-zonal-shift.ap-east-1.amazonaws.com	HTTPS	
Asie-Pacifique (Hyderabad)	ap-south-2	arc-zonal-shift.ap-south-2.amazonaws.com	HTTPS	
Asie-Pacifique (Jakarta)	ap-southeast-3	arc-zonal-shift.ap-southeast-3.amazonaws.com	HTTPS	
Asie-Pacifique (Melbourne)	ap-southeast-4	arc-zonal-shift.ap-southeast-4.amazonaws.com	HTTPS	
Asia Pacific (Mumbai)	ap-south-1	arc-zonal-shift.ap-south-1.amazonaws.com	HTTPS	
Asie-Pacifique (Osaka)	ap-northeast-3	arc-zonal-shift.ap-northeast-3.amazonaws.com	HTTPS	
Asia Pacific (Seoul)	ap-northeast-2	arc-zonal-shift.ap-northeast-2.amazonaws.com	HTTPS	

Nom de la région	Région	Point de terminaison	Protocole	
Asie-Pacifique (Singapour)	ap-southeast-1	arc-zonal-shift.ap-southeast-1.amazonaws.com	HTTPS	
Asia Pacific (Sydney)	ap-southeast-2	arc-zonal-shift.ap-southeast-2.amazonaws.com	HTTPS	
Asia Pacific (Tokyo)	ap-northeast-1	arc-zonal-shift.ap-northeast-1.amazonaws.com	HTTPS	
Canada (Central)	ca-central-1	arc-zonal-shift.ca-central-1.amazonaws.com	HTTPS	
Canada Ouest (Calgary)	ca-west-1	arc-zonal-shift.ca-west-1.amazonaws.com	HTTPS	
Europe (Francfort)	eu-central-1	arc-zonal-shift.eu-central-1.amazonaws.com	HTTPS	
Europe (Irlande)	eu-west-1	arc-zonal-shift.eu-west-1.amazonaws.com	HTTPS	
Europe (Londres)	eu-west-2	arc-zonal-shift.eu-west-2.amazonaws.com	HTTPS	
Europe (Milan)	eu-south-1	arc-zonal-shift.eu-south-1.amazonaws.com	HTTPS	
Europe (Paris)	eu-west-3	arc-zonal-shift.eu-west-3.amazonaws.com	HTTPS	

Nom de la région	Région	Point de terminaison	Protocole	
Europe (Espagne)	eu-south-2	arc-zonal-shift.eu-south-2.amazonaws.com	HTTPS	
Europe (Stockholm)	eu-north-1	arc-zonal-shift.eu-north-1.amazonaws.com	HTTPS	
Europe (Zurich)	eu-central-2	arc-zonal-shift.eu-central-2.amazonaws.com	HTTPS	
Israël (Tel Aviv)	il-central-1	arc-zonal-shift.il-central-1.amazonaws.com	HTTPS	
Moyen-Orient (Bahreïn)	me-south-1	arc-zonal-shift.me-south-1.amazonaws.com	HTTPS	
Moyen-Orient (EAU)	me-central-1	arc-zonal-shift.me-central-1.amazonaws.com	HTTPS	
Amérique du Sud (São Paulo)	sa-east-1	arc-zonal-shift.sa-east-1.amazonaws.com	HTTPS	
AWS GovCloud (USA Est)	us-gov-east-1	arc-zonal-shift.us-gov-east-1.amazonaws.com	HTTPS	
AWS GovCloud (US-Ouest)	us-gov-west-1	arc-zonal-shift.us-gov-west-1.amazonaws.com	HTTPS	

Composants de décalage zonal

Le schéma suivant illustre un exemple de changement de zone déplaçant le trafic hors d'une zone de disponibilité dans un Région AWS. Les contrôles intégrés au décalage de zone vous empêchent de commencer un autre changement de zone pour une ressource alors qu'un changement de zone est déjà actif.



Voici les composants de la capacité de changement de zone de Route 53 ARC.

Changement de zone

Vous entamez un changement de zone pour une ressource gérée de votre AWS compte afin de déplacer temporairement le trafic d'une zone de disponibilité d'une zone de disponibilité vers une Région AWS zone saine de la région, afin de remédier rapidement à un problème dans une zone de disponibilité. Actuellement, vous pouvez démarrer un changement de zone uniquement pour les équilibreurs de charge réseau et les équilibreurs de charge d'application pour lesquels l'équilibrage de charge entre zones n'est pas configuré. Les équilibreurs de charge pris en charge sont automatiquement enregistrés pour vous dans Route 53 ARC.

Contrôles de sécurité intégrés

Les contrôles intégrés à la Route 53 ARC empêchent que plusieurs changements de trafic soient effectués à la fois pour une ressource. En d'autres termes, un seul changement de zone initié par le client, un changement de zone par entraînement ou un changement automatique pour la ressource peuvent entraîner un transfert actif du trafic hors d'une zone de disponibilité. Par exemple, si vous commencez un changement de zone pour une ressource alors qu'elle est actuellement déplacée avec le décalage automatique, votre changement de zone est prioritaire.

Pour plus d'informations, voir Autoshift zonal dans le contrôleur de restauration d'applications Amazon Route 53 et Résultats des séances d'entraînement.

Identificateur de ressource

Identifiant d'une ressource à inclure dans un décalage de zone. L'identifiant est le Amazon Resource Name (ARN) de la ressource.

Pour un changement de zone, vous ne pouvez sélectionner les ressources de votre compte que pour un AWS service pris en charge par Route 53 ARC. Les ressources prises en charge dans ces AWS services sont automatiquement enregistrées auprès de Route 53 ARC par le AWS service.

> **Note**
>
> Actuellement, vous ne pouvez démarrer un changement de zone que pour les équilibreurs de charge réseau et les équilibreurs de charge d'application lorsque l'équilibrage de charge entre zones est désactivé.

Ressource gérée

AWS les services enregistrent automatiquement les ressources auprès de la Route 53 ARC pour le changement de zone. Une ressource qui a été enregistrée est une ressource gérée dans Route 53 ARC.

Nom de la ressource

Nom d'une ressource dans Route 53 ARC que vous pouvez spécifier pour un décalage de zone.

État (statut de changement de zone)

Un statut pour un changement de zone. Le `Status` décalage zonal peut prendre l'une des valeurs suivantes :

- ACTIF : Le changement de zone est lancé et actif.
- EXPIRÉ : Le décalage de zone a expiré (le délai d'expiration a été dépassé).
- ANNULÉ : Le changement de zone a été annulé.

Statut appliqué

Un statut appliqué indique si un changement est en cours pour une ressource. Le changement ayant le statut `APPLIED` détermine la zone de disponibilité dans laquelle le trafic applicatif a été transféré pour une ressource, et la date à laquelle ce décalage prend fin.

Heure d'expiration (heure d'expiration)

Heure d'expiration (heure d'expiration) d'un changement de zone. Les changements de zone sont temporaires. Pour un changement de zone initié par le client, vous pouvez initialement définir un changement de zone pour qu'il soit actif pendant trois jours maximum (72 heures).

Lorsque vous commencez un changement de zone, vous spécifiez la durée pendant laquelle vous souhaitez qu'il soit actif, ce que Route 53 ARC convertit en heure d'expiration (heure d'expiration). Vous pouvez annuler un changement de zone initié par le client, par exemple, si vous êtes prêt à rétablir le trafic vers la zone de disponibilité. Vous pouvez également prolonger un changement de zone initié par le client en le mettant à jour pour spécifier une autre durée d'expiration.

Vous pouvez annuler à la fois les changements de zone initiés par le client et les changements de zone qui AWS commencent pour une séance d'entraînement avec le changement automatique de zone.

Plans de données et de contrôle pour le changement de zone

Lorsque vous planifiez le basculement et la reprise après sinistre, évaluez la résilience de vos mécanismes de basculement. Nous vous recommandons de vous assurer que les mécanismes sur lesquels vous comptez lors du basculement sont hautement disponibles, afin de pouvoir les utiliser lorsque vous en avez besoin en cas de sinistre. En règle générale, vous devez utiliser les fonctions du plan de données pour vos mécanismes chaque fois que vous le pouvez, pour une fiabilité et une tolérance aux pannes optimales. Dans cette optique, il est important de comprendre comment les fonctionnalités d'un service sont réparties entre les plans de contrôle et les plans de données, et de comprendre dans quels cas vous pouvez compter sur une fiabilité extrême en ce qui concerne le plan de données d'un service.

Comme pour la plupart des AWS services, la fonctionnalité de changement de zone est prise en charge par les plans de contrôle et les plans de données. Bien que les deux soient conçus pour être fiables, un plan de contrôle est optimisé pour la cohérence des données, tandis qu'un plan de données est optimisé pour la disponibilité. Un plan de données est conçu pour être résilient afin de

maintenir sa disponibilité même en cas d'événements perturbateurs, lorsqu'un plan de contrôle peut devenir indisponible.

En général, un plan de contrôle vous permet d'exécuter des fonctions de gestion de base, telles que la création, la mise à jour et la suppression de ressources dans le service. Un plan de données fournit les fonctionnalités de base d'un service.

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

Tarification du changement de zone dans Amazon Route 53 Application Recovery Controller

Pour le changement de zone, vous pouvez démarrer un changement de zone pour les ressources prises en charge, afin de récupérer votre application en cas de problème dans une zone de disponibilité. L'utilisation du changement de zone est gratuite.

Vous ne payez que pour ce que vous utilisez dans Amazon Route 53 Application Recovery Controller. Pour obtenir des informations détaillées sur les tarifs de Route 53 ARC et des exemples de tarification, consultez la section Tarification d'Amazon Route 53 et faites défiler la page vers le bas jusqu'à Amazon Route 53 Application Recovery Controller.

Meilleures pratiques pour les changements de zone sur la Route 53 ARC

Nous recommandons les meilleures pratiques suivantes pour utiliser les décalages de zone pour la restauration multi-AZ dans Route 53 ARC. Les changements de zone réduisent généralement la capacité d'une application en ligne. Il est donc important de faire preuve de prudence lorsque vous les utilisez en production.

Rubriques

- Planification des capacités et pré-dimensionnement
- Limitez le temps pendant lequel les clients restent connectés à vos terminaux
- Testez à l'avance les décalages de zone de départ
- Assurez-vous que toutes les zones de disponibilité sont saines et qu'elles accueillent du trafic
- Utiliser les opérations de l'API du plan de données pour la reprise après sinistre
- Déplacez le trafic avec un changement de zone uniquement temporairement

Planification des capacités et pré-dimensionnement

Assurez-vous d'avoir prévu une capacité suffisante, que vous l'avez prédimensionnée ou que vous pouvez la dimensionner automatiquement, pour faire face à la charge supplémentaire imposée aux zones de disponibilité lorsque vous commencez un changement de zone. Dans le cas d'une architecture axée sur la restauration, il est généralement recommandé de prédimensionner la capacité de calcul afin d'inclure une marge de manœuvre suffisante pour répondre aux pics de trafic lorsque l'une de vos trois répliques (généralement) est hors ligne.

Lorsque vous commencez un changement de zone pour une seule ressource d'équilibreur de charge, par exemple, la capacité d'une zone de disponibilité est temporairement supprimée derrière l'équilibreur de charge. En fonction des changements de zone que vous commencez et de la configuration de vos équilibreurs de charge, vous devez vous assurer d'avoir soigneusement planifié la gestion de la charge accrue sur les zones de disponibilité restantes.

Limitez le temps pendant lequel les clients restent connectés à vos terminaux

Lorsqu'Amazon Route 53 Application Recovery Controller déplace le trafic pour éviter une perturbation, par exemple en utilisant le décalage de zone ou le décalage automatique de zone, le mécanisme utilisé par Route 53 ARC pour déplacer le trafic de votre application est une mise à jour DNS. Une mise à jour du DNS entraîne le renvoi de toutes les nouvelles connexions hors de la zone affectée.

Cependant, les clients disposant de connexions ouvertes préexistantes peuvent continuer à faire des demandes concernant l'emplacement altéré jusqu'à ce qu'ils se reconnectent. Pour garantir un rétablissement rapide, nous vous recommandons de limiter la durée pendant laquelle les clients restent connectés à vos terminaux.

Si vous utilisez un Application Load Balancer, vous pouvez utiliser `keepalive` cette option pour configurer la durée des connexions. Pour plus d'informations, consultez la section Durée de conservation du client HTTP dans le guide de l'utilisateur d'Application Load Balancer.

Par défaut, les équilibreurs de charge d'application définissent la durée de conservation du client HTTP sur 3 600 secondes, soit 1 heure. Nous vous suggérons de réduire la valeur pour qu'elle corresponde à votre objectif de temps de restauration pour votre application, par exemple 300 secondes. Lorsque vous choisissez une durée de conservation d'un client HTTP, considérez que cette valeur représente un compromis entre une reconnexion plus fréquente en général, ce qui peut affecter la latence, et le déplacement plus rapide de tous les clients loin d'une zone ou d'une région altérée.

Testez à l'avance les décalages de zone de départ

Testez régulièrement le déplacement du trafic hors des zones de disponibilité pour votre application en commençant par des changements de zone. Planifiez et exécutez les changements de zone de départ, de préférence dans les environnements de test et de production, dans le cadre des tests de basculement réguliers visant à restaurer vos applications en cas de sinistre. Des tests réguliers sont essentiels pour garantir que vous êtes prêt et que vous avez la confiance nécessaire pour atténuer les problèmes lorsqu'un événement opérationnel se produit.

Assurez-vous que toutes les zones de disponibilité sont saines et qu'elles accueillent du trafic

Les décalages zonaux fonctionnent en marquant une ressource, c'est-à-dire une réplique d'application, comme étant défectueuse dans une zone de disponibilité. Il est donc essentiel de s'assurer que les cibles des équilibreurs de charge pour vos applications sont généralement saines et qu'elles absorbent activement le trafic dans les zones de disponibilité d'une région. Nous vous recommandons de disposer de tableaux de bord pour en assurer le suivi, notamment des métriques Elastic Load Balancing pour les cibles non conformes et des octets traités par zone de disponibilité.

Envisagez de surveiller l'état de vos ressources depuis une deuxième région adjacente. Les avantages de cette approche sont qu'elle peut être plus représentative de l'expérience de vos utilisateurs finaux et qu'elle réduit également le risque que votre application et votre surveillance soient touchées par le même sinistre en même temps (« destin partagé »).

Utiliser les opérations de l'API du plan de données pour la reprise après sinistre

Pour démarrer un changement de zone lorsque vous devez restaurer une application rapidement, avec peu de dépendances, nous vous recommandons d'utiliser l'API AWS Command Line Interface or avec des actions de changement de zone, avec des informations d'identification préenregistrées, si possible. Vous pouvez également commencer à changer de zone dans le AWS Management Console, pour faciliter l'utilisation. Mais lorsqu'une restauration rapide et fiable est essentielle, les opérations sur le plan de données constituent un meilleur choix. Pour plus d'informations, consultez le Guide de référence de l'API Zonal Shift.

Déplacez le trafic avec un changement de zone uniquement temporairement

Un changement de zone déplace le trafic hors d'une zone de disponibilité de façon temporaire, afin d'atténuer une détérioration. Vous devez restaurer la ressource pour la mise en service de l'application dès que vous avez pris des mesures pour corriger un problème. Cela garantit que l'ensemble de votre application est restauré dans son état d'origine entièrement redondant et résilient.

Opérations de l'API Zonal Shift

Le tableau suivant répertorie les opérations de l'API ARC Route 53 que vous pouvez utiliser à l'aide du décalage de zone, qui déplace le trafic hors d'une zone de disponibilité pour les applications multi-AZ. Le tableau inclut également des liens vers la documentation pertinente.

Pour des exemples d'utilisation des opérations d'API de changement de zone courantes avec le AWS Command Line Interface, voirExemples d'utilisation de la fonction AWS CLI avec décalage de zone.

Action	Utilisation de la console Route 53 ARC	Utilisation de l'API ARC Route 53
Lancement d'un changement de zone	Consultez Commencer un changement de zone.	Voir StartZonalShift
Mise à jour d'un changement de zone	Consultez Mettre à jour ou annuler un changement de zone.	Voir UpdateZonalShift
Répertorier les décalages de zone	Consultez Changement de zone dans Amazon Route 53 Application Recovery Controller.	Voir ListZonalShifts
Répertorier les ressources gérées	Consultez Ressources prises en charge pour le changement de zone et le décalage automatique de zone.	Voir les ListManagedressources
Obtenez une ressource gérée	Consultez Ressources prises en charge pour le changement de zone et le décalage automatique de zone.	Voir la GetManagedressource
Annulation d'un changement de zone	Consultez Mettre à jour ou annuler un changement de zone.	Voir CancelZonalShift

Exemples d'utilisation de la fonction AWS CLI avec décalage de zone

Cette section présente des exemples d'applications simples d'utilisation du décalage de zone, en utilisant la fonctionnalité AWS Command Line Interface de décalage zonal d'Amazon Route 53 Application Recovery Controller à l'aide d'opérations d'API. Les exemples sont destinés à vous aider à acquérir une compréhension de base de la manière d'utiliser le décalage zonal à l'aide de la CLI.

Le changement de zone dans Route 53 ARC vous permet de déplacer temporairement le trafic vers les ressources prises en charge hors d'une zone de disponibilité afin que votre application puisse continuer à fonctionner normalement avec les autres zones de disponibilité d'une. Région AWS Zonal Shift prend actuellement en charge les équilibreurs de charge réseau et les équilibreurs de charge d'application lorsque l'équilibrage de charge entre zones est désactivé.

Regardons un exemple de démarrage d'un décalage de zone à l'aide du AWS Command Line Interface. Vous pouvez également utiliser le AWS CLI pour mettre à jour un décalage de zone, par exemple pour définir une nouvelle date d'expiration. Tous les décalages de zone sont temporaires et doivent être initialement définis pour expirer dans les trois jours. Toutefois, vous pouvez mettre à jour un décalage de zone ultérieurement pour définir une nouvelle date d'expiration.

Pour plus d'informations sur l'utilisation du AWS CLI, consultez la référence des AWS CLI commandes. Pour obtenir la liste des actions de l'API Zonal Shift et des liens vers des informations supplémentaires, consultezOpérations de l'API Zonal Shift.

Commencer le changement de zone

Vous pouvez démarrer un changement de zone avec la CLI à l'aide de la `start-zonal-shift` commande.

```
aws arc-zonal-shift start-zonal-shift \
      --resource-identifier="arn:aws:testservice::111122223333:ExampleALB123456890" \
      --away-from="usw2-az1" \
      --expires-in="5m" \
      --comment="Shifting traffic away from USW2-AZ1"
```

```
{
   "zonalShiftId": "2222222-3333-444-1111",
   "resourceIdentifier": "arn:aws:testservice::111122223333:ExampleALB123456890",
   "awayFrom": "usw2-az1",
   "expiryTime": 2022-11-14T01:40:42+00:00,
   "startTime": 2022-11-14T01:35:42+00:00,
```

```
   "status": "ACTIVE",
   "comment": "Shifting traffic away from USW2-AZ1"
}
```

Obtenez une ressource gérée

Vous pouvez obtenir des informations sur une ressource gérée à l'aide de la CLI à l'aide de la `get-managed-resource` commande.

```
aws arc-zonal-shift get-managed-resource \
   --resource-identifier="arn:aws:testservice::111122223333:ExampleALB123456890
```

```
{
    "arn": "arn:aws:testservice::111122223333:ExampleALB123456890",
    "name": "TestResource",
    "appliedWeights": {
        "usw2-az1": 1.0,
        "usw2-az2": 1.0,
        "usw2-az3": 1.0
    },
    "zonalShifts": []
}
```

Répertorier les ressources gérées

Vous pouvez répertorier les ressources gérées de votre compte à l'aide de la CLI à l'aide de la `list-managed-resources` commande.

```
aws arc-zonal-shift list-managed-resources
```

```
{
    "items": [
        {
            "arn": "arn:aws:testservice::111122223333:ExampleALB123456890",
            "name": "TestResource",
            "availabilityZones": [
                "usw2-az1",
                "usw2-az2",
                "usw2-az3"
            ]
        }
```

```
    ]
}
```

Répertorier les décalages de zone

Vous pouvez répertorier les changements de zone de votre compte à l'aide de la CLI à l'aide de la `list-zonal-shifts` commande.

```
aws arc-zonal-shift list-zonal-shifts
```

```
{
    "items": [
        {
            "zonalShiftId": "2222222-3333-444-1111",
            "resourceIdentifier":
 "arn:aws:testservice::111122223333:ExampleALB123456890",
            "awayFrom": "usw2-az1",
            "expiryTime": 2022-11-15T09:10:42+00:00,
            "startTime": 2022-11-13T01:35:42+00:00,
            "status": "ACTIVE",
            "comment": "Shifting traffic away from USW2-AZ1"
        }
    ]
}
```

Mettre à jour le changement de zone

Vous pouvez mettre à jour un décalage de zone avec la CLI à l'aide de la `update-zonal-shift` commande.

```
aws arc-zonal-shift update-zonal-shift \
   --zonal-shift-id="="arn:aws:testservice::111122223333:ExampleALB123456890" \
   --expires-in="1h" \
   --comment="Still shifting traffic away from USW2-AZ1"
```

```
{
    "zonalShiftId": "2222222-3333-444-1111",
    "resourceIdentifier": "arn:aws:testservice::111122223333:ExampleALB123456890",
    "awayFrom": "usw2-az1",
    "expiryTime": 2022-11-15T10:35:42+00:00,
    "startTime": 2022-11-15T09:35:42+00:00,
```

```
    "status": "ACTIVE",
    "comment": "Still shifting traffic away from USW2-AZ1"
}
```

Annuler le changement de zone

Vous pouvez annuler un changement de zone à l'aide de la CLI à l'aide de la `cancel-zonal-shift` commande.

```
aws arc-zonal-shift cancel-zonal-shift \
   --zonal-shift-id="="arn:aws:testservice::111122223333:ExampleALB123456890"
```

```
{
    "zonalShiftId": "2222222-3333-444-1111",
    "resourceIdentifier": "arn:aws:testservice::111122223333:ExampleALB123456890",
    "awayFrom": "usw2-az1",
    "expiryTime": 2022-11-15T10:35:42+00:00,
    "startTime": 2022-11-15T09:35:42+00:00,
    "status": "CANCELED",
    "comment": "Shifting traffic away from USW2-AZ1"
}
```

Ressources prises en charge pour le changement de zone et le décalage automatique de zone

Amazon Route 53 Application Recovery Controller prend actuellement en charge les ressources suivantes pour le changement de zone et le décalage automatique de zone :

- Network Load Balancers
- Application Load Balancers

Les ressources d'équilibrage de charge prises en charge sont automatiquement enregistrées auprès de Route 53 ARC afin que vous puissiez les utiliser avec le décalage zonal (et le décalage automatique zonal). Vous pouvez commencer un changement de zone pour un équilibreur de charge dans la console Elastic Load Balancing (dans la plupart des cas Régions AWS) ou dans Route 53 ARC.

Passez en revue les conditions suivantes pour travailler avec les changements de zone et les ressources dans Route 53 ARC :

- Le décalage zonal n'est pas pris en charge avec l'équilibrage de charge entre zones. Pour qu'un équilibreur de charge soit enregistré auprès de Route 53 ARC, assurez-vous que vous avez désactivé l'équilibrage de charge entre zones pour l'équilibreur de charge dans Elastic Load Balancing.
- dans certains scénarios spécifiques, le changement de zone ne déplace pas le trafic depuis l'AZ. Par exemple, si les groupes cibles de l'équilibreur de charge dans les AZ ne possèdent aucune instance, ou si toutes les instances ne fonctionnent pas correctement, l'équilibreur de charge est en état d'échec ouvert et vous ne pouvez pas déplacer l'un des AZ.
- Les équilibreurs de charge réseau publics et internes (privés) et les équilibreurs de charge d'application sont pris en charge.
- Une ressource doit être active et entièrement provisionnée pour transférer le trafic vers elle. Avant de commencer un changement de zone pour une ressource, assurez-vous qu'il s'agit d'une ressource gérée dans Route 53 ARC. Par exemple, vous pouvez afficher la liste des ressources gérées dans le AWS Management Console, ou vous pouvez utiliser l'`get-managed-resource`opération avec l'identifiant de la ressource.
- Le changement de zone n'est pas pris en charge pour les équilibreurs de charge d'application qui sont les points de terminaison des accélérateurs. AWS Global Accelerator
- Lorsqu'un Application Load Balancer est la cible d'un Network Load Balancer, commencez le changement de zone à partir du Network Load Balancer. Si vous commencez le changement de zone à partir de l'Application Load Balancer, le Network Load Balancer n'arrête pas d'envoyer du trafic vers l'Application Load Balancer et ses cibles.
- La ressource pour un changement de zone doit être une ressource gérée enregistrée auprès de Route 53 ARC par un AWS service. Elastic Load Balancing s'enregistre automatiquement auprès des équilibreurs de charge réseau Route 53 ARC et des équilibreurs de charge d'application lorsque l'équilibrage de charge entre zones est désactivé.
- Pour démarrer un changement de zone avec une ressource, celle-ci doit être déployée dans la zone de disponibilité et Région AWS là où vous commencez le changement. Assurez-vous de commencer un changement de zone dans la même région que celle dans laquelle se trouve l'AZ correspondant au quart de travail, et que la ressource pour laquelle vous transférez le trafic se trouve également dans la même zone et dans la même région.
- Assurez-vous que vous disposez des autorisations IAM appropriées pour utiliser le décalage de zone avec une ressource. Pour plus d’informations, consultez IAM et autorisations pour le changement de zone.

Démarrer, mettre à jour ou annuler un changement de zone

Cette section décrit les procédures relatives à l'utilisation des décalages de zone, notamment le démarrage d'un décalage de zone et son annulation.

Commencer un changement de zone

Les étapes décrites dans cette section expliquent comment démarrer un changement de zone initié par le client sur la console Amazon Route 53 Application Recovery Controller. Pour utiliser le décalage de zone par programmation, consultez le guide de référence de l'API Zonal Shift.

Outre le lancement d'un changement de zone dans Route 53 ARC, vous pouvez également démarrer un changement de zone pour un équilibreur de charge dans la console Elastic Load Balancing (dans les régions prises en charge). Pour plus d'informations, consultez la section Zonal shift dans le guide de l'utilisateur d'Elastic Load Balancing.

Pour démarrer un changement de zone

1. Ouvrez la console Route 53 ARC à l'adressehttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Sous Multi-AZ, choisissez Zonal Shift.
3. Sur la page Zonal shift, sélectionnez Start zonal shift.
4. Sélectionnez la zone de disponibilité depuis laquelle vous voulez déplacer le trafic.
5. Sélectionnez un équilibreur de charge dans le tableau des ressources pour déplacer le trafic.
6. Pour Définir l'expiration du décalage de zone, choisissez ou entrez une date d'expiration pour le décalage de zone. Un changement de zone peut être configuré pour être actif initialement pendant 1 minute ou jusqu'à trois jours (72 heures).

   Tous les changements de zone sont temporaires. Vous devez définir une date d'expiration, mais vous pouvez mettre à jour les équipes actives ultérieurement pour définir une nouvelle période d'expiration pouvant aller jusqu'à trois jours.
7. Saisissez un commentaire. Vous pouvez mettre à jour le changement de zone ultérieurement pour modifier le commentaire, si vous le souhaitez.
8. Cochez la case pour confirmer que le lancement d'un changement de zone réduira la capacité disponible pour votre application en déplaçant le trafic hors de la zone de disponibilité.
9. Sélectionnez Démarrer.

Mettre à jour ou annuler un changement de zone

Les étapes décrites dans cette section expliquent comment mettre à jour un changement de zone que vous initiez, ou comment annuler un changement de zone, sur la console Amazon Route 53 Application Recovery Controller. Pour utiliser le décalage de zone par programmation, consultez le guide de référence de l'API Zonal Shift.

Vous pouvez mettre à jour un décalage de zone pour définir une nouvelle date d'expiration, ou modifier ou remplacer le commentaire correspondant au décalage de zone. Vous pouvez annuler un changement de zone à tout moment avant son expiration.

Vous pouvez annuler les changements de zone que vous initiez, ou les changements de zone qui AWS commencent pour une ressource dans le cadre d'une séance d'entraînement pour le changement automatique de zone. Pour en savoir plus sur les changements pratiques en matière de changement automatique zonal, voir. Comment fonctionnent l'autoshift zonal et les courses d'entraînement

Pour mettre à jour un décalage de zone

1. Ouvrez la console Route 53 ARC à l'adressehttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Sous Multi-AZ, choisissez Zonal Shift.
3. Sélectionnez le décalage de zone que vous souhaitez mettre à jour, puis choisissez Mettre à jour le décalage de zone.
4. Pour Définir l'expiration du changement de zone, sélectionnez ou saisissez éventuellement une date d'expiration.
5. Pour Commentaire, modifiez éventuellement le commentaire existant ou saisissez-en un nouveau.
6. Choisissez Mettre à jour.

Pour annuler un changement de zone

1. Ouvrez la console Route 53 ARC à l'adressehttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Sous Multi-AZ, choisissez Zonal Shift.
3. Sélectionnez le décalage de zone que vous souhaitez annuler, puis choisissez Annuler le décalage de zone.

4. Dans la boîte de dialogue modale de confirmation, choisissez Confirmer.

Enregistrement et surveillance du changement de zone dans Amazon Route 53 Application Recovery Controller

Vous pouvez utiliser AWS CloudTrail Amazon EventBridge pour surveiller le changement de zone dans Amazon Route 53 Application Recovery Controller, afin d'analyser les modèles et de résoudre les problèmes.

Rubriques

- Enregistrement des appels d'API Zonal Shift à l'aide de AWS CloudTrail
- Utilisation du décalage zonal avec Amazon EventBridge

Enregistrement des appels d'API Zonal Shift à l'aide de AWS CloudTrail

Zonal Shift for Amazon Route 53 Application Recovery Controller 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 ARC. CloudTrail capture tous les appels d'API pour le changement de zone sous forme d'événements. Les appels capturés incluent des appels provenant de la console Route 53 ARC et des appels de code vers les opérations de l'API Route 53 ARC pour le changement de zone.

Si vous créez un suivi, vous pouvez activer la diffusion continue des CloudTrail événements vers un compartiment Amazon S3, y compris les événements liés au changement de zone. 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 de changement de zone qui a été faite à Route 53 ARC, 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.

Pour en savoir plus CloudTrail, consultez le guide de AWS CloudTrail l'utilisateur.

Informations sur le décalage zonal dans CloudTrail

CloudTrail est activé sur votre compte Compte AWS lorsque vous créez le compte. Lorsqu'une activité se produit sur Route 53 ARC pour un changement de zone, 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 Compte AWS. Pour plus d'informations, consultez la section Utilisation de l'historique des CloudTrail événements.

Pour un enregistrement continu des événements survenus dans votre région Compte AWS, y compris les événements liés au changement de zone sur la Route 53 ARC, 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 Régions AWS. 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 afin d'analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et d'agir en conséquence. Pour plus d'informations, consultez les ressources suivantes :

- Présentation de la création d'un journal de suivi
- 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 ARC de Route 53 sont enregistrées CloudTrail et documentées dans le Guide de référence de l'API de contrôle de routage pour Amazon Route 53 Application Recovery Controller. Par exemple, les appels aux `ListManagedResources` actions `StartZonalShift` et 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 faite avec les informations d'identification de l'utilisateur root ou AWS Identity and Access Management (IAM).
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la demande a été faite par un autre AWS service.

Pour plus d'informations, consultez l'élément CloudTrail UserIdentity.

Afficher les événements de la Route 53 ARC dans l'historique des événements

CloudTrail vous permet de consulter les événements récents dans l'historique des événements. Pour plus d'informations, consultez la section Utilisation de l'historique des CloudTrail événements dans le guide de AWS CloudTrail l'utilisateur.

Comprendre les entrées du fichier journal des décalages zonaux

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'exemple suivant montre une entrée de CloudTrail journal illustrant l'`ListManagedResources`action à effectuer pour le changement de zone.


```
{
      "eventVersion": "1.08",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:role/admin",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "sessionIssuer": {
            "type": "Role",
            "principalId": "AROA33L3W36EXAMPLE",
            "arn": "arn:aws:iam::111122223333:role/admin",
            "accountId": "111122223333",
            "userName": "EXAMPLENAME"
          },
          "webIdFederationData": {},
          "attributes": {
            "creationDate": "2022-11-14T16:01:51Z",
            "mfaAuthenticated": "false"
          }
        }
      },
```

```
      "eventTime": "2022-11-14T16:14:41Z",
      "eventSource": "arc-zonal-shift.amazonaws.com",
      "eventName": "ListManagedResources",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.50",
      "userAgent": "Boto3/1.17.101 Python/3.8.10 Linux/4.14.231-180.360.amzn2.x86_64
 exec-env/AWS_Lambda_python3.8 Botocore/1.20.102",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "VGXG4ZUE7UZTVCMTJGIAF_EXAMPLE",
      "eventID": "4b5c42df-1174-46c8-be99-d67_EXAMPLE",
      "readOnly": true,
      "eventType": "AwsApiCall",
      "managementEvent": true,
      "recipientAccountId": "111122223333"
      "eventCategory": "Management"
      }
    }
```

L'exemple suivant montre une entrée de CloudTrail journal qui illustre l'`StartZonalShift`action avec une exception de conflit pour le décalage de zone.

```
{
      "eventVersion": "1.08",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:role/admin",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "sessionIssuer": {
            "type": "Role",
            "principalId": "AROA33L3W36EXAMPLE",
            "arn": "arn:aws:iam::111122223333:role/admin",
            "accountId": "111122223333",
            "userName": "EXAMPLENAME"
          },
          "webIdFederationData": {},
          "attributes": {
            "creationDate": "2022-11-14T16:01:51Z",
            "mfaAuthenticated": "false"
          }
```

```
        }
      },
      "eventTime": "2022-11-14T16:10:38Z",
      "eventSource": "arc-zonal-shift.amazonaws.com",
      "eventName": "StartZonalShift",
     "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.50",
      "userAgent": "Boto3/1.17.101 Python/3.8.10 Linux/4.14.231-180.360.amzn2.x86_64
 exec-env/AWS_Lambda_python3.8 Botocore/1.20.102",
      "errorCode": "ConflictException",
      "errorMessage": "There's already an active zonal shift for that resource
 identifier: 'arn:aws:testservice:us-west-2:077059137270:testResource/456apples'.
 Active zonal shift: 'bac23b74-176e-c073-de8f-484ca508910f'",
      "requestParameters": {
        "resourceIdentifier": "arn:aws:testservice:us-
west-2:077059137270:testResource/456apples",
        "awayFrom": "usw2-az1",
        "expiresIn": "2m",
        "comment": "HIDDEN_FOR_SECURITY_REASONS"
      },
      "responseElements": null,
      "requestID": "OP4OYXZ54HUPMIPGWH_EXAMPLE",
      "eventID": "0bca6660-e999-43a5-9008-EXAMPLE",
      "readOnly": false,
      "eventType": "AwsApiCall",
      "managementEvent": true,
      "recipientAccountId": "111122223333"
      "eventCategory": "Management"
      }
    }
```

Utilisation du décalage zonal avec Amazon EventBridge

À l'aide d'Amazon EventBridge, vous pouvez configurer des règles basées sur des événements qui surveillent vos ressources de transfert de zone et initient des actions ciblées utilisant d'autres services. AWS Par exemple, vous pouvez définir une règle pour l'envoi de notifications par e-mail en signalant un sujet Amazon SNS lorsqu'un changement de zone commence.

Vous pouvez créer des règles dans Amazon EventBridge pour agir sur le décalage zonal. Un événement de changement de zone spécifie les informations d'état relatives aux décalages de zone. Par exemple, un événement est créé lorsque vous commencez un changement de zone.

Pour capturer les événements de décalage de zone spécifiques qui vous intéressent, définissez des modèles spécifiques à l'événement qui EventBridge peuvent être utilisés pour détecter les événements. Les modèles d'événements ont la même structure que les événements auxquels ils correspondent. Le modèle place entre guillemets les champs que vous voulez faire correspondre et fournit les valeurs que vous recherchez.

Les événements sont générés dans la mesure du possible. Ils sont livrés depuis la Route 53 ARC EventBridge en temps quasi réel, dans des circonstances opérationnelles normales. Cependant, des situations peuvent survenir susceptibles de retarder ou d'empêcher la livraison d'un événement.

Pour plus d'informations sur le fonctionnement EventBridge des règles avec les modèles d'événements, consultez la section Événements et modèles d'événements dans EventBridge.

Surveillez une ressource de déplacement zonal avec EventBridge

Avec EventBridge, vous pouvez créer des règles qui définissent les actions à entreprendre lorsque Route 53 ARC émet des événements pour ses ressources. Par exemple, vous pouvez créer une règle qui envoie un message électronique lorsque vous commencez un changement de zone.

Pour taper ou copier-coller un modèle d'événement dans la EventBridge console, sélectionnez l'option Enter my own option dans la console. Pour vous aider à déterminer les modèles d'événements susceptibles de vous être utiles, cette rubrique inclut des exemples de modèles de correspondance d'événements par décalage zonal.

Pour créer une règle pour un événement de ressource

1. Ouvrez la EventBridge console Amazon à l'adresse https://console.aws.amazon.com/events/.
2. Choisissez la région dans Région AWS laquelle vous souhaitez créer la règle, c'est-à-dire la région pour laquelle vous souhaitez suivre des événements.
3. Choisissez Create rule.
4. Entrez un nom et éventuellement une description pour la règle.
5. Pour Event bus, laissez la valeur par défaut, default.
6. Choisissez Suivant.
7. Pour l'étape Créer un modèle d'événement, pour Source d'événement, laissez la valeur par défaut, AWS events.
8. Sous Exemple d'événement, choisissez Enter my own.
9. Pour Exemples d'événements, tapez ou copiez-collez un modèle d'événement.

Exemples de modèles d'événements ARC de la Route 53

Les modèles d'événements ont la même structure que les événements auxquels ils correspondent. Le modèle place entre guillemets les champs que vous voulez faire correspondre et fournit les valeurs que vous recherchez.

- Sélectionnez tous les événements dans le décalage de zone de la Route 53 ARC.

```
{
    "source": [
        "aws.arc-zonal-shift"
    ]
}
```

Spécifiez un groupe de CloudWatch journaux à utiliser comme cible

Lorsque vous créez une EventBridge règle, vous devez spécifier la cible vers laquelle les événements correspondant à la règle sont envoyés. Pour obtenir la liste des cibles disponibles pour EventBridge, consultez la section Cibles disponibles dans la EventBridge console. L'une des cibles que vous pouvez ajouter à une EventBridge règle est un groupe de CloudWatch journaux Amazon. Cette section décrit les exigences relatives à l'ajout de groupes de CloudWatch journaux en tant que cibles et fournit une procédure pour ajouter un groupe de journaux lorsque vous créez une règle.

Pour ajouter un groupe de CloudWatch journaux en tant que cible, vous pouvez effectuer l'une des opérations suivantes :

- Création d'un nouveau groupe de journaux
- Choisissez un groupe de journaux existant

Si vous spécifiez un nouveau groupe de journaux à l'aide de la console lorsque vous créez une règle, le groupe de journaux est EventBridge automatiquement créé pour vous. Assurez-vous que le groupe de journaux que vous utilisez comme cible pour la EventBridge règle commence par`/aws/events`. Si vous souhaitez choisir un groupe de journaux existant, sachez que seuls les groupes de journaux commençant par `/aws/events` apparaissent sous forme d'options dans le menu déroulant. Pour plus d'informations, consultez la section Créer un nouveau groupe de journaux dans le guide de CloudWatch l'utilisateur Amazon.

Si vous créez ou utilisez un groupe de CloudWatch journaux à utiliser comme cible à l'aide d' CloudWatch opérations en dehors de la console, assurez-vous de définir correctement les autorisations. Si vous utilisez la console pour ajouter un groupe de journaux à une EventBridge règle, la politique basée sur les ressources pour le groupe de journaux est automatiquement mise à jour. Toutefois, si vous utilisez le AWS Command Line Interface ou un AWS SDK pour spécifier un groupe de journaux, vous devez mettre à jour la politique basée sur les ressources pour le groupe de journaux. L'exemple de politique suivant illustre les autorisations que vous devez définir dans une stratégie basée sur les ressources pour le groupe de journaux :

```
{
  "Statement": [
    {
      "Action": [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "events.amazonaws.com",
          "delivery.logs.amazonaws.com"
        ]
      },
      "Resource": "arn:aws:logs:region:account:log-group:/aws/events/*:*",
      "Sid": "TrustEventsToStoreLogEvent"
    }
  ],
  "Version": "2012-10-17"
}
```

Vous ne pouvez pas configurer une politique basée sur les ressources pour un groupe de journaux à l'aide de la console. Pour ajouter les autorisations requises à une politique basée sur les ressources, utilisez l'opération CloudWatch PutResourcePolicyAPI. Vous pouvez ensuite utiliser la commande describe-resource-policiesCLI pour vérifier que votre politique a été correctement appliquée.

Pour créer une règle pour un événement de ressource et spécifier une cible de groupe de CloudWatch journaux

1. Ouvrez la EventBridge console Amazon à l'adresse https://console.aws.amazon.com/events/.
2. Choisissez Région AWS celui dans lequel vous souhaitez créer la règle.

3. Choisissez Créer une règle, puis entrez les informations relatives à cette règle, telles que le modèle d'événement ou les détails du calendrier.

   Pour plus d'informations sur la création de EventBridge règles pour Route 53 ARC, consultez les sections précédentes dans cette rubrique.
4. Sur la page Sélectionner une cible, choisissez CloudWatchcomme cible.
5. Choisissez un groupe de CloudWatch journaux dans le menu déroulant.

Identity and Access Management pour le changement de zone dans Amazon Route 53 Application Recovery Controller

AWS Identity and Access Management (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les ressources ARC de la Route 53. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Table des matières

Comment fonctionne le changement de zone avec IAM

Avant d'utiliser IAM pour gérer l'accès au changement de zone dans Amazon Route 53 Application Recovery Controller, découvrez quelles fonctionnalités IAM peuvent être utilisées avec le changement de zone.

Fonctionnalités IAM que vous pouvez utiliser avec le changement de zone

Fonction IAM	Support de changement de zone
Politiques basées sur l’identité	Oui
Politiques basées sur les ressources	Non
Actions de politique	Oui

Fonction IAM	Support de changement de zone
Ressources de politique	Oui
Clés de condition d'une politique	Oui
ACL	Non
ABAC (identifications dans les politiques)	Partielle
Informations d'identification temporaires	Oui
Autorisations de principal	Oui
Fonctions du service	Non
Rôles liés à un service	Oui

Pour obtenir une vue globale de haut niveau du fonctionnement des AWS services avec la plupart des fonctionnalités IAM, consultez la section AWS Services compatibles avec IAM dans le Guide de l'utilisateur IAM.

Politiques basées sur l'identité pour Route 53 ARC

Prend en charge les politiques basées sur l'identité	Oui

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Création de politiques IAM dans le Guide de l'utilisateur IAM.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Vous ne pouvez pas spécifier le principal dans une politique basée sur une identité car celle-ci s'applique à l'utilisateur ou au rôle auquel elle est attachée. Pour découvrir tous les éléments

que vous utilisez dans une politique JSON, consultez Références des éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

Pour consulter des exemples de politiques basées sur l'identité de Route 53 ARC, consultez. Exemples de politiques basées sur l'identité dans Amazon Route 53 Application Recovery Controller

Politiques basées sur les ressources au sein de Route 53 ARC

Prend en charge les politiques basées sur les ressources	Non

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique.

Actions politiques pour le changement de zone

Prend en charge les actions de politique	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Les actions de stratégie portent généralement le même nom que l'opération AWS d'API associée. Il existe quelques exceptions, telles que les actions avec autorisations uniquement qui n'ont pas d'opération API correspondante. Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une stratégie afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour consulter la liste des actions ARC de Route 53 pour le changement de zone, consultez la section Actions définies par Amazon Route 53 Zonal Shift dans la référence d'autorisation de service.

Les actions politiques de Route 53 ARC relatives au changement de zone utilisent les préfixes suivants avant l'action :

```
arc-zonal-shift
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules. Par exemple, ce qui suit :

```
"Action": [
      "arc-zonal-shift:action1",
      "arc-zonal-shift:action2"
         ]
```

Vous pouvez aussi spécifier plusieurs actions à l'aide de caractères génériques (*). Par exemple, pour spécifier toutes les actions qui commencent par le mot `Describe`, incluez l'action suivante :

```
"Action": "arc-zonal-shift:Describe*"
```

Pour consulter des exemples de politiques basées sur l'identité de la Route 53 ARC pour le changement de zone, voir. Exemples de politiques basées sur l'identité pour le changement de zone dans Amazon Route 53 Application Recovery Controller

Ressources politiques pour le changement de zone

Prend en charge les ressources de politique	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

```
"Resource": "*"
```

Pour consulter la liste des types de ressources et de leurs ARN, ainsi que les actions que vous pouvez spécifier avec l'ARN de chaque ressource, consultez la rubrique suivante dans la référence d'autorisation de service :

- Actions définies par Amazon Route 53 - Zonal Shift

Pour connaître les actions et les ressources que vous pouvez utiliser avec une clé de condition, consultez la rubrique suivante dans la référence d'autorisation de service :

- Clés de condition définies par Amazon Route 53 - Zonal Shift

Pour consulter des exemples de politiques basées sur l'identité de la Route 53 ARC pour le changement de zone, voir. Exemples de politiques basées sur l'identité pour le changement de zone dans Amazon Route 53 Application Recovery Controller

Clés de conditions politiques pour le changement de zone

Prend en charge les clés de condition de politique spécifiques au service	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` (ou le bloc `Condition`) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément `Condition` est facultatif. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande.

Si vous spécifiez plusieurs éléments `Condition` dans une instruction, ou plusieurs clés dans un seul élément `Condition`, AWS les évalue à l'aide d'une opération `AND` logique. Si vous spécifiez

plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une `OR` opération logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez accorder à un utilisateur IAM l'autorisation d'accéder à une ressource uniquement si elle est balisée avec son nom d'utilisateur IAM. Pour plus d'informations, consultez Éléments d'une politique IAM : variables et identifications dans le Guide de l'utilisateur IAM.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques au service. Pour voir toutes les clés de condition AWS globales, voir les clés de contexte de condition AWS globales dans le guide de l'utilisateur IAM.

Pour consulter la liste des clés de condition de changement de zone, consultez la rubrique suivante dans la référence d'autorisation de service :

- Clés de condition définies par Amazon Route 53 - Zonal Shift

Pour connaître les actions et les ressources que vous pouvez utiliser avec une clé de condition, consultez les rubriques suivantes dans la référence d'autorisation de service :

- Actions définies par Amazon Route 53 - Zonal Shift
- Types de ressources définis par Amazon Route 53 - Zonal Shift

Pour consulter des exemples de politiques basées sur l'identité de la Route 53 ARC pour le changement de zone, voir. Exemples de politiques basées sur l'identité pour le changement de zone dans Amazon Route 53 Application Recovery Controller

Listes de contrôle d'accès (ACL) dans Route 53 ARC

Prend en charge les listes ACL	Non

Les listes de contrôle d'accès (ACL) vérifient quels principaux (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Contrôle d'accès basé sur les attributs (ABAC) avec Route 53 ARC

Prise en charge d’ABAC (identifications dans les politiques)	Partielle

Le contrôle d’accès basé sur les attributs (ABAC) est une politique d’autorisation qui définit des autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et à de nombreuses AWS ressources. L’étiquetage des entités et des ressources est la première étape d’ABAC. Vous concevez ensuite des politiques ABAC pour autoriser des opérations quand l’identification du principal correspond à celle de la ressource à laquelle il tente d’accéder.

L’ABAC est utile dans les environnements qui connaissent une croissance rapide et pour les cas où la gestion des politiques devient fastidieuse.

Pour contrôler l’accès basé sur des étiquettes, vous devez fournir les informations d’étiquette dans l’élément de condition d’une politique utilisant les clés de condition `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d’informations sur l’ABAC, consultez Qu’est-ce que le contrôle d’accès basé sur les attributs (ABAC) ? dans le Guide de l’utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration de l’ABAC, consultez Utilisation du contrôle d’accès par attributs (ABAC) dans le Guide de l’utilisateur IAM.

Route 53 ARC inclut la prise en charge partielle suivante pour ABAC :

- Le changement de zone prend en charge l'ABAC pour les ressources gérées enregistrées dans Route 53 ARC pour le décalage de zone. Pour plus d'informations sur les ressources gérées par ABAC for Network Load Balancer et Application Load Balancer, consultez la section ABAC with Elastic Load Balancing dans le guide de l'utilisateur d'Elastic Load Balancing.

Utilisation d'informations d'identification temporaires avec Route 53 ARC

Prend en charge les informations d’identification temporaires	Oui

Certains Services AWS ne fonctionnent pas lorsque vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, y compris celles qui Services AWS fonctionnent avec des informations d'identification temporaires, consultez Services AWS la section relative à l'utilisation d'IAM dans le guide de l'utilisateur d'IAM.

Vous utilisez des informations d'identification temporaires si vous vous connectez à l' AWS Management Console aide d'une méthode autre qu'un nom d'utilisateur et un mot de passe. Par exemple, lorsque vous accédez à AWS l'aide du lien d'authentification unique (SSO) de votre entreprise, ce processus crée automatiquement des informations d'identification temporaires. Vous créez également automatiquement des informations d’identification temporaires lorsque vous vous connectez à la console en tant qu’utilisateur, puis changez de rôle. Pour plus d’informations sur le changement de rôle, consultez Changement de rôle (console) dans le Guide de l’utilisateur IAM.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide de l' AWS API AWS CLI or. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour y accéder AWS. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d’informations, consultez Informations d’identification de sécurité temporaires dans IAM.

Autorisations principales interservices pour Route 53 ARC

Prend en charge les sessions d'accès direct (FAS)	Oui

Lorsque vous utilisez une entité IAM (utilisateur ou rôle) pour effectuer des actions AWS, vous êtes considéré comme un mandant. Les politiques accordent des autorisations au principal. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui déclenche une autre action dans un autre service. Dans ce cas, vous devez disposer d’autorisations nécessaires pour effectuer les deux actions.

Pour savoir si une action nécessite des actions dépendantes supplémentaires dans une politique, consultez la rubrique suivante dans la référence d'autorisation de service :

- Changement de zone sur Amazon Route 53

Rôles de service pour Route 53 ARC

Prend en charge les fonctions de service	Non

Une fonction du service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du 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.

Rôles liés à un service pour Route 53 ARC

Prend en charge les rôles liés à un service.	Oui

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 au service apparaissent dans votre Compte AWS fichier et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Le changement de zone n'utilise pas de rôles liés à un service.

IAM et autorisations pour le changement de zone

Cette section fournit des informations supplémentaires sur le fonctionnement des autorisations pour la fonctionnalité de changement de zone dans Amazon Route 53 Application Recovery Controller, en particulier si vous utilisez cette fonctionnalité depuis un autre AWS service, tel qu'Elastic Load Balancing. Pour en savoir plus sur le fonctionnement des fonctionnalités ARC de Route 53 avec l'IAM et les autorisations en général, consultez les informations de la rubrique de présentation,Identity and Access Management pour le changement de zone dans Amazon Route 53 Application Recovery Controller.

Outre les autorisations décrites dans la rubrique de présentation de l'IAM, les règles suivantes s'appliquent au décalage de zone pour l'IAM et aux autorisations :

- Assurez-vous que vous disposez des autorisations requises pour utiliser le décalage de zone dans Route 53 ARC. Pour plus d'informations, consultez les sections Accès à la console de changement de zone et Accès aux opérations de changement de zone.
- Il n'est pas nécessaire d'ajouter des autorisations Elastic Load Balancing supplémentaires avec IAM pour gérer les décalages de zone pour les ressources d'équilibreur de charge gérées dans votre compte dans Route 53 ARC.
- Une politique AWS gérée qui fournit un accès complet à Elastic Load Balancing inclut des autorisations pour travailler avec des décalages de zone. Si vous utilisez des politiques AWS gérées pour accéder à Elastic Load Balancing, vous n'avez pas besoin d'autorisations supplémentaires dans IAM pour le changement de zone pour démarrer des décalages de zone pour les équilibreurs de charge ou pour travailler avec eux dans la console Elastic Load Balancing. Pour plus d'informations, consultez les politiques AWS gérées pour Elastic Load Balancing.

Exemples de politiques basées sur l'identité pour le changement de zone dans Amazon Route 53 Application Recovery Controller

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier les ressources ARC de la Route 53. Ils ne peuvent pas non plus effectuer de tâches à l'aide de l'API AWS Management Console, AWS Command Line Interface (AWS CLI) ou de AWS l'API. Pour octroyer aux utilisateurs des autorisations d’effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L’administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Pour apprendre à créer une politique basée sur l’identité IAM à l’aide de ces exemples de documents de politique JSON, consultez Création de politiques dans l’onglet JSON dans le Guide de l’utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par Route 53 ARC, y compris le format des ARN pour chacun des types de ressources, consultez la section Actions, ressources et clés de condition pour Amazon Route 53 Application Recovery Controller dans le Service Authorization Reference.

Rubriques

- Bonnes pratiques en matière de politiques
- Exemple : accès à la console Zonal Shift
- Exemple : actions de l'API Zonal Shift

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer des ressources Route 53 ARC dans votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez politiques gérées par AWS ou politiques gérées par AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.
- Accorder les autorisations de moindre privilège : lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l'exécution d'une seule tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation de IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utiliser des conditions dans les politiques IAM pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que AWS CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez IAM Access Analyzer pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : IAM Access Analyzer valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez Validation de politique IAM Access Analyzer dans le Guide de l'utilisateur IAM.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue.

Compte AWS Pour exiger le MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Configuration de l'accès aux API protégé par MFA dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

Exemple : accès à la console Zonal Shift

Pour accéder à la console Amazon Route 53 Application Recovery Controller, vous devez disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et d'afficher les détails des ressources ARC de la Route 53 présentes dans votre Compte AWS. Si vous créez une stratégie basée sur l'identité qui est plus restrictive que l'ensemble minimum d'autorisations requis, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs ou rôles) tributaires de cette stratégie.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement l'API AWS CLI ou l' AWS API. Autorisez plutôt l'accès à uniquement aux actions qui correspondent à l'opération d'API qu'ils tentent d'effectuer.

Pour donner aux utilisateurs un accès complet à l'utilisation du décalage de zone dans le AWS Management Console, associez une politique telle que la suivante à l'utilisateur :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                   "arc-zonal-shift:ListManagedResources",
                   "arc-zonal-shift:GetManagedResource",
                   "arc-zonal-shift:ListZonalShifts",
                   "arc-zonal-shift:StartZonalShift",
                   "arc-zonal-shift:UpdateZonalShift",
                   "arc-zonal-shift:CancelZonalShift"
             ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeAvailabilityZones",
```

```
            "Resource": "*"
        }
    ]
}
```

Exemple : actions de l'API Zonal Shift

L'API Zonal Shift déplace temporairement le trafic hors d'une zone de disponibilité pour récupérer une application.

Pour garantir qu'un utilisateur peut utiliser les actions d'API de changement de zone, associez une politique correspondant aux opérations d'API avec lesquelles l'utilisateur doit travailler, telle que la suivante :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                   "arc-zonal-shift:ListManagedResources",
                   "arc-zonal-shift:GetManagedResource",
                   "arc-zonal-shift:ListZonalShifts",
                   "arc-zonal-shift:StartZonalShift",
                   "arc-zonal-shift:UpdateZonalShift",
                   "arc-zonal-shift:CancelZonalShift"
             ],
            "Resource": "*"
        }
    ]
}
```

Autoshift zonal dans le contrôleur de restauration d'applications Amazon Route 53

Avec l'autoshift zonal, vous autorisez AWS le transfert du trafic des ressources d'une application depuis une zone de disponibilité lors d'événements, en votre nom, afin de réduire le délai de restauration. AWS lance un changement automatique lorsque la télémétrie interne indique une altération de la zone de disponibilité susceptible d'avoir un impact sur les clients. Lorsqu'un transfert

automatique AWS démarre, le trafic des applications vers les ressources que vous avez configurées pour le transfert automatique zonal commence à s'éloigner de la zone de disponibilité.

Sachez que la Route 53 ARC n'inspecte pas l'état des ressources individuelles. AWS lance un changement automatique lorsque la AWS télémétrie détecte une altération de la zone de disponibilité susceptible d'avoir un impact sur les clients. Dans certains cas, le trafic peut être transféré vers des ressources qui ne subissent aucun impact.

Avec l'autoshift zonal, vous autorisez AWS également le transfert du trafic des ressources d'une application depuis une zone de disponibilité, en votre nom, pour des essais réguliers. Des essais d'entraînement sont nécessaires pour le changement automatique zonal. Les changements de zone initiés par la Route 53 ARC pour les essais vous aident à vous assurer que le fait de vous éloigner du trafic d'une zone de disponibilité lors d'un changement automatique est sans danger pour votre application. Des tests pratiques permettent de vérifier régulièrement que votre application peut fonctionner normalement sans zone de disponibilité en déclenchant des décalages de zone qui déplacent le trafic vers une ressource hors d'une zone de disponibilité. Les séances d'entraînement ont lieu chaque semaine et fournissent un résultat, tel que `SUCCEEDED` ou, pour vous `FAILED` aider à comprendre si l'application fonctionne comme prévu.

> **⚠ Important**
>
> Avant de configurer les exécutions pratiques ou d'activer l'autoshift zonal, nous vous recommandons vivement de prédimensionner la capacité des ressources de votre application dans toutes les zones de disponibilité de la région où les ressources de vos applications sont déployées. Vous ne devez pas vous fier à la mise à l'échelle à la demande lorsqu'un passage automatique ou un entraînement commence. L'autoshift zonal, y compris les essais, fonctionne indépendamment et n'attend pas la fin des actions de mise à l'échelle automatique. Si vous optez pour le dimensionnement automatique plutôt que pour le dimensionnement préalable, la restauration de votre application peut prendre plus de temps. Si vous utilisez la mise à l'échelle automatique pour gérer des cycles de trafic réguliers, nous vous recommandons vivement de configurer la capacité minimale de votre mise à l'échelle automatique pour continuer à fonctionner normalement en cas de perte d'une zone de disponibilité.

Si vous prévoyez d'activer le décalage automatique par zone ou de configurer des exécutions pratiques, après avoir prédimensionné la capacité des ressources de votre application, vérifiez que

votre application peut fonctionner normalement sans zone de disponibilité. Pour tester cela, lancez un changement de zone afin de déplacer le trafic vers une ressource hors d'une zone de disponibilité.

Pour garantir l'efficacité de vos tests avec changement de zone, il est important de vérifier que le trafic s'écoule comme prévu en provenance de l'AZ que vous quittez. Les équilibreurs de charge d'application et les équilibreurs de charge réseau fournissent des métriques par AZ sur Amazon CloudWatch que vous pouvez utiliser pour surveiller cela. En fonction de la durée pendant laquelle un service et les clients réutilisent les connexions, le trafic peut continuer à atteindre l'AZ que vous avez quitté plus longtemps que prévu. Pour en savoir plus, consultez Limitez le temps pendant lequel les clients restent connectés à vos terminaux.

Une fois que vous avez vérifié, en démarrant et en évaluant un changement de zone, que votre application peut continuer à fonctionner normalement même si le trafic est déplacé hors d'une zone de disponibilité, les essais réguliers effectués par Route 53 ARC vous aident à confirmer, de manière continue, que vous disposez d'une capacité suffisante pour effectuer un changement automatique.

En plus d'activer l'autoshift zonal pour une ressource d'équilibreur de charge dans la console Route 53 ARC, vous avez la possibilité d'activer l'autoshift zonal pour un équilibreur de charge spécifique dans la console Amazon EC2. Pour en savoir plus sur l'activation de l'autoshift zonal avec Elastic Load Balancing, voir Zonal Shift dans le guide de l'utilisateur d'Elastic Load Balancing.

Les changements de zone automatiques et les changements de zone pour essais sont temporaires. Avec les transferts automatiques, lorsque la zone de disponibilité affectée se rétablit, le trafic destiné aux ressources AWS cesse d'être transféré hors de la zone de disponibilité. Le trafic des applications pour les clients revient vers toutes les zones de disponibilité de la région. Lors d'une séance d'entraînement, le trafic est déplacé hors d'une zone de disponibilité pour une seule ressource pendant environ 30 minutes, puis redirigé vers toutes les zones de disponibilité de la région.

Vous pouvez configurer les EventBridge notifications Amazon pour vous avertir des changements automatiques et des séances d'entraînement. Pour plus d’informations, consultez Utilisation de l'autoshift zonal avec Amazon EventBridge.

Comment fonctionnent l'autoshift zonal et les courses d'entraînement

La fonctionnalité de transfert automatique zonal d'Amazon Route 53 Application Recovery Controller permet de AWS transférer le trafic d'une ressource hors d'une zone de disponibilité, en votre nom, lorsqu'il est AWS déterminé qu'une défaillance est susceptible d'affecter les clients de la zone de disponibilité. L'autoshift zonal est conçu pour une ressource pré-dimensionnée dans toutes les zones

de disponibilité d'un an Région AWS, afin qu'une application puisse fonctionner normalement en cas de perte d'une zone de disponibilité.

Avec l'autoshift zonal, vous devez configurer des courses d'entraînement, au cours desquelles la Route 53 ARC déplace régulièrement le trafic vers la ressource hors d'une zone de disponibilité. Route 53 ARC planifie des séances d'entraînement environ une fois par semaine pour chaque ressource associée à une configuration d'entraînement. Les séances d'entraînement pour chaque ressource sont planifiées indépendamment.

Pour chaque course d'entraînement, la Route 53 ARC enregistre un résultat. Si un essai est interrompu par une condition bloquante, le résultat de l'essai n'est pas marqué comme réussi. Pour plus d'informations sur les résultats des essais, consultez la section Résultats des essais.

Vous pouvez configurer les EventBridge notifications Amazon pour qu'elles vous envoient des informations sur les changements automatiques et les entraînements. Pour plus d'informations, consultez Utilisation de l'autoshift zonal avec Amazon EventBridge.

Rubriques

- Quand AWS démarre et arrête les changements automatiques
- Lorsque la Route 53 ARC planifie, commence et se termine, les séances d'entraînement
- Priorité pour les changements de zone, les essais d'entraînement et les changements automatiques
- Arrêt d'un changement automatique actif ou d'un entraînement pour une ressource
- Comment le trafic est redirigé
- Alarmes pour les séances d'entraînement
- Dates bloquées et fenêtres bloquées (UTC)

Quand AWS démarre et arrête les changements automatiques

Lorsque vous activez le transfert automatique zonal pour une ressource, vous autorisez AWS le transfert du trafic des ressources d'une application depuis une zone de disponibilité lors d'événements, en votre nom, afin de réduire le délai de restauration.

Pour ce faire, l'autoshift zonal utilise la AWS télémétrie pour détecter, le plus tôt possible, toute altération de la zone de disponibilité susceptible d'avoir un impact sur les clients. Lorsqu'un transfert automatique AWS démarre, le trafic vers les ressources configurées commence

immédiatement à s'éloigner de la zone de disponibilité altérée, ce qui pourrait avoir un impact sur les clients.

L'autoshift zonal est une fonctionnalité conçue pour les clients qui ont prédimensionné leurs ressources applicatives pour toutes les zones de disponibilité d'un. Région AWS Vous ne devez pas vous fier à la mise à l'échelle à la demande lorsqu'un passage automatique ou un entraînement commence.

AWS met fin à un changement automatique lorsqu'il détermine que la zone de disponibilité est rétablie.

Lorsque la Route 53 ARC planifie, commence et se termine, les séances d'entraînement

Route 53 ARC planifie une course d'entraînement pour une ressource chaque semaine, pendant environ 30 minutes. Route 53 ARC planifie, démarre et gère les essais pour chaque ressource de manière indépendante. Route 53 ARC ne regroupe pas les essais d'entraînement pour les ressources d'un même compte.

Lorsqu'une séance d'entraînement se poursuit pendant la durée prévue, sans interruption, elle est marquée par un résultat de`SUCCESSFUL`. Plusieurs autres résultats sont possibles : `FAILED`, et`INTERRUPTED`. `PENDING` Les valeurs et les descriptions des résultats sont incluses dans la section Résultats des essais.

Dans certains scénarios, la Route 53 ARC interrompt un entraînement et y met fin. Par exemple, si un changement automatique démarre pendant un entraînement, Route 53 ARC interrompt l'entraînement et y met fin. Autre exemple, supposons que la ressource réagit négativement à un entraînement et déclenche une alarme que vous avez spécifiée pour surveiller le passage à un `ALARM` état de l'entraînement. Dans ce scénario, la Route 53 ARC interrompt également l'entraînement et y met fin.

En outre, il existe plusieurs scénarios dans lesquels Route 53 ARC ne démarre pas un exercice d'entraînement de planification pour une ressource.

En réponse à des essais d'entraînement interrompus et bloqués pour une ressource, Route 53 ARC effectue les opérations suivantes :

- Si une course d'entraînement pour une ressource est interrompue alors qu'elle est en cours, Route 53 ARC considère que la course d'entraînement hebdomadaire est terminée et planifie une nouvelle course d'entraînement pour la ressource pour la semaine suivante. Le résultat de l'entraînement hebdomadaire correspond `INTERRUPTED` à ce scénario, non`FAILED`. Le résultat

de l'entraînement est défini sur `FAILED` uniquement lorsque l'alarme de résultat qui surveille l'entraînement passe à un `ALARM` état pendant l'entraînement.

- S'il existe une contrainte de blocage lorsqu'il est prévu de démarrer un entraînement pour une ressource, Route 53 ARC ne démarre pas l'entraînement. Route 53 ARC continue de surveiller régulièrement, afin de déterminer s'il existe toujours une ou plusieurs contraintes de blocage. Lorsqu'il n'y a aucune contrainte de blocage, Route 53 ARC lance l'entraînement pour la ressource.

Voici des exemples de contraintes de blocage qui empêchent Route 53 ARC de démarrer ou de poursuivre un entraînement pour une ressource :

- Route 53 ARC ne démarre ni ne poursuit les essais lorsqu'une AWS Fault Injection Service expérience est en cours. Si un AWS FIS événement est actif alors que Route 53 ARC a planifié le début d'une course d'entraînement, Route 53 ARC ne démarre pas la course d'entraînement. Route 53 ARC surveille tout au long des essais les contraintes de blocage, y compris un AWS FIS événement. Si un AWS FIS événement commence alors qu'une course d'entraînement est active, Route 53 ARC met fin à la course d'entraînement et n'essaie pas d'en démarrer une autre avant la prochaine course d'entraînement régulièrement planifiée pour la ressource.
- S'il y a un AWS événement en cours dans une région, la Route 53 ARC ne commence pas les courses d'entraînement pour les ressources, mais met fin aux courses d'entraînement actives dans la région.

Lorsque la course d'entraînement se termine sans être interrompue, la Route 53 ARC planifie la prochaine course d'entraînement dans une semaine, comme d'habitude. Si une course d'entraînement n'est pas démarrée en raison d'une contrainte de blocage, telle qu'une AWS FIS expérience ou une fenêtre temporelle bloquée que vous avez spécifiée, Route 53 ARC continue de tenter de démarrer une course d'entraînement jusqu'à ce que celle-ci puisse être démarrée.

Priorité pour les changements de zone, les essais d'entraînement et les changements automatiques

Il ne peut y avoir qu'un seul changement de trafic pour une ressource qui est effectif à la fois, c'est-à-dire un seul changement de zone d'entraînement, un changement de zone initié par le client ou un transfert automatique pour la ressource. Lorsque plusieurs changements de trafic sont en cours, Route 53 ARC suit une priorité pour déterminer quel changement de trafic est en vigueur pour une ressource.

Le principe général de la priorité est que les changements de zone que vous commencez en tant que client ont priorité sur les changements automatiques, qui ont priorité sur les essais. C'est-à-dire que les changements de zone initiés par le client > les changements automatiques > les changements de zone s'entraînent à exécuter des changements de zone.

Pour illustrer cela, voici comment fonctionne la priorité pour quelques exemples de scénarios :

- Si un changement automatique est actif et que vous commencez un changement de zone pour une ressource pour laquelle le changement automatique est activé, le décalage de zone que vous commencez est. `APPLIED` La ressource est désormais déplacée hors de la zone de disponibilité à laquelle s'applique le changement de zone. Si le décalage de zone se AWS termine avant la fin du décalage automatique, le décalage automatique devient le changement de rapport. `APPLIED` La ressource est donc déplacée hors de la zone de disponibilité où le transfert automatique AWS est en cours.
- S'il existe un changement de zone actif que vous lancez pour une ressource pour laquelle le décalage automatique est activé et que vous lancez un AWS changement automatique, le décalage automatique existe pour la ressource. Toutefois, le décalage de zone est réglé sur `APPLIED` et le décalage automatique est réglé sur `NOT APPLIED` jusqu'à ce que le décalage de zone soit terminé. Ensuite, le statut du changement automatique est mis à jour `APPLIED` et le changement automatique déplace le trafic vers la ressource jusqu'à la AWS fin du changement automatique.
- S'il y a un exercice d'entraînement actif pour une ressource et que vous entamez un changement de zone pour la ressource qui déplace le trafic vers la même zone de disponibilité, le cycle d'entraînement est interrompu. Si vous entamez un changement de zone qui déplace le trafic vers une autre zone de disponibilité, les essais se poursuivent comme d'habitude.
- S'il y a un changement de zone actif pour une ressource et qu'il est prévu que Route 53 ARC commence une course d'entraînement, celle-ci est reportée d'une heure. Route 53 ARC tente ensuite à nouveau de démarrer la course d'entraînement. Route 53 ARC continue de vérifier toutes les heures jusqu'à ce qu'une course d'entraînement puisse commencer.

Le changement de trafic actuellement en vigueur pour la ressource a un statut de décalage zonal appliqué défini sur. `APPLIED` Un seul quart de travail est défini `APPLIED` à la fois. Les autres changements en cours sont programmés pour`ACTIVE`.

Arrêt d'un changement automatique actif ou d'un entraînement pour une ressource

Pour arrêter un changement automatique en cours pour une ressource, désactivez le décalage automatique zonal pour la ressource.

Lorsque vous désactivez l'autoshift zonal, la configuration des exercices pratiques pour la ressource n'est pas affectée. Des séances d'entraînement régulières ont toujours lieu pour la ressource, selon le même calendrier. Si vous souhaitez arrêter les essais en plus de désactiver les changements automatiques, vous devez supprimer la configuration des essais associés à la ressource.

Lorsque vous supprimez une configuration d'entraînement, AWS cesse d'effectuer des essais qui déplacent le trafic de la ressource hors d'une zone de disponibilité chaque semaine. En outre, étant donné que le décalage automatique zonal nécessite des essais, lorsque vous supprimez une configuration d'entraînement à l'aide de la console Route 53 ARC, cette action désactive également le décalage automatique zonal pour la ressource. Notez toutefois que si vous utilisez l'API zonal autoshift pour supprimer un exercice d'entraînement, vous devez d'abord désactiver le décalage automatique zonal pour la ressource.

Pour arrêter un entraînement actif, annulez le changement de zone du cycle d'entraînement. Pour plus d’informations, consultez Annulation d'un entraînement : changement de zone.

Comment le trafic est redirigé

Pour les changements de zone automatiques et les changements de zone effectués par entraînement, le trafic est transféré hors d'une zone de disponibilité en utilisant le même mécanisme que celui utilisé par Route 53 ARC pour les changements de zone initiés par le client. Pour déplacer le trafic hors d'une zone de disponibilité pour les équilibreurs de charge dont l'équilibrage de charge entre zones est désactivé, Route 53 ARC définit le bilan de santé de l'équilibreur de charge pour la zone de disponibilité sur un état défectueux, de sorte que celui-ci échoue. Un bilan de santé défaillant entraîne à son tour le retrait par Amazon Route 53 des adresses IP correspondantes à la ressource du DNS, de sorte que le trafic est redirigé depuis la zone de disponibilité. Les nouvelles connexions sont désormais routées vers d'autres zones de disponibilité Région AWS .

Avec un changement automatique, lorsqu'une zone de disponibilité se rétablit et AWS décide de mettre fin au changement automatique, Route 53 ARC inverse le processus de vérification de l'état, demandant que les bilans de santé de la Route 53 soient annulés. Les adresses IP zonales d'origine sont ensuite restaurées et, si les contrôles de santé continuent de fonctionner correctement, la zone de disponibilité est à nouveau incluse dans le routage de l'équilibreur de charge.

Il est important de savoir que les changements automatiques ne sont pas basés sur des contrôles de santé qui surveillent l'état sous-jacent des équilibreurs de charge ou des applications. Route 53 ARC utilise des bilans de santé pour éloigner le trafic des zones de disponibilité, en demandant que les bilans de santé soient définis comme non sains, puis rétablit les bilans de santé à la normale lorsqu'elle met fin à un changement automatique ou à un changement de zone.

Alarmes pour les séances d'entraînement

Vous pouvez spécifier deux CloudWatch alarmes pour les essais en mode automatique zonal. La première alarme, l'alarme de résultat, est requise. Vous devez configurer l'alarme de résultat pour surveiller l'état de votre application lorsque le trafic est déplacé hors d'une zone de disponibilité au cours de chaque essai de 30 minutes.

Pour qu'un exercice d'entraînement soit efficace, spécifiez comme alarme de résultat une CloudWatch alarme qui surveille les mesures relatives à la ressource, ou à votre application, qui répondent à un `ALARM` état lorsque votre application est affectée négativement par la perte d'une zone de disponibilité. Pour plus d'informations, consultez la section Alarmes que vous spécifiez pour les séances d'entraînement dansBonnes pratiques lors de la configuration de l'autoshift zonal.

L'alarme de résultat fournit également des informations sur le résultat de la course d'entraînement que Route 53 ARC indique pour chaque course d'entraînement. Si l'alarme entre dans un `ALARM` état, le cycle d'entraînement est terminé et le résultat de l'essai est renvoyé sous la forme`FAILED`. Si le cycle d'entraînement termine la période de test planifiée de 30 minutes et que l'alarme de résultat n'entre pas dans un `ALARM` état, le résultat est renvoyé sous la forme`SUCCEEDED`. Une liste de toutes les valeurs de résultats, avec des descriptions, est fournie dans la section Résultats des essais.

Vous pouvez éventuellement définir une deuxième alarme, l'alarme de blocage. L'alarme de blocage bloque l'entraînement dès le démarrage ou la poursuite lorsqu'elle est dans un `ALARM` état. Cette alarme empêche le démarrage des changements de trafic d'entraînement et arrête tout entraînement en cours lorsque l'alarme est activée. `ALARM`

Par exemple, dans une architecture de grande envergure comportant plusieurs microservices, lorsqu'un microservice rencontre un problème, vous souhaitez généralement arrêter toutes les autres modifications apportées à l'environnement de l'application, y compris le blocage des exécutions pratiques.

Dates bloquées et fenêtres bloquées (UTC)

Vous avez la possibilité de bloquer les séances d'entraînement pour des dates calendaires spécifiques ou pour des créneaux horaires spécifiques, c'est-à-dire des jours et des heures, en UTC.

Par exemple, si le lancement d'une mise à jour de l'application est prévu pour le 1er mai 2024 et que vous ne souhaitez pas que les séances d'entraînement réduisent le trafic à ce moment-là, vous pouvez définir une date de blocage pour`2024-05-01`.

Ou imaginons que vous publiez des résumés de rapports commerciaux trois jours par semaine. Pour ce scénario, vous pouvez définir les jours et heures récurrents suivants comme fenêtres bloquées, par exemple, en UTC :`MON-20:30-21:30 WED-20:30-21:30 FRI-20:30-21:30`.

À propos de Zonal Autoshift

L'autoshift zonal est une fonctionnalité qui AWS déplace le trafic des ressources applicatives hors d'une zone de disponibilité, en votre nom. AWS lance un changement automatique lorsque la télémétrie interne indique une altération de la zone de disponibilité susceptible d'avoir un impact sur les clients. La télémétrie interne intègre des métriques provenant de plusieurs sources, notamment le AWS réseau et les services Amazon EC2 et Elastic Load Balancing.

Vous pouvez activer l'autoshift zonal pour les équilibreurs de charge réseau et les équilibreurs de charge d'application lorsque l'équilibrage de charge entre zones est désactivé.

Lorsque vous déployez et exécutez AWS des applications sur des équilibreurs de charge dans plusieurs zones (généralement trois) d'une région, et que vous les dimensionnez à l'avance pour garantir une stabilité statique, vous AWS pouvez rapidement récupérer les applications clients dans une zone de zone en transférant le trafic grâce à un transfert automatique. En transférant le trafic des ressources vers d'autres zones de la région, AWS vous pouvez réduire la durée et la gravité de l'impact potentiel causé par des pannes de courant, des problèmes matériels ou logiciels dans une zone de disponibilité ou d'autres déficiences.

Lorsque AWS commence un transfert automatique pour une ressource d'équilibrage de charge, Route 53 ARC définit les tests de santé d'Amazon Route 53 sur un état défectueux pour les adresses IP correspondantes pour la ressource d'équilibrage de charge, de sorte que le trafic de la ressource n'est plus dirigé vers l'AZ. Lorsqu'il est AWS déterminé que l'AZ est prête pour le retour du trafic des applications, Route 53 ARC rétablit les bilans de santé de la Route 53 et les adresses IP zonales d'origine sont restaurées.

Lorsque vous activez l'autoshift zonal pour une ressource, vous devez également configurer un exercice d'entraînement pour la ressource. AWS effectue des séances d'entraînement environ une fois par semaine, pendant 30 minutes, afin de vous assurer que vous disposez d'une capacité suffisante pour exécuter votre application sans l'une des zones de disponibilité de la région.

Comme dans le cas du changement de zone, il existe quelques scénarios spécifiques dans lesquels le changement automatique de zone n'éloigne pas le trafic de l'AZ. Par exemple, si les groupes cibles de l'équilibreur de charge dans les AZ ne possèdent aucune instance, ou si toutes les instances ne fonctionnent pas correctement, l'équilibreur de charge est en état d'échec ouvert et vous ne pouvez pas déplacer l'un des AZ.

Pour en savoir plus sur l'autoshift zonal, voir. Autoshift zonal dans le contrôleur de restauration d'applications Amazon Route 53

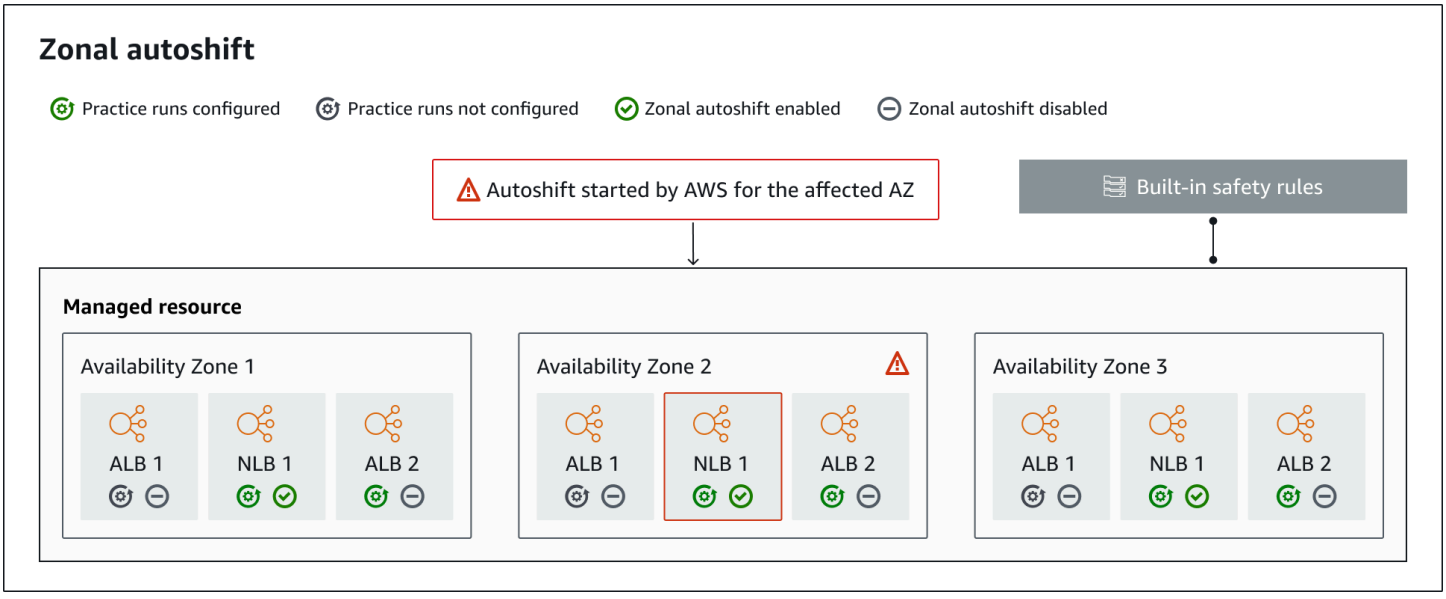
Région AWS disponibilité de l'autoshift zonal

L'autoshift zonal est actuellement disponible dans la publicité. Régions AWS

Pour obtenir des informations détaillées sur le support régional et les points de terminaison de service pour Amazon Route 53 Application Recovery Controller, consultez la section Points de terminaison et quotas Amazon Route 53 Application Recovery Controller dans le manuel Amazon Web Services General Reference.

Composants de changement automatique zonaux

Le schéma suivant illustre un exemple de transfert automatique qui déplace le trafic hors d'une zone de disponibilité. AWS lance un changement automatique lorsque la télémétrie interne indique une altération de la zone de disponibilité susceptible d'avoir un impact sur les clients.



Voici les composants des fonctionnalités de changement automatique zonal de Route 53 ARC.

Autoshift zonal

L'autoshift zonal déplace le trafic vers une ressource, sans que vous ayez à effectuer aucune action. L'autoshift zonal est une fonctionnalité de Route 53 ARC qui permet de AWS démarrer un changement automatique lorsque la télémétrie interne indique une altération de la zone de disponibilité susceptible d'avoir un impact sur les clients. Sachez que, dans certains cas, des ressources peuvent être transférées sans que cela n'ait d'impact.

Pistes d'entraînement

Lorsque vous activez l'autoshift zonal pour une ressource, vous devez également configurer des essais pratiques de décalage automatique zonal pour la ressource. AWS effectue un changement de zone pour les séances d'entraînement environ une fois par semaine, pendant environ 30 minutes. Les exécutions pratiques garantissent que votre application peut fonctionner normalement en cas de perte d'une zone de disponibilité. Lors d'un essai, AWS déplace le trafic d'une ressource hors d'une zone de disponibilité par un changement de zone, puis redirige le trafic à la fin du cycle d'entraînement.

Entraînez-vous à exécuter la configuration

Une configuration d'entraînement définit les dates et les fenêtres bloquées, le cas échéant, ainsi que les CloudWatch alarmes que vous spécifiez pour l'entraînement d'une ressource dans Zonal Autoshift. Vous pouvez modifier un exercice d'entraînement à tout moment, pour ajouter ou modifier des dates ou des fenêtres bloquées, ou pour mettre à jour les alarmes relatives à l'entraînement.

Pour activer l'autoshift zonal, vous devez disposer d'une configuration d'entraînement pour une ressource. Vous pouvez également supprimer un essai d'entraînement. Pour supprimer une configuration d'entraînement pour une ressource, le décalage automatique zonal doit être désactivé.

Entraînez-vous à courir avec alarme

Lorsque vous configurez des exercices pratiques, vous spécifiez les CloudWatch alarmes que vous créez dans CloudWatch, en fonction des besoins en ressources et en applications. Les alarmes que vous spécifiez peuvent bloquer le démarrage d'un exercice d'entraînement ou peuvent arrêter un entraînement en cours si votre application est affectée négativement par l'entraînement.

Si une alarme que vous spécifiez passe à un `ALARM` état, Route 53 ARC met fin au décalage de zone pour la course d'entraînement, de sorte que le trafic de la ressource n'est plus éloigné de la zone de disponibilité.

Vous pouvez spécifier deux types d'alarmes pour les exercices pratiques : une alarme de résultat, pour surveiller l'état de votre ressource et de votre application pendant l'entraînement, et une alarme de blocage, que vous pouvez configurer pour empêcher le démarrage des exercices d'entraînement ou pour arrêter un entraînement en cours. L'alarme de résultat est obligatoire ; l'alarme de blocage est facultative.

Résultat de la course d'entraînement

Route 53 ARC rapporte un résultat pour chaque course d'entraînement. Les résultats possibles de l'entraînement sont les suivants :

- EN ATTENTE : Le changement de zone pour l'entraînement est actif (en cours). Il n'y a pas encore de résultat à obtenir.
- SUCCÈS : L'alarme de résultat n'est pas entrée dans un `ALARM` état pendant l'essai, et le cycle d'entraînement a terminé la période de test complète de 30 minutes.
- INTERROMPU : La séance d'entraînement s'est terminée pour une raison qui n'était pas le fait que l'alarme entrait dans un `ALARM` état. Une course d'entraînement peut être interrompue pour diverses raisons. Par exemple, une séance d'entraînement qui se termine parce que l'alarme de blocage spécifiée pour l'essai est entrée dans un `ALARM` état a pour résultat`INTERRUPTED`. Pour plus d'informations sur les raisons d'un `INTERRUPTED` résultat, voir Résultats pour les essais.
- ÉCHEC : L'alarme de résultat est entrée dans un `ALARM` état pendant l'entraînement.

Règles de sécurité intégrées

Les règles de sécurité intégrées à la Route 53 ARC empêchent que plusieurs changements de trafic soient effectués simultanément pour une ressource. En d'autres termes, un seul changement de zone initié par le client, un changement de zone par entraînement ou un changement automatique pour la ressource peuvent entraîner un transfert actif du trafic hors d'une zone de disponibilité. Par exemple, si vous commencez un changement de zone pour une ressource alors qu'elle est actuellement déplacée avec le décalage automatique, votre changement de zone est prioritaire. Pour plus d'informations, consultez la section Résultats des essais.

Identificateur de ressource

L'identifiant d'une ressource pour laquelle le changement automatique zonal est activé, qui est le nom de ressource Amazon (ARN) de la ressource.

Vous ne pouvez activer le transfert automatique zonal que pour les ressources de votre compte appartenant à un AWS service pris en charge par Route 53 ARC. Les ressources prises en charge dans ces AWS services sont automatiquement enregistrées auprès de Route 53 ARC par le AWS service.

> **Note**
>
> Vous ne pouvez configurer l'autoshift zonal que pour les équilibreurs de charge réseau et les équilibreurs de charge d'application lorsque l'équilibrage de charge entre zones est désactivé.

Ressource gérée

AWS les services enregistrent automatiquement les ressources auprès de Route 53 ARC pour le changement automatique zonal. Une ressource enregistrée est une ressource gérée dans Route 53 ARC.

Nom de la ressource

Nom d'une ressource gérée dans Route 53 ARC.

Statut appliqué

Un statut appliqué indique si un changement de trafic est en cours pour une ressource. Lorsque vous configurez le changement automatique de zone, une ressource peut avoir plusieurs transferts de trafic actifs, à savoir un décalage de zone exécuté par entraînement, un changement de zone initié par le client ou un décalage automatique. Cependant, une seule est appliquée, c'est-à-dire qu'elle est en vigueur pour la ressource à la fois. Le changement ayant le statut `APPLIED` détermine la zone de disponibilité dans laquelle le trafic applicatif a été transféré pour une ressource, et la date à laquelle ce transfert de trafic prend fin.

Plans de données et de contrôle pour le changement automatique par zone

Lorsque vous planifiez le basculement et la reprise après sinistre, évaluez la résilience de vos mécanismes de basculement. Nous vous recommandons de vous assurer que les mécanismes sur

lesquels vous comptez lors du basculement sont hautement disponibles, afin de pouvoir les utiliser lorsque vous en avez besoin en cas de sinistre. En règle générale, vous devez utiliser les fonctions du plan de données pour vos mécanismes chaque fois que vous le pouvez, pour une fiabilité et une tolérance aux pannes optimales. Dans cette optique, il est important de comprendre comment les fonctionnalités d'un service sont réparties entre les plans de contrôle et les plans de données, et de comprendre dans quels cas vous pouvez compter sur une fiabilité extrême en ce qui concerne le plan de données d'un service.

En général, un plan de contrôle vous permet d'exécuter des fonctions de gestion de base, telles que la création, la mise à jour et la suppression de ressources dans le service. Un plan de données fournit les fonctionnalités de base d'un service.

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

Tarification de l'autoshift zonal dans Amazon Route 53 Application Recovery Controller

Dans le cas du transfert automatique zonal, AWS déplace le trafic d'une zone de disponibilité en votre nom vers les ressources prises en charge lorsqu'il est AWS déterminé qu'un problème potentiel peut avoir une incidence négative sur les applications des clients. L'activation de l'autoshift zonal est gratuite.

Vous ne payez que pour ce que vous utilisez dans Amazon Route 53 Application Recovery Controller. Pour obtenir des informations détaillées sur les tarifs de Route 53 ARC et des exemples de tarification, consultez la section Tarification d'Amazon Route 53 et faites défiler la page vers le bas jusqu'à Amazon Route 53 Application Recovery Controller.

Bonnes pratiques lors de la configuration de l'autoshift zonal

Tenez compte des meilleures pratiques et considérations suivantes lorsque vous activez le changement automatique de zone dans Amazon Route 53 Application Recovery Controller.

Le changement automatique de zone comprend deux types de changements de circulation : les changements automatiques et les changements de zone pour entraînement.

- Le transfert automatique AWS permet de réduire le délai de restauration en transférant le trafic des ressources applicatives depuis une zone de disponibilité lors d'événements, en votre nom.

- Avec les courses d'entraînement, la Route 53 ARC amorce un changement de zone en votre nom. Le changement de zone déplace le trafic hors d'une zone de disponibilité pour une ressource, et inversement, selon une cadence hebdomadaire. Les essais pratiques vous aident à vous assurer que vous avez suffisamment augmenté la capacité des zones de disponibilité d'une région pour que votre application puisse tolérer la perte d'une zone de disponibilité.

Il existe plusieurs bonnes pratiques et considérations à prendre en compte en ce qui concerne les changements de vitesse automatiques et les essais d'entraînement. Consultez les rubriques suivantes avant d'activer le changement automatique par zone ou de configurer des essais pratiques pour une ressource.

Rubriques

Limitez le temps pendant lequel les clients restent connectés à vos terminaux

Lorsqu'Amazon Route 53 Application Recovery Controller déplace le trafic pour éviter une perturbation, par exemple en utilisant le décalage de zone ou le décalage automatique de zone, le mécanisme utilisé par Route 53 ARC pour déplacer le trafic de votre application est une mise à jour DNS. Une mise à jour du DNS entraîne le renvoi de toutes les nouvelles connexions hors de la zone affectée. Cependant, les clients disposant de connexions ouvertes préexistantes peuvent continuer à faire des demandes concernant l'emplacement altéré jusqu'à ce qu'ils se reconnectent. Pour garantir un rétablissement rapide, nous vous recommandons de limiter la durée pendant laquelle les clients restent connectés à vos terminaux.

Si vous utilisez un Application Load Balancer, vous pouvez utiliser `keepalive` cette option pour configurer la durée des connexions. Nous vous suggérons de réduire la `keepalive` valeur pour qu'elle corresponde à votre objectif de temps de restauration pour votre application, par exemple 300 secondes. Lorsque vous choisissez une `keepalive` heure, considérez que cette valeur représente un compromis entre une reconnexion plus fréquente en général, ce qui peut affecter le temps de latence, et le fait de déplacer plus rapidement tous les clients d'une zone ou d'une région affectée.

Pour plus d'informations sur la définition de l'`keepalive`option Application Load Balancer, consultez la durée de conservation du client HTTP dans le Guide de l'utilisateur de l'Application Load Balancer.

Prédimensionnez la capacité de vos ressources et testez l'évolution du trafic

Lorsque AWS vous déplacez le trafic d'une zone de disponibilité pour un transfert de zone ou un transfert automatique, il est important que les zones de disponibilité restantes puissent répondre aux taux de demandes accrus pour votre ressource. Ce modèle est connu sous le nom de stabilité statique. Pour plus d'informations, consultez le livre blanc sur la stabilité statique à l'aide des zones de disponibilité dans la bibliothèque Amazon Builder.

Par exemple, si votre application a besoin de 30 instances pour servir ses clients, vous devez en fournir 15 dans trois zones de disponibilité, pour un total de 45 instances. Ce faisant, when AWS déplace le trafic d'une zone de disponibilité (avec un transfert automatique ou lors d'un entraînement)AWS peut toujours servir les clients de votre application avec le total de 30 instances restantes, réparties dans deux zones de disponibilité.

La fonctionnalité de transfert automatique zonal de Route 53 ARC vous aide à vous remettre rapidement des AWS événements survenus dans une zone de disponibilité lorsque vous avez une application dont les ressources sont prédimensionnées pour fonctionner normalement en cas de perte d'une zone de disponibilité. Avant d'activer le transfert automatique zonal pour une ressource, augmentez la capacité de votre ressource dans toutes les zones de disponibilité configurées dans un. Région AWS Commencez ensuite les changements de zone pour la ressource, afin de vérifier que votre application fonctionne toujours normalement lorsque le trafic est déplacé hors d'une zone de disponibilité.

Après avoir testé avec des décalages de zone, activez le décalage automatique zonal et configurez les essais pratiques pour les ressources de l'application. Des séances d'entraînement régulières avec changement automatique par zone vous aident à vous assurer, sur une base continue, que votre capacité est toujours adaptée. Avec une capacité suffisante dans toutes les zones de disponibilité, votre application peut continuer à servir les clients, sans interruption, pendant un transfert automatique.

Pour plus d'informations sur le lancement d'un changement de zone pour une ressource, consultezChangement de zone dans Amazon Route 53 Application Recovery Controller.

Soyez conscient des types de ressources et des restrictions

L'autoshift zonal prend en charge le transfert du trafic hors d'une zone de disponibilité pour toutes les ressources prises en charge par le transfert zonal. En général, les équilibreurs de charge

réseau et les équilibreurs de charge d'application dont l'équilibrage de charge entre zones est désactivé sont pris en charge. Dans certains scénarios de ressources spécifiques, le transfert automatique zonal ne déplace pas le trafic depuis une zone de disponibilité pour un transfert automatique.

Par exemple, si les groupes cibles de l'équilibreur de charge dans les zones de disponibilité ne possèdent aucune instance, ou si toutes les instances ne fonctionnent pas correctement, l'équilibreur de charge est dans un état d'ouverture défaillante. Dans ce scénario, si AWS un autoshift est lancé pour un équilibreur de charge, celui-ci ne modifie pas les zones de disponibilité utilisées par l'équilibreur de charge, car celui-ci est déjà dans un état ouvert en cas de défaillance. Ce comportement est normal. Le changement automatique ne peut pas rendre une zone de disponibilité défectueuse et déplacer le trafic vers les autres zones de disponibilité Région AWS si toutes les zones de disponibilité ne sont pas ouvertes (dysfonctionnements).

Un deuxième scénario est celui du AWS démarrage d'un autoshift pour un Application Load Balancer qui est le point de terminaison d'un accélérateur dans. AWS Global Accelerator Comme pour le changement de zone, le décalage automatique n'est pas pris en charge pour les équilibreurs de charge d'application qui sont les points de terminaison des accélérateurs dans Global Accelerator.

Pour en savoir plus sur les ressources prises en charge, y compris toutes les exigences et exceptions à connaître, consultezRessources prises en charge pour le changement de zone et le décalage automatique de zone.

Spécifiez les alarmes pour les essais

Vous configurez au moins une alarme, l'alarme de résultat, pour les séances d'entraînement avec le changement automatique zonal. En option, vous pouvez également configurer une deuxième alarme, l'alarme de blocage.

Lorsque vous considérez les CloudWatch alarmes que vous configurez pour les essais pratiques de votre ressource, gardez à l'esprit les points suivants :

- Pour l'alarme de résultat, qui est requise, nous vous recommandons de configurer une CloudWatch alarme pour qu'elle passe à un `ALARM` état dans lequel les mesures relatives à la ressource ou à votre application indiquent que le fait de déplacer le trafic hors de la zone de disponibilité a un impact négatif sur les performances. Par exemple, vous pouvez déterminer un seuil pour les taux de demandes pour votre ressource, puis configurer une alarme pour qu'elle passe à un `ALARM` état lorsque le seuil est dépassé. Vous êtes chargé de configurer une alarme appropriée qui met fin AWS à l'entraînement et renvoie un `FAILED` résultat.

- Nous vous recommandons de suivre le AWS Well Architected Framework, qui vous conseille de mettre en œuvre des indicateurs de performance clés (KPI) sous forme CloudWatch d'alarmes. Dans ce cas, vous pouvez utiliser ces alarmes pour créer une alarme composite à utiliser comme déclencheur de sécurité, afin d'empêcher les essais de démarrer au cas où votre application risquerait de manquer un KPI. Lorsque l'alarme n'est plus en `ALARM` état, Route 53 ARC lance des essais la prochaine fois qu'un entraînement est planifié pour la ressource.
- Pour l'alarme de blocage des essais, si vous choisissez de la configurer, vous pouvez choisir de suivre une métrique spécifique que vous utilisez pour indiquer que vous ne souhaitez pas qu'un entraînement commence.
- Pour vous entraîner à exécuter des alarmes, vous devez spécifier le nom de ressource Amazon (ARN) pour chaque alarme, que vous devez d'abord configurer dans Amazon CloudWatch. Les CloudWatch alarmes que vous spécifiez peuvent être des alarmes composites, afin de vous permettre d'inclure plusieurs mesures et contrôles pour votre application et votre ressource susceptibles de déclencher le passage de l'alarme à un `ALARM` état. Pour plus d'informations, consultez Combiner des alarmes dans le guide de CloudWatch l'utilisateur Amazon.
- Assurez-vous que les CloudWatch alarmes que vous spécifiez pour les essais se trouvent dans la même région que la ressource pour laquelle vous configurez un entraînement.

Évaluer les résultats des séances d'entraînement

Route 53 ARC rapporte un résultat pour chaque course d'entraînement. Après un entraînement, évaluez le résultat et déterminez si vous devez agir. Par exemple, vous devrez peut-être augmenter la capacité ou ajuster la configuration d'une alarme.

Les résultats possibles de l'entraînement sont les suivants :

- SUCCÈS : L'alarme de résultat n'est pas entrée dans un `ALARM` état pendant l'essai, et le cycle d'entraînement a terminé la période de test complète de 30 minutes.
- ÉCHEC : L'alarme de résultat est entrée dans un `ALARM` état pendant l'entraînement.
- INTERROMPU : La séance d'entraînement s'est terminée pour une raison qui n'était pas le fait que l'alarme entrait dans un `ALARM` état. Un entraînement peut être interrompu pour diverses raisons, notamment les suivantes :
  - La séance d'entraînement a pris fin parce qu'un changement automatique avait AWS commencé Région AWS ou parce qu'une alarme s'était produite dans la région.
  - L'exercice d'entraînement a été interrompu car la configuration du cycle d'entraînement a été supprimée pour la ressource.

- Le cycle d'entraînement a pris fin parce qu'un changement de zone initié par le client a été lancé pour la ressource de la zone de disponibilité à partir de laquelle le changement de zone d'entraînement détournait le trafic.
- L'exercice d'entraînement a été interrompu car une CloudWatch alarme spécifiée pour la configuration de l'essai n'est plus accessible.
- L'essai s'est terminé car l'alarme de blocage spécifiée pour l'essai est entrée dans un `ALARM` état.
- La course d'entraînement a été interrompue pour une raison inconnue.

- EN ATTENTE : La séance d'entraînement est active (en cours). Il n'y a pas encore de résultat à obtenir.

Opérations de l'API Zonal Autoshift

Le tableau suivant répertorie les opérations de l'API ARC Route 53 que vous pouvez utiliser avec l'autoshift zonal. Pour des exemples d'utilisation des opérations de l'API Zonal Autoshift avec le AWS CLI, voir.

Pour des exemples d'utilisation des opérations courantes de l'API Zonal Autoshift avec le AWS Command Line Interface, voir. Exemples d'utilisation de l' AWS CLI autoshift avec zone

Action	Utilisation de la console Route 53 ARC	Utilisation de l'API ARC Route 53
Création d'une configuration d'exécution d'entraînement	Consultez Activation ou désactivation de l'autoshift zonal.	Voir CreatePracticeRunConfiguration
Supprimer une configuration d'exécution d'entraînement	Consultez Configuration, modification ou suppression d'une configuration d'entraînement.	Voir DeletePracticeRunConfiguration
Répertorier les changements automatiques	Consultez Autoshift zonal dans le contrôleur de restauration d'applications Amazon Route 53.	Consultez ListAutoshifts

Action	Utilisation de la console Route 53 ARC	Utilisation de l'API ARC Route 53
Répertorier les ressources pour l'autoshift zonal	Consultez Ressources prises en charge pour le changement de zone et le décalage automatique de zone.	Voir les ListManagedressources
Obtenez des ressources pour le changement automatique par zone	Consultez Ressources prises en charge pour le changement de zone et le décalage automatique de zone.	Voir la GetManagedressource
Modifier la configuration d'une exécution d'entraînement	Consultez Configuration, modification ou suppression d'une configuration d'entraînement.	Voir UpdatePracticeRunConfiguration
Activer ou désactiver l'autoshift zonal	Consultez Activation ou désactivation de l'autoshift zonal.	Voir UpdateZonalAutoshiftConfiguration

Exemples d'utilisation de l' AWS CLI autoshift avec zone

Cette section présente des exemples d'applications simples illustrant l'utilisation de l'autoshift zonal, en utilisant la fonctionnalité AWS Command Line Interface de changement automatique zonal dans Amazon Route 53 Application Recovery Controller à l'aide d'opérations d'API. Les exemples sont destinés à vous aider à acquérir une compréhension de base de la manière d'utiliser l'autoshift zonal à l'aide de la CLI.

L'autoshift zonal est une fonctionnalité de Route 53 ARC. Avec l'autoshift zonal, vous autorisez AWS le transfert du trafic des ressources applicatives prises en charge depuis une zone de disponibilité lors d'événements, en votre nom, afin de réduire le délai de restauration. L'autoshift zonal inclut des essais pratiques, qui permettent également de déplacer le trafic hors des zones de disponibilité, afin de vérifier, sur une base continue, que les changements automatiques sont sûrs pour votre application.

L'autoshift zonal prend actuellement en charge les équilibreurs de charge réseau et les équilibreurs de charge d'application lorsque l'équilibrage de charge entre zones est désactivé.

Pour plus d'informations, consultez Ressources prises en charge pour le changement de zone et le décalage automatique de zone.

Cette section fournit les exemples suivants pour illustrer comment démarrer et utiliser l'autoshift zonal :

- Créez une configuration d'exécution d'entraînement pour une ressource.
- Activez et désactivez les changements automatiques pour une ressource.
- Mettez fin à un entraînement en cours en annulant le décalage de zone entamé par le cycle d'entraînement.
- Mettez fin à un changement automatique en cours en désactivant la fonction de décalage automatique zonal pour une ressource.
- Modifiez la configuration d'une exécution d'entraînement pour une ressource afin de modifier les alarmes spécifiées, les dates ou les fenêtres bloquées.
- Supprimez une configuration d'exécution d'entraînement pour une ressource.

Pour plus d'informations sur l'utilisation du AWS CLI, consultez la référence des AWS CLI commandes. Pour obtenir la liste des actions de l'API Autoshift zonal et des liens vers des informations supplémentaires, consultez. Opérations de l'API Zonal Autoshift

Création d'une configuration d'exécution par entraînement

Avant de pouvoir activer le décalage automatique zonal pour une ressource, vous devez créer une configuration d'entraînement pour la ressource, afin de choisir les options pour les essais requis. Vous créez une configuration d'exécution d'entraînement pour une ressource à l'aide de la CLI à l'aide de la `create-practice-run-configuration` commande.

Lorsque vous créez une configuration d'exécution d'entraînement pour une ressource, tenez compte des points suivants :

- Le seul type d'alarme pris en charge pour le moment est`CLOUDWATCH`.
- Vous devez utiliser des alarmes qui se trouvent dans le même emplacement Région AWS que celui dans lequel votre ressource est déployée.
- Il est nécessaire de spécifier une alarme de résultat. La spécification d'une alarme de blocage est facultative.

- La spécification de dates bloquées ou de fenêtres bloquées est facultative.

Vous créez une configuration d'exécution pratique avec la CLI à l'aide de la `create-practice-run-configuration` commande.

Par exemple, pour créer une configuration d'exécution d'entraînement pour une ressource, utilisez une commande comme celle-ci :

```
aws arc-zonal-shift create-practice-run-configuration \
      --resource-
identifier="arn:aws:elasticloadbalancing:Region:111122223333:ExampleALB123456890" \
      --outcome-alarms
 type=CLOUDWATCH,alarmIdentifier=arn:aws:cloudwatch:Region:111122223333:alarm:Region-
MyAppHealthAlarm \
      --blocking-alarms
 type=CLOUDWATCH,alarmIdentifier=arn:aws:cloudwatch:Region:111122223333:alarm:Region-
BlockWhenALARM \
      --blocked-dates 2023-12-01 --blocked-windows Mon:10:00-Mon:10:30
```

```
{
   "arn": "arn:aws:elasticloadbalancing:us-west-2:111122223333:ExampleALB123456890",
   "name": "zonal-shift-elb"
   "zonalAutoshiftStatus": "DISABLED",
   "practiceRunConfiguration": {
       "blockingAlarms": [
                  {
              "type": "CLOUDWATCH",
              "alarmIdentifier": "arn:aws:cloudwatch:us-west-2:111122223333:alarm:us-
west-2-BlockWhenALARM"
           }
       ]
       "outcomeAlarms": [
           {
               "type": "CLOUDWATCH",
               "alarmIdentifier": "arn:aws:cloudwatch:us-west-2:111122223333:alarm:us-
west-2-MyAppHealthAlarm"
           }
       ],
       "blockedWindows": [
           "Mon:10:00-Mon:10:30"
       ],
       "blockedDates": [
```

```
            "2023-12-01"
        ]
}
```

Activer ou désactiver les changements automatiques

Vous activez ou désactivez le décalage automatique pour une ressource en mettant à jour l'état du décalage automatique zonal à l'aide de la CLI. Pour modifier le statut de l'autoshift zonal, utilisez la `update-zonal-autoshift-configuration` commande.

Par exemple, pour activer les changements automatiques pour une ressource, utilisez une commande comme celle-ci :

```
aws arc-zonal-shift update-zonal-autoshift-configuration \
      --resource-
identifier="arn:aws:elasticloadbalancing:Region:111122223333:ExampleALB123456890" \
      --zonal-autoshift-status="ENABLED"
```

```
{
   "resourceIdentifier": "arn:aws:elasticloadbalancing:us-
west-2:111122223333:ExampleALB123456890",
   "zonalAutoshiftStatus": "ENABLED"
}
```

Annuler un changement automatique en cours

Pour annuler un changement automatique en cours pour une ressource, vous devez désactiver la fonction de changement automatique zonal. Il s'agit de la même commande que celle que vous utilisez pour désactiver le décalage automatique zonal en général. Ainsi, lorsque vous désactivez le décalage automatique zonal pour annuler un changement automatique en cours, la ressource n'est pas non plus affectée par les futurs changements automatiques. Vous pouvez mettre à jour l'autoshift zonal pour le réactiver à tout moment.

Notez que vous pouvez désactiver le décalage automatique zonal pour une ressource sans supprimer la configuration d'entraînement de la ressource.

Pour annuler un changement automatique à l'aide de la CLI, désactivez le décalage automatique zonal à l'aide de la commande. `update-zonal-autoshift-configuration` Par exemple, pour mettre fin à un transfert automatique pour une ressource, utilisez une commande comme celle-ci :

```
aws arc-zonal-shift update-zonal-autoshift-configuration \
      --resource-
identifier="arn:aws:elasticloadbalancing:Region:111122223333:ExampleALB123456890" \
      --zonal-autoshift-status="DISABLED"
```

```
{
   "resourceIdentifier": "arn:aws:elasticloadbalancing:us-
west-2:111122223333:ExampleALB123456890",
   "zonalAutoshiftStatus": "DISABLED"
}
```

Annuler une séance d'entraînement en cours

Vous pouvez annuler une séance d'entraînement en cours avec la CLI en annulant le décalage de zone que l'exécution d'entraînement a commencé pour la ressource. Pour annuler un entraînement, utilisez la `cancel-zonal-shift` commande.

Par exemple, pour annuler un entraînement pour une ressource, utilisez une commande comme celle-ci :

```
aws arc-zonal-shift cancel-zonal-shift \
   --zonal-shift-id="="arn:aws:testservice::111122223333:ExampleALB123456890"
```

```
{
    "zonalShiftId": "2222222-3333-444-1111",
    "resourceIdentifier": "arn:aws:testservice::111122223333:ExampleALB123456890",
    "awayFrom": "usw2-az1",
    "expiryTime": 2024-11-15T10:35:42+00:00,
    "startTime": 2024-11-15T09:35:42+00:00,
    "status": "CANCELED",
    "comment": "Practice Run Started"
}
```

Modifier la configuration d'une exécution d'entraînement

Vous pouvez modifier la configuration d'une exécution d'entraînement pour une ressource à l'aide de la CLI afin de mettre à jour différentes options de configuration, telles que la modification des alarmes pour les essais ou la mise à jour des dates bloquées ou des fenêtres bloquées, lorsque Route 53 ARC ne démarre pas les essais. Pour modifier la configuration d'une exécution d'entraînement, utilisez la `update-practice-run-configuration` commande.

Notez ce qui suit lorsque vous modifiez la configuration d'une exécution d'entraînement pour une ressource :

- Le seul type d'alarme pris en charge pour le moment est`CLOUDWATCH`.
- Vous devez utiliser des alarmes qui se trouvent dans le même emplacement Région AWS que celui dans lequel votre ressource est déployée.
- Il est nécessaire de spécifier une alarme de résultat. La spécification d'une alarme de blocage est facultative.
- La spécification de dates bloquées ou de fenêtres bloquées est facultative.
- Les dates bloquées ou les fenêtres bloquées que vous spécifiez remplacent toutes les valeurs existantes.

Par exemple, pour modifier la configuration d'une exécution d'entraînement pour une ressource afin de spécifier une nouvelle date de blocage, utilisez une commande comme celle-ci :

```
aws arc-zonal-shift update-practice-run-configuration \
      --resource-
identifier="arn:aws:elasticloadbalancing:Region:111122223333:ExampleALB123456890" \
      --blocked-dates 2024-03-01
```

```
{
   "arn": "arn:aws:elasticloadbalancing:us-west-2:111122223333:ExampleALB123456890",
   "name": "zonal-shift-elb"
   "zonalAutoshiftStatus": "DISABLED",
   "practiceRunConfiguration": {
       "blockingAlarms": [
                   {
               "type": "CLOUDWATCH",
               "alarmIdentifier": "arn:aws:cloudwatch:us-west-2:111122223333:alarm:us-
west-2-BlockWhenALARM"
           }
       ]
       "outcomeAlarms": [
           {
               "type": "CLOUDWATCH",
               "alarmIdentifier": "arn:aws:cloudwatch:us-west-2:111122223333:alarm:us-
west-2-MyAppHealthAlarm"
           }
       ],
```

```
        "blockedWindows": [
            "Mon:10:00-Mon:10:30"
        ],
        "blockedDates": [
            "2024-03-01"
        ]
}
```

Supprimer une configuration d'exécution d'entraînement

Vous pouvez supprimer une configuration d'entraînement pour une ressource, mais vous devez d'abord désactiver le décalage automatique zonal pour la ressource. Une ressource est requise pour qu'une configuration d'entraînement soit activée afin que le changement automatique zonal soit activé. Des exécutions régulières vous aident à vous assurer que votre application peut fonctionner normalement sans zone de disponibilité.

Pour supprimer une configuration d'exécution d'entraînement à l'aide de la CLI, désactivez d'abord l'autoshift zonal, si nécessaire à l'aide de la `update-zonal-autoshift` commande. Ensuite, pour supprimer la configuration de l'exécution d'entraînement, utilisez la `delete-practice-run-configuration` commande.

Tout d'abord, désactivez le décalage automatique zonal pour la ressource, à l'aide d'une commande comme celle-ci :

```
aws arc-zonal-shift update-zonal-autoshift-configuration \
      --resource-
identifier="arn:aws:elasticloadbalancing:Region:111122223333:ExampleALB123456890" \
      --zonal-autoshift-status="DISABLED"
```

```
{
   "resourceIdentifier": "arn:aws:elasticloadbalancing:us-
west-2:111122223333:ExampleALB123456890",
   "zonalAutoshiftStatus": "DISABLED"
}
```

Supprimez ensuite la configuration de l'exécution d'entraînement à l'aide d'une commande comme celle-ci :

```
aws arc-zonal-shift delete-practice-run-configuration \
```

```
      --resource-
identifier="arn:aws:elasticloadbalancing:Region:111122223333:ExampleALB123456890"
```

```
{
   "arn": "arn:aws:elasticloadbalancing:us-west-2:111122223333:ExampleALB123456890",
   "name": "TestResource",
   "zonalAutoshiftStatus": "DISABLED"
}
```

Activation et utilisation de l'autoshift zonal

Cette section décrit les procédures relatives à l'utilisation des décalages automatiques zonaux dans Amazon Route 53 Application Recovery Controller, notamment l'activation et la désactivation du décalage automatique zonal, la configuration des essais pratiques et l'annulation des essais en cours.

Activation ou désactivation de l'autoshift zonal

Les étapes décrites dans cette section expliquent comment activer ou désactiver l'autoshift zonal sur la console Amazon Route 53 Application Recovery Controller. Pour utiliser l'autoshift zonal par programmation, consultez le guide de référence de l'API Zonal Shift et Zonal Autoshift.

Lorsque le transfert automatique zonal est activé, vous autorisez AWS le transfert du trafic des ressources applicatives depuis une zone de disponibilité lors d'événements, en votre nom, afin de réduire le délai de restauration.

Pour activer ou désactiver le changement automatique zonal

1. Ouvrez la console Route 53 ARC à l'adressehttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Sous Multi-AZ, choisissez Zonal autoshift.
3. Sous Configurations de transfert automatique par zone de ressources, sélectionnez une ressource.
4. Dans le menu Actions, choisissez Activer le décalage automatique zonal ou Désactiver le décalage automatique zonal, puis suivez les étapes pour terminer la mise à jour.

Si la ressource ne possède pas de configuration d'exécution d'entraînement, l'option Enable zonal Autoshift n'est pas disponible. Pour configurer une configuration d'entraînement et activer l'autoshift zonal, choisissez Configure Zonal Autoshift.

Configuration, modification ou suppression d'une configuration d'entraînement

Les étapes décrites dans cette section expliquent comment modifier ou supprimer une configuration d'entraînement sur la console Amazon Route 53 Application Recovery Controller. Pour utiliser l'autoshift zonal de manière programmatique, y compris pour modifier les configurations d'exécution, consultez le guide de référence de l'API Zonal Shift et Zonal Autoshift.

Si vous supprimez une configuration d'entraînement dans la console, le changement automatique zonal est désactivé. Avant de pouvoir supprimer une configuration d'entraînement à l'aide d'une opération d'API, vous devez désactiver l'autoshift zonal. Vous pouvez configurer un exercice d'entraînement sans activer le changement automatique par zone. Toutefois, pour que le changement automatique zonal soit activé pour une ressource, vous devez configurer un exercice d'entraînement pour cette ressource.

Pour configurer un exercice d'entraînement

1. Ouvrez la console Route 53 ARC à l'adressehttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Sous Multi-AZ, choisissez Zonal autoshift.
3. Choisissez Configurer l'autoshift zonal.
4. Choisissez une ressource à configurer pour l'autoshift zonal.
5. Choisissez de désactiver le changement automatique zonal si vous ne AWS souhaitez pas démarrer un changement automatique pour une ressource en cas d'événement. AWS Vous pouvez continuer à utiliser l'assistant pour configurer une configuration d'entraînement sans activer les changements automatiques, si vous le souhaitez.
6. Choisissez des options pour les séances d'entraînement pour la ressource. Pour les alarmes, vous pouvez effectuer les opérations suivantes :

   - (Obligatoire) Spécifiez une alarme de résultat pour surveiller les essais pour cette ressource.
   - (Facultatif) Spécifiez une alarme de blocage pour les essais de cette ressource.

   Pour plus d'informations, consultez la section Alarmes que vous spécifiez pour les séances d'entraînement dansBonnes pratiques lors de la configuration de l'autoshift zonal.

7. Spécifiez éventuellement des dates bloquées et des fenêtres bloquées. Choisissez des dates ou des fenêtres (jours et heures) pour empêcher la Route 53 ARC de commencer les essais pour cette ressource. Toutes les dates et heures sont exprimées en UTC.
8. Cochez la case pour confirmer que vous avez lu l'accusé de réception.
9. Choisissez Créer.

Pour modifier la configuration d'une exécution d'entraînement

1. Ouvrez la console Route 53 ARC à l'adressehttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Sous Multi-AZ, choisissez Zonal autoshift.
3. Sous Configurations de transfert automatique par zone de ressources, sélectionnez une ressource.
4. Dans le menu Actions, choisissez Modifier la configuration des essais pratiques.
5. Apportez des modifications à la configuration de l'exécution d'entraînement pour effectuer une ou plusieurs des opérations suivantes :
   - Pour les alarmes, vous pouvez effectuer les opérations suivantes :
     - Pour l'alarme de blocage, vous pouvez ajouter une alarme, supprimer l'alarme ou définir une autre alarme de blocage.
     - Pour l'alarme de résultat qui surveille les séances d'entraînement, vous pouvez spécifier une autre CloudWatch alarme à utiliser. Les alarmes de résultat sont obligatoires, vous ne pouvez donc pas supprimer l'alarme de résultat.
   - Pour les dates bloquées et les fenêtres bloquées, vous pouvez ajouter de nouvelles dates ou de nouveaux jours et heures, ou vous pouvez supprimer ou mettre à jour des dates, des jours et des heures existants. Toutes les dates et heures sont exprimées en UTC.
6. Choisissez Enregistrer.

Pour supprimer une configuration d'entraînement

1. Ouvrez la console Route 53 ARC à l'adressehttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Sous Multi-AZ, choisissez Zonal autoshift.

3. Sous Configurations de transfert automatique par zone de ressources, sélectionnez une ressource.
4. Dans le menu Actions, choisissez Supprimer la configuration d'exécution d'exercices pratiques.
5. Dans la boîte de dialogue modale de confirmation`Delete`, tapez, puis choisissez Supprimer.

   Notez que la suppression d'une configuration d'entraînement dans la console désactive également le décalage automatique zonal pour la ressource. L'autoshift zonal nécessite la configuration d'un essai pour la ressource.

Annulation d'un entraînement : changement de zone

Les étapes décrites dans cette section expliquent comment annuler un changement de zone sur la console Amazon Route 53 Application Recovery Controller. Pour utiliser le décalage de zone et le décalage automatique de zone par programmation, consultez le guide de référence de l'API Zonal Shift et Zonal Autoshift.

Vous pouvez annuler les changements de zone que vous avez vous-même initiés. Vous pouvez également annuler les changements de zone qui AWS commencent pour une ressource dans le cadre d'une séance d'entraînement pour le changement automatique de zone.

Pour annuler un entraînement, exécutez un changement de zone

1. Ouvrez la console Route 53 ARC à l'adressehttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Sous Multi-AZ, choisissez Zonal Shift.
3. Sélectionnez le décalage de zone que vous souhaitez annuler, puis choisissez Annuler le décalage de zone.
4. Dans la boîte de dialogue modale de confirmation, choisissez Confirmer.

Journalisation et surveillance du changement automatique par zone dans Amazon Route 53 Application Recovery Controller

Vous pouvez utiliser AWS CloudTrail Amazon EventBridge pour surveiller l'autoshift zonal dans Amazon Route 53 Application Recovery Controller, afin d'analyser les modèles et de résoudre les problèmes.

Rubriques

- Enregistrement des appels d'API Zonal AutoShift à l'aide de AWS CloudTrail
- Utilisation de l'autoshift zonal avec Amazon EventBridge

Enregistrement des appels d'API Zonal AutoShift à l'aide de AWS CloudTrail

L'autoshift zonal pour Amazon Route 53 Application Recovery Controller 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 ARC. CloudTrail capture tous les appels d'API pour le changement de zone sous forme d'événements. Les appels capturés incluent des appels provenant de la console Route 53 ARC et des appels de code vers les opérations de l'API Route 53 ARC pour le changement de zone.

Si vous créez un suivi, vous pouvez activer la diffusion continue des CloudTrail événements vers un compartiment Amazon S3, y compris les événements liés au changement de zone. 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 de changement de zone qui a été faite à Route 53 ARC, 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.

Pour en savoir plus CloudTrail, consultez le guide de AWS CloudTrail l'utilisateur.

Informations de changement automatique zonal dans CloudTrail

CloudTrail est activé sur votre compte Compte AWS lorsque vous créez le compte. Lorsqu'une activité se produit sur Route 53 ARC pour le changement automatique zonal, 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 Compte AWS. Pour plus d'informations, consultez la section Utilisation de l'historique des CloudTrail événements.

Pour un enregistrement continu des événements survenus dans votre région Compte AWS, y compris les événements liés au changement automatique de zone sur Route 53 ARC, 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 Régions AWS. 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 afin d'analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et d'agir en conséquence. Pour plus d'informations, consultez les ressources suivantes :

- Présentation de la création d'un journal de suivi
- 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 ARC de Route 53 sont enregistrées CloudTrail et documentées dans le Guide de référence de l'API de contrôle de routage pour Amazon Route 53 Application Recovery Controller. Par exemple, les appels aux `ListManagedResources` actions `StartZonalShift` et 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 faite avec les informations d'identification de l'utilisateur root ou AWS Identity and Access Management (IAM).
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la demande a été faite par un autre AWS service.

Pour plus d'informations, consultez l'élément CloudTrail UserIdentity.

Afficher les événements de la Route 53 ARC dans l'historique des événements

CloudTrail vous permet de consulter les événements récents dans l'historique des événements. Pour plus d'informations, consultez la section Utilisation de l'historique des CloudTrail événements dans le guide de AWS CloudTrail l'utilisateur.

Comprendre les entrées du fichier journal Zonal AutoShift

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'exemple suivant montre une entrée de CloudTrail journal qui illustre l'`ListManagedResources`action du changement automatique zonal.


```
{
      "eventVersion": "1.08",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:role/admin",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "sessionIssuer": {
            "type": "Role",
            "principalId": "AROA33L3W36EXAMPLE",
            "arn": "arn:aws:iam::111122223333:role/admin",
            "accountId": "111122223333",
            "userName": "EXAMPLENAME"
          },
          "webIdFederationData": {},
          "attributes": {
            "creationDate": "2022-11-14T16:01:51Z",
            "mfaAuthenticated": "false"
          }
        }
      },
      "eventTime": "2022-11-14T16:14:41Z",
      "eventSource": "arc-zonal-shift.amazonaws.com",
      "eventName": "ListManagedResources",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.50",
      "userAgent": "Boto3/1.17.101 Python/3.8.10 Linux/4.14.231-180.360.amzn2.x86_64
 exec-env/AWS_Lambda_python3.8 Botocore/1.20.102",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "VGXG4ZUE7UZTVCMTJGIAF_EXAMPLE",
      "eventID": "4b5c42df-1174-46c8-be99-d67_EXAMPLE",
      "readOnly": true,
```

```
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333"
    "eventCategory": "Management"
    }
  }
```

Utilisation de l'autoshift zonal avec Amazon EventBridge

À l'aide d'Amazon EventBridge, vous pouvez configurer des règles basées sur les événements qui surveillent vos ressources de transfert automatique zonales et initient des actions ciblées utilisant d'autres services. AWS Par exemple, vous pouvez définir une règle pour l'envoi de notifications par e-mail en signalant un sujet Amazon SNS lorsqu'une séance d'entraînement commence pour le changement automatique zonal.

Vous pouvez créer des règles dans Amazon EventBridge pour agir sur l'autoshift zonal. Un événement pour un événement de changement automatique zonal fournit des informations d'état sur les changements automatiques des cycles d'entraînement, par exemple lorsqu'un entraînement est en cours.

Pour capturer les événements de décalage automatique zonaux spécifiques qui vous intéressent, définissez des modèles spécifiques aux événements qui EventBridge peuvent être utilisés pour détecter les événements. Les modèles d'événements ont la même structure que les événements auxquels ils correspondent. Le modèle place entre guillemets les champs que vous voulez faire correspondre et fournit les valeurs que vous recherchez.

Les événements sont générés dans la mesure du possible. Ils sont livrés depuis la Route 53 ARC EventBridge en temps quasi réel, dans des circonstances opérationnelles normales. Cependant, des situations peuvent survenir susceptibles de retarder ou d'empêcher la livraison d'un événement.

Pour plus d'informations sur le fonctionnement EventBridge des règles avec les modèles d'événements, consultez la section Événements et modèles d'événements dans EventBridge.

Surveillez une ressource de transfert automatique zonale avec EventBridge

Avec EventBridge, vous pouvez créer des règles qui définissent les actions à entreprendre lorsque Route 53 ARC émet des événements pour ses ressources. Par exemple, vous pouvez créer une règle qui envoie un message électronique au début d'une séance d'entraînement pour le changement automatique zonal.

Pour taper ou copier-coller un modèle d'événement dans la EventBridge console, sélectionnez l'option Enter my own option dans la console. Pour vous aider à déterminer les modèles d'événements susceptibles de vous être utiles, cette rubrique inclut des exemples de modèles de correspondance d'événements de décalage automatique zonaux et d'événements de décalage automatique zonaux que vous pouvez utiliser.

Pour créer une règle pour un événement de ressource

1. Ouvrez la EventBridge console Amazon à l'adresse https://console.aws.amazon.com/events/.
2. Choisissez la région dans Région AWS laquelle vous souhaitez créer la règle, c'est-à-dire la région pour laquelle vous souhaitez suivre des événements.
3. Choisissez Create rule.
4. Entrez un nom et éventuellement une description pour la règle.
5. Pour Event bus, laissez la valeur par défaut, default.
6. Choisissez Suivant.
7. Pour l'étape Créer un modèle d'événement, pour Source d'événement, laissez la valeur par défaut, AWS events.
8. Sous Exemple d'événement, choisissez Enter my own.
9. Pour Exemples d'événements, tapez ou copiez-collez un modèle d'événement.

Exemples de modèles d'événements de décalage automatique zonaux

Les modèles d'événements ont la même structure que les événements auxquels ils correspondent. Le modèle place entre guillemets les champs que vous voulez faire correspondre et fournit les valeurs que vous recherchez.

Vous pouvez copier et coller des modèles d'événements depuis cette section EventBridge pour créer des règles que vous pouvez utiliser pour surveiller les actions et les ressources liées au transfert automatique par zone.

Lorsque vous créez des modèles d'événements pour des événements de décalage automatique zonaux, vous pouvez spécifier l'une des options suivantes pour : `detail-type`

- `Autoshift In Progress`
- `Autoshift Completed`
- `Practice Run Started`

- `Practice Run Succeeded`
- `Practice Run Interrupted`
- `Practice Run Failed`

Lorsqu'un entraînement est interrompu, pour plus d'informations sur la cause de l'interruption, consultez le `additionalFailureInfo` champ.

- Sélectionnez tous les événements dans l'autoshift zonal où une course d'entraînement a commencé. .

```
{
    "source": [
        "aws.arc-zonal-shift"
    ],
    "detail-type": [
        "Practice Run Started"
    ]
}
```

- Sélectionnez tous les événements du changement automatique de zone en cas d'échec d'un entraînement. .

```
{
    "source": [
        "aws.arc-zonal-shift"
    ],
    "detail-type": [
        "Practice Run Failed"
    ]
}
```

Exemples d'événements de décalage automatique zonaux

Voici un exemple d'événement pour une action de changement automatique zonal :

```
{
    "version": "0",
    "id": "05d4d2d5-9c76-bfea-72d2-d4614802adb4",
    "detail-type": "Practice Run Interrupted",
    "source": "aws.arc-zonal-shift",
```

```
    "account": "111122223333",
    "time": "2023-11-16T23:38:14Z",
    "region": "us-east-1",
    "resources": [
        "TEST-EXAMPLE-2023-11-16-23-28-11-5"
    ],
    "detail": {
        "version": "0.0.1",
        "data": {
            "additionalFailureInfo": "Practice run interrupted. The blocking alarm
 entered ALARM state."
        },
        "metadata": {
            "awayFrom": "use1-az2"
        }
    }
}
```


Spécifiez un groupe de CloudWatch journaux à utiliser comme cible

Lorsque vous créez une EventBridge règle, vous devez spécifier la cible vers laquelle les événements correspondant à la règle sont envoyés. Pour obtenir la liste des cibles disponibles pour EventBridge, consultez la section Cibles disponibles dans la EventBridge console. L'une des cibles que vous pouvez ajouter à une EventBridge règle est un groupe de CloudWatch journaux Amazon. Cette section décrit les exigences relatives à l'ajout de groupes de CloudWatch journaux en tant que cibles et fournit une procédure pour ajouter un groupe de journaux lorsque vous créez une règle.

Pour ajouter un groupe de CloudWatch journaux en tant que cible, vous pouvez effectuer l'une des opérations suivantes :

- Création d'un nouveau groupe de journaux
- Choisissez un groupe de journaux existant

Si vous spécifiez un nouveau groupe de journaux à l'aide de la console lorsque vous créez une règle, le groupe de journaux est EventBridge automatiquement créé pour vous. Assurez-vous que le groupe de journaux que vous utilisez comme cible pour la EventBridge règle commence par`/aws/events`. Si vous souhaitez choisir un groupe de journaux existant, sachez que seuls les groupes de journaux commençant par `/aws/events` apparaissent sous forme d'options dans le menu déroulant. Pour plus d'informations, consultez la section Créer un nouveau groupe de journaux dans le guide de CloudWatch l'utilisateur Amazon.

Si vous créez ou utilisez un groupe de CloudWatch journaux à utiliser comme cible à l'aide d' CloudWatch opérations en dehors de la console, assurez-vous de définir correctement les autorisations. Si vous utilisez la console pour ajouter un groupe de journaux à une EventBridge règle, la politique basée sur les ressources pour le groupe de journaux est automatiquement mise à jour. Toutefois, si vous utilisez le AWS Command Line Interface ou un AWS SDK pour spécifier un groupe de journaux, vous devez mettre à jour la politique basée sur les ressources pour le groupe de journaux. L'exemple de politique suivant illustre les autorisations que vous devez définir dans une stratégie basée sur les ressources pour le groupe de journaux :

```
{
  "Statement": [
    {
      "Action": [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "events.amazonaws.com",
          "delivery.logs.amazonaws.com"
        ]
      },
      "Resource": "arn:aws:logs:region:account:log-group:/aws/events/*:*",
      "Sid": "TrustEventsToStoreLogEvent"
    }
  ],
  "Version": "2012-10-17"
}
```

Vous ne pouvez pas configurer une politique basée sur les ressources pour un groupe de journaux à l'aide de la console. Pour ajouter les autorisations requises à une politique basée sur les ressources, utilisez l'opération CloudWatch PutResourcePolicyAPI. Vous pouvez ensuite utiliser la commande describe-resource-policiesCLI pour vérifier que votre politique a été correctement appliquée.

Pour créer une règle pour un événement de ressource et spécifier une cible de groupe de CloudWatch journaux

1. Ouvrez la EventBridge console Amazon à l'adresse https://console.aws.amazon.com/events/.
2. Choisissez Région AWS celui dans lequel vous souhaitez créer la règle.

3. Choisissez Créer une règle, puis entrez les informations relatives à cette règle, telles que le modèle d'événement ou les détails du calendrier.

   Pour plus d'informations sur la création de EventBridge règles pour Route 53 ARC, consultez les sections précédentes dans cette rubrique.
4. Sur la page Sélectionner une cible, choisissez CloudWatchcomme cible.
5. Choisissez un groupe de CloudWatch journaux dans le menu déroulant.

Identity and Access Management pour l'autoshift zonal

AWS Identity and Access Management (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les ressources ARC de la Route 53. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Table des matières

Comment fonctionne l'autoshift zonal dans Amazon Route 53 Application Recovery Controller avec IAM

Avant d'utiliser IAM pour gérer l'accès à l'autoshift zonal dans Amazon Route 53 Application Recovery Controller, découvrez quelles fonctionnalités IAM peuvent être utilisées avec le changement automatique zonal.

Fonctionnalités IAM que vous pouvez utiliser avec le changement automatique par zone dans Amazon Route 53 Application Recovery Controller

Fonction IAM	Support de changement automatique par zone
Politiques basées sur l’identité	Oui

Fonction IAM	Support de changement automatique par zone
Politiques basées sur les ressources	Non
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition d'une politique	Oui
ACL	Non
ABAC (identifications dans les politiques)	Partielle
Informations d'identification temporaires	Oui
Autorisations de principal	Oui
Fonctions du service	Non
Rôles liés à un service	Oui

Pour obtenir une vue globale de haut niveau du fonctionnement des AWS services avec la plupart des fonctionnalités IAM, consultez la section AWS Services compatibles avec IAM dans le Guide de l'utilisateur IAM.

Politiques basées sur l'identité pour Route 53 ARC

Prend en charge les politiques basées sur l'identité	Oui

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Création de politiques IAM dans le Guide de l'utilisateur IAM.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou

refusées. Vous ne pouvez pas spécifier le principal dans une politique basée sur une identité car celle-ci s'applique à l'utilisateur ou au rôle auquel elle est attachée. Pour découvrir tous les éléments que vous utilisez dans une politique JSON, consultez Références des éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

Pour consulter des exemples de politiques basées sur l'identité de Route 53 ARC, consultez. Exemples de politiques basées sur l'identité dans Amazon Route 53 Application Recovery Controller

Politiques basées sur les ressources au sein de Route 53 ARC

Prend en charge les politiques basées sur les ressources	Non

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique.

Actions politiques pour la Route 53 ARC

Prend en charge les actions de politique	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Les actions de stratégie portent généralement le même nom que l'opération AWS d'API associée. Il existe quelques exceptions, telles que les actions avec autorisations uniquement qui n'ont pas d'opération API correspondante. Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une stratégie afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour consulter la liste des actions ARC de Route 53 pour le changement automatique de zone, consultez la section Actions définies par Amazon Route 53 Zonal Shift dans la référence d'autorisation de service.

Les actions politiques de Route 53 ARC pour le décalage automatique zonal utilisent les préfixes suivants avant l'action :

```
arc-zonal-shift
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules. Par exemple, ce qui suit :

```
"Action": [
      "arc-zonal-shift:action1",
      "arc-zonal-shift:action2"
         ]
```

Vous pouvez aussi spécifier plusieurs actions à l'aide de caractères génériques (*). Par exemple, pour spécifier toutes les actions qui commencent par le mot `Describe`, incluez l'action suivante :

```
"Action": "arc-zonal-shift:Describe*"
```

Pour consulter des exemples de politiques basées sur l'identité de la Route 53 ARC pour le changement automatique zonal, consultez. Exemples de politiques basées sur l'identité pour le changement automatique zonal

Ressources relatives aux politiques relatives au changement automatique par zone sur la Route 53 ARC

Prend en charge les ressources de politique	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Vous pouvez le faire pour des actions

qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

```
"Resource": "*"
```

Pour consulter la liste des types de ressources et de leurs ARN, ainsi que les actions que vous pouvez spécifier avec l'ARN de chaque ressource, consultez la rubrique suivante dans la référence d'autorisation de service :

- Actions définies par Amazon Route 53 - Zonal Shift

Pour connaître les actions et les ressources que vous pouvez utiliser avec une clé de condition, consultez la rubrique suivante dans la référence d'autorisation de service :

- Clés de condition définies par Amazon Route 53 - Zonal Shift

Pour consulter des exemples de politiques basées sur l'identité de la Route 53 ARC pour le changement automatique zonal, consultez. Exemples de politiques basées sur l'identité pour le changement automatique zonal

Clés de condition de politique pour le changement automatique par zone sur la Route 53 ARC

Prend en charge les clés de condition de politique spécifiques au service	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` (ou le bloc `Condition`) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément `Condition` est facultatif. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande.

Si vous spécifiez plusieurs éléments `Condition` dans une instruction, ou plusieurs clés dans un seul élément `Condition`, AWS les évalue à l'aide d'une opération `AND` logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une `OR` opération logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez accorder à un utilisateur IAM l'autorisation d'accéder à une ressource uniquement si elle est balisée avec son nom d'utilisateur IAM. Pour plus d'informations, consultez Éléments d'une politique IAM : variables et identifications dans le Guide de l'utilisateur IAM.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques au service. Pour voir toutes les clés de condition AWS globales, voir les clés de contexte de condition AWS globales dans le guide de l'utilisateur IAM.

Pour consulter la liste des clés de condition ARC de la Route 53 pour le changement automatique zonal, consultez les rubriques suivantes dans la référence d'autorisation de service :

- Clés de condition pour Amazon Route 53 Zonal Shift

Pour connaître les actions et les ressources que vous pouvez utiliser avec une clé de condition, consultez les rubriques suivantes dans la référence d'autorisation de service :

- Actions définies par Amazon Route 53 Zonal Shift

Pour consulter des exemples de politiques basées sur l'identité de la Route 53 ARC pour le changement automatique zonal, consultez. Exemples de politiques basées sur l'identité pour le changement automatique zonal

Listes de contrôle d'accès (ACL) dans Route 53 ARC

Prend en charge les listes ACL	Non

Les listes de contrôle d'accès (ACL) vérifient quels principaux (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Contrôle d'accès basé sur les attributs (ABAC) avec Route 53 ARC

Prise en charge d’ABAC (identifications dans les politiques)	Partielle

Le contrôle d’accès basé sur les attributs (ABAC) est une politique d’autorisation qui définit des autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et à de nombreuses AWS ressources. L’étiquetage des entités et des ressources est la première étape d’ABAC. Vous concevez ensuite des politiques ABAC pour autoriser des opérations quand l’identification du principal correspond à celle de la ressource à laquelle il tente d’accéder.

L’ABAC est utile dans les environnements qui connaissent une croissance rapide et pour les cas où la gestion des politiques devient fastidieuse.

Pour contrôler l’accès basé sur des étiquettes, vous devez fournir les informations d’étiquette dans l’élément de condition d’une politique utilisant les clés de condition `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d’informations sur l’ABAC, consultez Qu’est-ce que le contrôle d’accès basé sur les attributs (ABAC) ? dans le Guide de l’utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration de l’ABAC, consultez Utilisation du contrôle d’accès par attributs (ABAC) dans le Guide de l’utilisateur IAM.

L'autoshift zonal de Route 53 ARC inclut la prise en charge partielle suivante de l'ABAC :

- L'autoshift zonal prend en charge l'ABAC pour les ressources gérées enregistrées dans Route 53 ARC pour le décalage zonal. Pour plus d'informations sur les ressources gérées par ABAC for Network Load Balancer et Application Load Balancer, consultez la section ABAC with Elastic Load Balancing dans le guide de l'utilisateur d'Elastic Load Balancing.

Utilisation d'informations d'identification temporaires avec Route 53 ARC

Prend en charge les informations d’identification temporaires	Oui

Certains Services AWS ne fonctionnent pas lorsque vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, y compris celles qui Services AWS fonctionnent avec des informations d'identification temporaires, consultez Services AWS la section relative à l'utilisation d'IAM dans le guide de l'utilisateur d'IAM.

Vous utilisez des informations d'identification temporaires si vous vous connectez à l' AWS Management Console aide d'une méthode autre qu'un nom d'utilisateur et un mot de passe. Par exemple, lorsque vous accédez à AWS l'aide du lien d'authentification unique (SSO) de votre entreprise, ce processus crée automatiquement des informations d'identification temporaires. Vous créez également automatiquement des informations d’identification temporaires lorsque vous vous connectez à la console en tant qu’utilisateur, puis changez de rôle. Pour plus d’informations sur le changement de rôle, consultez Changement de rôle (console) dans le Guide de l’utilisateur IAM.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide de l' AWS API AWS CLI or. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour y accéder AWS. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d’informations, consultez Informations d’identification de sécurité temporaires dans IAM.

Autorisations principales interservices pour Route 53 ARC

Prend en charge les sessions d'accès direct (FAS)	Oui

Lorsque vous utilisez une entité IAM (utilisateur ou rôle) pour effectuer des actions AWS, vous êtes considéré comme un mandant. Les politiques accordent des autorisations au principal. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui déclenche une autre action dans un autre service. Dans ce cas, vous devez disposer d’autorisations nécessaires pour effectuer les deux actions.

Pour savoir si une action nécessite des actions dépendantes supplémentaires dans une politique, consultez la rubrique suivante dans la référence d'autorisation de service :

- Changement de zone sur Amazon Route 53

Rôles de service pour Route 53 ARC

Prend en charge les fonctions de service	Non

Une fonction du service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du 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.

Rôles liés à un service pour Route 53 ARC

Prend en charge les rôles liés à un service.	Oui

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.

Pour plus de détails sur la création ou la gestion des rôles liés au service Route 53 ARC, consultez. Utilisation du rôle lié au service pour le changement automatique de zone dans Route 53 ARC

Pour plus d'informations sur la création ou la gestion des rôles liés à un service, consultez Services AWS qui fonctionnent avec IAM. Recherchez un service dans le tableau qui inclut un `Yes` dans la colonne Rôle lié à un service. Choisissez le lien Oui pour consulter la documentation du rôle lié à ce service.

Exemples de politiques basées sur l'identité pour le changement automatique zonal

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier les ressources ARC de la Route 53. Ils ne peuvent pas non plus effectuer de tâches à l'aide de l'API AWS Management Console, AWS Command Line Interface (AWS CLI) ou de AWS l'API. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Pour apprendre à créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, consultez Création de politiques dans l'onglet JSON dans le Guide de l'utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par Route 53 ARC, y compris le format des ARN pour chacun des types de ressources, consultez la section Actions, ressources et clés de condition pour Amazon Route 53 Application Recovery Controller dans le Service Authorization Reference.

Rubriques

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer des ressources Route 53 ARC dans votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez politiques gérées par AWS ou politiques gérées par AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.
- Accorder les autorisations de moindre privilège : lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l'exécution d'une seule tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation de IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utiliser des conditions dans les politiques IAM pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes

doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que AWS CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

- Utilisez IAM Access Analyzer pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : IAM Access Analyzer valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez Validation de politique IAM Access Analyzer dans le Guide de l'utilisateur IAM.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue. Compte AWS Pour exiger le MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Configuration de l'accès aux API protégé par MFA dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

Exemple : accès à la console Zonal Autoshift

Pour accéder à la console Amazon Route 53 Application Recovery Controller, vous devez disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et d'afficher les détails des ressources ARC de la Route 53 présentes dans votre Compte AWS. Si vous créez une stratégie basée sur l'identité qui est plus restrictive que l'ensemble minimum d'autorisations requis, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs ou rôles) tributaires de cette stratégie.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement l'API AWS CLI ou l' AWS API. Autorisez plutôt l'accès à uniquement aux actions qui correspondent à l'opération d'API qu'ils tentent d'effectuer.

Pour effectuer certaines tâches, les utilisateurs doivent être autorisés à créer le rôle lié au service associé au changement automatique de zone dans Route 53 ARC. Pour en savoir plus, veuillez consulter la section Utilisation du rôle lié au service pour le changement automatique de zone dans Route 53 ARC.

Pour donner aux utilisateurs un accès complet à l'utilisation de l'autoshift zonal dans le AWS Management Console, associez une politique telle que la suivante à l'utilisateur :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                   "arc-zonal-shift:ListManagedResources",
                   "arc-zonal-shift:GetManagedResource",
                   "arc-zonal-shift:ListZonalShifts",
                   "arc-zonal-shift:StartZonalShift",
                   "arc-zonal-shift:UpdateZonalShift",
                   "arc-zonal-shift:CancelZonalShift",
                   "arc-zonal-shift:CreatePracticeRunConfiguration",
                   "arc-zonal-shift:DeletePracticeRunConfiguration",
                   "arc-zonal-shift:ListAutoshifts",
                   "arc-zonal-shift:UpdatePracticeRunConfiguration",
                   "arc-zonal-shift:UpdateZonalAutoshiftConfiguration"
             ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeAvailabilityZones",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "cloudwatch:DescribeAlarms",
            "Resource": "*"
        }
    ]
}
```

Exemples : actions de l'API ARC Route 53

Vous pouvez utiliser une politique garantissant qu'un utilisateur peut utiliser les actions de l'API ARC Route 53 pour le changement automatique zonal afin de configurer le transfert automatique zonal afin de transférer le trafic des ressources applicatives d'une zone de disponibilité, en votre nom, vers des zones de disponibilité saines dans la zone, afin de réduire le Région AWS temps de restauration en

cas d'événements. AWS Pour fournir ces autorisations, associez une politique correspondant aux opérations d'API avec lesquelles l'utilisateur doit travailler, comme décrit ci-dessous.

Pour effectuer certaines tâches, les utilisateurs doivent disposer d'autorisations pour le rôle lié au service associé à Route 53 ARC. Les autorisations nécessaires pour créer le rôle lié à un service sont incluses dans l'exemple de politique suivant. Pour en savoir plus, veuillez consulter la section Utilisation du rôle lié au service pour le changement automatique de zone dans Route 53 ARC.

Pour utiliser les opérations d'API pour le changement automatique zonal, associez une politique telle que la suivante à l'utilisateur :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                   "arc-zonal-shift:ListManagedResources",
                   "arc-zonal-shift:GetManagedResource",
                   "arc-zonal-shift:ListZonalShifts",
                   "arc-zonal-shift:StartZonalShift",
                   "arc-zonal-shift:UpdateZonalShift",
                   "arc-zonal-shift:CancelZonalShift",
                   "arc-zonal-shift:CreatePracticeRunConfiguration",
                   "arc-zonal-shift:DeletePracticeRunConfiguration",
                   "arc-zonal-shift:ListAutoshifts",
                   "arc-zonal-shift:UpdatePracticeRunConfiguration",
                   "arc-zonal-shift:UpdateZonalAutoshiftConfiguration"
             ],
            "Resource": "*"
        },
        {
            "Effect" : "Allow",
            "Action" : [
                   "cloudwatch:DescribeAlarms",
                   "health:DescribeEvents"
            ],
            "Resource" : "*"
        },
        {
            "Effect" : "Allow",
            "Action" : [
                   "arc-zonal-shift:CancelZonalShift",
```

```
                    "arc-zonal-shift:GetManagedResource",
                    "arc-zonal-shift:StartZonalShift",
                    "arc-zonal-shift:UpdateZonalShift"
            ],
            "Resource" : "*"
        }
    ]
}
```

Utilisation du rôle lié au service pour le changement automatique de zone dans Route 53 ARC

L'autoshift zonal dans Amazon Route 53 Application Recovery Controller utilise un rôle lié à un AWS Identity and Access Management service (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié à un service, dans ce cas, Route 53 ARC. Le rôle lié au service est prédéfini par Route 53 ARC et inclut toutes les autorisations dont le service a besoin pour appeler d'autres AWS services en votre nom à des fins spécifiques.

Un rôle lié à un service facilite la configuration de Route 53 ARC, car vous n'avez pas à ajouter manuellement les autorisations nécessaires. Route 53 ARC définit les autorisations pour le rôle lié au service, et sauf indication contraire, seule la Route 53 ARC peut assumer 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 de ses ressources connexes. Cela protège vos ressources de transfert automatique zonales de la Route 53 ARC, car vous ne pouvez pas supprimer par inadvertance l'autorisation d'accès aux ressources.

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés à un service, consultez la section AWS Services qui fonctionnent avec IAM et recherchez les services dont la valeur est Oui dans la colonne Rôle lié au service. Choisissez un Yes (oui) ayant un lien permettant de consulter les détails du rôle pour ce service.

Autorisations de rôle liées à un service pour AWSServiceRoleForZonalAutoshiftPracticeRun

Route 53 ARC utilise le rôle lié au service nommé AWSServiceRoleForZonalAutoshiftPracticeRunpour effectuer les opérations suivantes :

- Surveillez les CloudWatch alarmes et les AWS Health Dashboard événements Amazon fournis par les clients pour les séances d'entraînement

- Gérer les courses d'entraînement (changements de zone d'entraînement)

Cette section décrit les autorisations pour le rôle lié au service, ainsi que des informations sur la création, la modification et la suppression du rôle.

Autorisations de rôle liées à un service pour AWSServiceRoleForZonalAutoshiftPracticeRun

Ce rôle lié à un service utilise la politique gérée. `AWSZonalAutoshiftPracticeRunSLRPolicy`

Le rôle AWSServiceRoleForZonalAutoshiftPracticeRunlié à un service fait confiance au service suivant pour assumer le rôle :

- `practice-run.arc-zonal-shift.amazonaws.com`

Pour consulter les autorisations associées à cette politique, reportez-vous AWSZonalAutoshiftPracticeRunSLRPolicyà la référence des politiques AWS gérées.

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 Autorisations de rôles liés à un service dans le Guide de l'utilisateur IAM.

Création du rôle AWSServiceRoleForZonalAutoshiftPracticeRunlié à un service pour Route 53 ARC

Il n'est pas nécessaire de créer manuellement le rôle AWSServiceRoleForZonalAutoshiftPracticeRunlié à un service. Lorsque vous créez la première configuration d'exécution dans le SDK AWS Management Console AWS CLI, le ou un AWS SDK, Route 53 ARC crée le rôle lié au service pour vous.

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 la première configuration d'exécution, Route 53 ARC crée à nouveau le rôle lié au service pour vous.

Modification du rôle AWSServiceRoleForZonalAutoshiftPracticeRunlié à un service pour Route 53 ARC

Route 53 ARC ne vous permet pas de modifier le rôle AWSServiceRoleForZonalAutoshiftPracticeRunlié au service. Après avoir créé le rôle lié à un service, vous ne pouvez pas modifier le nom du rôle car d'autres entités peuvent le référencer. 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 du rôle AWSServiceRoleForZonalAutoshiftPracticeRunlié à un service pour Route 53 ARC

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. Toutefois, vous devez nettoyer les ressources d'un rôle lié à un service avant de pouvoir le supprimer manuellement.

Après avoir désactivé le changement automatique, vous pouvez supprimer le rôle lié au AWSServiceRoleForZonalAutoshiftPracticeRunservice. Pour plus d'informations sur la fonctionnalité de changement automatique, consultezChangement de zone dans Amazon Route 53 Application Recovery Controller.

> **Note**
>
> Si le service Route 53 ARC utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression du rôle de service risque d'échouer. Dans ce cas, attendez quelques minutes et réessayez de supprimer le rôle.

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 AWSServiceRoleForZonalAutoshiftPracticeRun service. Pour plus d'informations, consultez Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Mises à jour du rôle lié au service Route 53 ARC pour le changement automatique zonal

Pour les mises à jour des politiques AWS gérées pour les rôles liés au service Route 53 ARC, consultez le tableau des mises à jour des politiques AWS gérées pour Route 53 ARC. Vous pouvez également vous abonner aux alertes RSS automatiques sur la page d'historique des documents ARC de la Route 53.

AWS politiques gérées pour l'autoshift zonal dans Amazon Route 53 Application Recovery Controller

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 la section Politiques gérées par AWS dans le Guide de l'utilisateur IAM.

AWS politique gérée : AWSZonalAutoshiftPracticeRunSLRPolicy

Vous ne pouvez pas joindre de `AWSZonalAutoshiftPracticeRunSLRPolicy` à vos entités IAM. Cette politique est associée à un rôle lié à un service qui permet à Amazon Route 53 Application Recovery Controller d'effectuer les opérations suivantes pour le transfert automatique zonal :

- Surveillez les CloudWatch alarmes et les AWS Health Dashboard événements Amazon fournis par les clients pour les séances d'entraînement
- Gérer les courses d'entraînement (changements de zone d'entraînement)

Pour plus d'informations, consultez Utilisation du rôle lié au service pour le changement automatique de zone dans Route 53 ARC.

Mises à jour des politiques AWS gérées pour l'autoshift zonal

Pour plus de détails sur les mises à jour des politiques AWS gérées pour le changement automatique zonal dans Route 53 ARC depuis que ce service a commencé à suivre ces modifications, consultez. Mises à jour des politiques AWS gérées pour Amazon Route 53 Application Recovery Controller Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au fil RSS sur la page d'historique du document ARC Route 53.

Utiliser le contrôle du routage pour restaurer des applications multirégionales dans Amazon Route 53 Application Recovery Controller

Cette section explique comment utiliser la fonctionnalité de contrôle du routage d'Amazon Route 53 Application Recovery Controller afin de minimiser les perturbations et d'assurer la continuité pour vos utilisateurs lorsqu'une AWS application est déployée en plusieurs Régions AWS.

Vous pouvez également en apprendre davantage sur le contrôle de préparation, une fonctionnalité de Route 53 ARC que vous pouvez utiliser pour savoir si vos applications et vos ressources sont prêtes à être restaurées.

Les rubriques de cette section décrivent les fonctionnalités de contrôle du routage et de vérification de l'état de préparation, comment les configurer et comment les utiliser.

Rubriques

Contrôle du routage dans Amazon Route 53 Application Recovery Controller

Pour transférer le trafic vers plusieurs répliques d'applications Régions AWS, vous pouvez utiliser les contrôles de routage d'Amazon Route 53 Application Recovery Controller qui sont intégrés à un type spécifique de bilan de santé dans Amazon Route 53. Les commandes de routage sont de simples commutateurs marche-arrêt qui vous permettent de faire passer le trafic de votre client d'une réplique régionale à une autre. Le réacheminement du trafic est effectué par des vérifications de l'état du contrôle du routage configurées avec les enregistrements DNS Amazon Route 53. Par exemple, les enregistrements de basculement du DNS, associés aux noms de domaine qui font apparaître les répliques de votre application dans chaque région.

Cette section explique comment fonctionne le contrôle de routage, comment configurer les composants de contrôle de routage et comment les utiliser pour rediriger le trafic en cas de basculement.

Les composants du contrôle de routage de Route 53 ARC sont les suivants : les clusters, les panneaux de commande, les contrôles de routage et les bilans de santé du contrôle de routage. Toutes les commandes de routage sont regroupées sur des panneaux de commande. Vous pouvez les regrouper sur le panneau de configuration par défaut créé par Route 53 ARC pour votre cluster, ou créer vos propres panneaux de configuration personnalisés. Vous devez créer un cluster avant de créer un panneau de commande ou un contrôle de routage. Chaque cluster de Route 53 ARC est un plan de données composé de points de terminaison répartis en cinq Régions AWS.

Après avoir créé des contrôles de routage et des vérifications de l'état des contrôles de routage, vous pouvez créer des règles de sécurité pour le contrôle du routage afin de prévenir les effets secondaires involontaires de l'automatisation de la restauration. Vous pouvez mettre à jour les états du contrôle de routage pour rediriger le trafic, individuellement ou par lots, en utilisant les actions AWS CLI ou API (recommandées), ou en utilisant le. AWS Management Console

Cette section explique le fonctionnement des contrôles de routage, ainsi que la façon de les créer et de les utiliser pour rediriger le trafic de votre application.

> **Important**
>
> Pour savoir comment vous préparer à utiliser la Route 53 ARC pour rediriger le trafic dans le cadre d'un plan de basculement de votre application en cas de sinistre, voir. Meilleures pratiques pour le contrôle du routage dans Route 53 ARC

À propos du contrôle du routage

Le contrôle du routage redirige le trafic à l'aide de contrôles de santé dans Amazon Route 53 qui sont configurés avec des enregistrements DNS associés à la ressource de premier niveau des cellules de votre groupe de restauration, tels qu'un équilibreur de charge Elastic Load Balancing. Vous pouvez rediriger le trafic d'une cellule vers une autre, par exemple en mettant à jour un état de contrôle de routage `Off` (pour arrêter le flux de trafic vers une cellule) et en mettant à jour un autre état de contrôle de routage 0n (pour démarrer le flux de trafic vers une autre). Le processus qui modifie le flux de trafic est le bilan de santé de la Route 53 associé au contrôle de routage, une fois que Route 53 ARC l'a mis à jour pour le définir comme sain ou non sain, en fonction de l'état de contrôle de routage correspondant.

Les contrôles de routage prennent en charge le basculement sur tout AWS service doté d'un point de terminaison DNS. Vous pouvez mettre à jour les états du contrôle du routage pour faire basculer

le trafic à des fins de reprise après sinistre, lorsque vous détectez des baisses de latence pour votre application ou pour d'autres problèmes.

Vous pouvez également configurer des règles de sécurité pour le contrôle du routage, afin de vous assurer que le réacheminement du trafic à l'aide de contrôles de routage n'altère pas la disponibilité. Pour plus d'informations, consultez Création de règles de sécurité pour le contrôle du routage .

Il est important de noter que les contrôles de routage ne sont pas en eux-mêmes des bilans de santé destinés à surveiller l'état sous-jacent des terminaux. Par exemple, contrairement à une vérification de l'état de Route 53, un contrôle de routage ne surveille pas les temps de réponse ni les temps de connexion TCP. Un contrôle de routage est un simple interrupteur marche-arrêt qui commande un bilan de santé. Généralement, vous modifiez l'état pour rediriger le trafic, et ce changement d'état déplace le trafic vers un point de terminaison spécifique pour l'ensemble d'une pile d'applications, ou empêche le routage vers l'ensemble de la pile d'applications. Par exemple, dans un scénario simple, lorsque vous modifiez un état de contrôle de routage de `On` à`Off`, cela met à jour un bilan de santé de Route 53, que vous avez associé à un enregistrement de basculement DNS pour déplacer le trafic hors d'un point de terminaison.

Comment utiliser le contrôle de routage

Pour mettre à jour un état de contrôle de routage afin de pouvoir rediriger le trafic, vous devez vous connecter à l'un des points de terminaison de votre cluster dans Route 53 ARC. Si le point de terminaison auquel vous essayez de vous connecter n'est pas disponible, essayez de changer l'état avec un autre point de terminaison du cluster. Votre processus de modification des états de contrôle de routage doit être prêt à essayer chaque point de terminaison à tour de rôle, car les points de terminaison du cluster passent par des états disponibles et indisponibles pour une maintenance et des mises à jour régulières.

Lorsque vous créez des contrôles de routage, vous configurez vos enregistrements DNS pour associer les contrôles de santé des contrôles de routage aux noms DNS Route 53 figurant devant chaque réplique d'application. Par exemple, pour contrôler les basculements de trafic entre deux équilibreurs de charge, un dans chacune des deux régions, vous créez deux contrôles de santé du contrôle du routage et vous les associez à deux enregistrements DNS, par exemple des enregistrements Alias dotés de politiques de routage de basculement, avec les noms de domaine des équilibreurs de charge respectifs.

Vous pouvez également configurer des scénarios de basculement du trafic plus complexes en utilisant le contrôle de routage ARC de la Route 53, les contrôles de santé de la Route 53 et les ensembles d'enregistrements DNS, en utilisant des enregistrements DNS avec des politiques de

routage pondérées. Pour obtenir un exemple détaillé, consultez la section sur le basculement du trafic utilisateur dans le billet de AWS blog suivant : Création d'applications hautement résilientes à l'aide d'Amazon Route 53 Application Recovery Controller, partie 2 : Stack multirégional

Lorsque vous lancez un basculement pour un Région AWS contrôle de routage utilisateur, en raison des étapes liées à la circulation, il est possible que le trafic ne quitte pas immédiatement la région. L'établissement des connexions existantes en cours dans la région peut également prendre un certain temps, en fonction du comportement du client et de la réutilisation des connexions. En fonction de vos paramètres DNS et d'autres facteurs, les connexions existantes peuvent être établies en quelques minutes ou prendre plus de temps. Pour plus d'informations, consultez la section Veiller à ce que les changements de trafic se terminent rapidement.

Comment utiliser le contrôle de routage

Un contrôle de routage dans Route 53 ARC présente plusieurs avantages par rapport au réacheminement du trafic avec les bilans de santé traditionnels. Par exemple :

- Un contrôle de routage vous permet de basculer sur l'ensemble d'une pile d'applications. Cela contraste avec le fait de basculer sur les composants individuels d'une pile, comme le font les instances Amazon EC2, sur la base de contrôles de santé au niveau des ressources.
- Un contrôle de routage permet une dérogation manuelle simple et sûre que vous pouvez utiliser pour réaffecter le trafic à des fins de maintenance ou de reprise après une panne lorsque les moniteurs internes ne détectent aucun problème.
- Vous pouvez utiliser un contrôle de routage associé à des règles de sécurité pour éviter les effets secondaires courants qui peuvent survenir grâce à une automatisation entièrement automatisée basée sur des contrôles de santé, tels que le basculement vers une infrastructure de secours qui n'est pas préparée au basculement.

Voici un exemple d'intégration de contrôles de routage dans votre stratégie de basculement, afin d'améliorer la résilience et la disponibilité de vos applications dans AWS.

Vous pouvez prendre en charge AWS des applications à haute disponibilité AWS en exécutant plusieurs (généralement trois) répliques redondantes dans différentes régions. Vous pouvez ensuite utiliser le contrôle de routage Amazon Route 53 pour acheminer le trafic vers la réplique appropriée.

Par exemple, vous pouvez configurer une réplique d'application pour qu'elle soit active et qu'elle serve le trafic des applications, tandis qu'une autre est une réplique de secours. En cas de défaillance de votre réplique active, vous pouvez y rediriger le trafic utilisateur pour rétablir la

disponibilité de votre application. Vous devez décider si vous souhaitez vous éloigner ou non d'une réplique en vous basant sur les informations provenant de vos systèmes de surveillance et de contrôle de santé.

Si vous souhaitez accélérer les restaurations, une autre option que vous pouvez choisir pour votre architecture est une implémentation active-active. Avec cette approche, vos répliques sont actives en même temps. Cela signifie que vous pouvez remédier aux défaillances en éloignant les utilisateurs d'une réplique d'application endommagée en redirigeant simplement le trafic vers une autre réplique active.

AWS Disponibilité des régions pour le contrôle du routage

Pour obtenir des informations détaillées sur le support régional et les points de terminaison de service pour Amazon Route 53 Application Recovery Controller, consultez la section Points de terminaison et quotas Amazon Route 53 Application Recovery Controller dans le manuel Amazon Web Services General Reference.

> **Note**
>
> Le contrôle du routage dans Amazon Route 53 Application Recovery Controller est une fonctionnalité globale. Toutefois, vous devez spécifier la région USA Ouest (Oregon) (spécifiez le paramètre`--region us-west-2`) dans les AWS CLI commandes ARC de la Route 53 régionale. C'est-à-dire lorsque vous créez des ressources telles que des clusters, des panneaux de commande ou des contrôles de routage.

Un contrôle de routage ARC Route 53 est un interrupteur activé/désactivé qui modifie l'état d'un contrôle de santé de la Route 53 ARC, qui peut ensuite être associé à un enregistrement DNS qui redirige le trafic, par exemple, d'une réplique de déploiement principale vers une réplique de déploiement de secours.

En cas de défaillance d'une application ou de problème de latence, vous pouvez mettre à jour les états du contrôle de routage pour transférer le trafic de votre réplique principale vers, par exemple, une réplique de secours. En utilisant les opérations hautement fiables de l'API du plan de données Route 53 ARC pour effectuer des requêtes de contrôle de routage et des mises à jour de l'état du contrôle de routage, vous pouvez compter sur Route 53 ARC pour le basculement lors de scénarios de reprise après sinistre. Pour plus d’informations, consultez Obtenir et mettre à jour les états de contrôle du routage à l'aide de l'API Route 53 ARC (recommandé).

Route 53 ARC maintient les états de contrôle du routage dans un cluster, qui est un ensemble de cinq points de terminaison régionaux redondants. Route 53 ARC propage les changements d'état du contrôle de routage à travers le cluster, qui est situé dans une flotte Amazon EC2, afin d'obtenir un quorum dans cinq régions AWS . Après la propagation, lorsque vous demandez à Route 53 ARC un état de contrôle de routage, à l'aide de l'API et du plan de données hautement fiable, la vue consensuelle est renvoyée.

Vous pouvez interagir avec l'un des cinq points de terminaison du cluster pour mettre à jour l'état d'un contrôle de routage depuis, par exemple, `0ff` vers`0n`. Route 53 ARC propage ensuite la mise à jour dans les cinq régions du cluster.

La cohérence des données entre les cinq points de terminaison du cluster est atteinte en 5 secondes en moyenne, et au plus tard après 15 secondes au maximum.

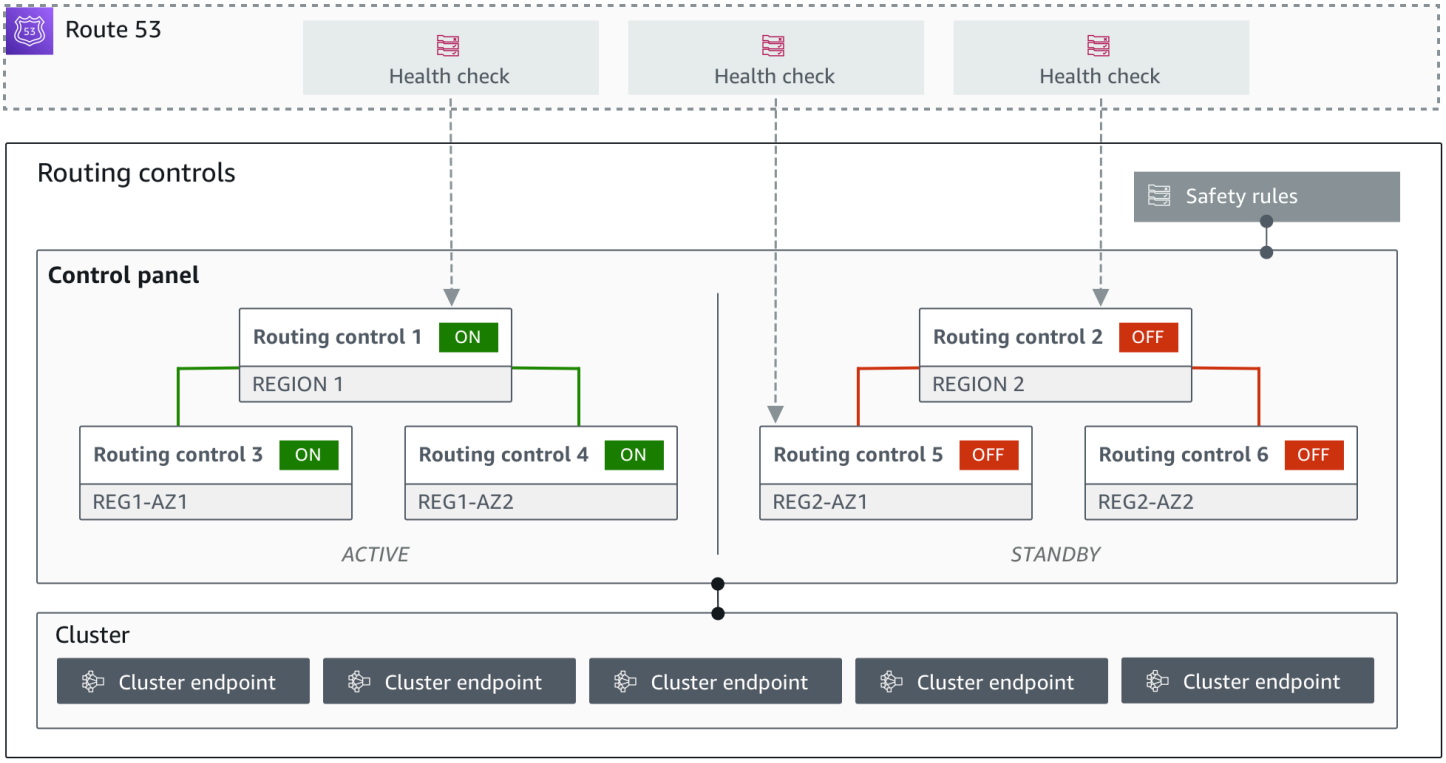
Route 53 ARC offre une fiabilité extrême grâce à son plan de données qui vous permet de basculer manuellement entre les cellules de votre application. Route 53 ARC garantit qu'au moins trois des cinq points de terminaison du cluster sont toujours accessibles pour effectuer des modifications d'état du contrôle du routage. Notez que chaque cluster ARC Route 53 est à locataire unique, afin de vous éviter d'être affecté par des « voisins bruyants » susceptibles de ralentir vos habitudes d'accès.

Lorsque vous modifiez les états du contrôle de routage, vous vous basez sur les trois critères suivants, qui sont très peu susceptibles d'échouer :

- Au moins trois de vos cinq points de terminaison sont disponibles et font partie du quorum.
- Vous disposez d'informations d'identification IAM valides et pouvez vous authentifier auprès d'un point de terminaison de cluster régional fonctionnel.
- Le plan de données Route 53 est en bon état (ce plan de données est conçu pour respecter un SLA de disponibilité à 100 %).

Composants de contrôle de routage

Le schéma suivant illustre un exemple de composants prenant en charge la fonctionnalité de contrôle de routage dans Route 53 ARC. Les contrôles de routage présentés ici (regroupés dans un seul panneau de configuration) vous permettent de gérer le trafic vers deux zones de disponibilité dans chacune des deux régions. Lorsque vous mettez à jour les états du contrôle de routage, Route 53 ARC modifie les contrôles de santé dans Amazon Route 53, qui redirigent le trafic DNS vers différentes cellules. Les règles de sécurité que vous configurez pour les contrôles de routage permettent d'éviter les scénarios d'ouverture défaillante et d'autres conséquences involontaires.



Voici les composants de la fonction de contrôle de routage de Route 53 ARC.

Cluster

Un cluster est un ensemble de cinq points de terminaison régionaux redondants par rapport auxquels vous lancez des appels d'API pour mettre à jour ou obtenir des états de contrôle de routage. Un cluster inclut un panneau de configuration par défaut, et vous pouvez héberger plusieurs panneaux de commande et contrôles de routage sur un seul cluster.

Contrôles de routage

Un contrôle de routage est un simple interrupteur marche/arrêt, hébergé sur un cluster, que vous utilisez pour contrôler le routage du trafic client entrant et sortant des cellules. Lorsque vous créez un contrôle de routage, vous ajoutez un contrôle de santé ARC de Route 53 dans Route 53. Cela vous permet de rediriger le trafic (à l'aide des contrôles de santé, configurés avec les enregistrements DNS pour vos applications) lorsque vous mettez à jour l'état du contrôle de routage dans Route 53 ARC.

Vérification de l'état du contrôle du routage

Les contrôles de routage sont intégrés aux contrôles de santé de Route 53. Les contrôles de santé sont associés aux enregistrements DNS qui précisent chaque réplique d'application, par exemple les enregistrements de basculement. Lorsque vous modifiez les états du contrôle de

routage, Route 53 ARC met à jour les contrôles de santé correspondants, qui redirigent le trafic, par exemple pour le basculer vers votre réplique de secours.

Panneau de commande

Un panneau de commande regroupe un ensemble de commandes de routage associées. Vous pouvez associer plusieurs contrôles de routage à un seul panneau de commande, puis créer des règles de sécurité pour le panneau de commande afin de garantir la sécurité des mises à jour de redirection du trafic que vous effectuez. Par exemple, vous pouvez configurer un contrôle de routage pour chacun de vos équilibreurs de charge dans chaque zone de disponibilité, puis les regrouper dans le même panneau de configuration. Vous pouvez ensuite ajouter une règle de sécurité (une « règle d'assertion ») qui garantit qu'au moins une zone (représentée par un contrôle de routage) est active à un moment donné, afin d'éviter des scénarios de « fail-open » involontaires.

Panneau de commande par défaut

Lorsque vous créez un cluster, Route 53 ARC crée un panneau de configuration par défaut. Par défaut, tous les contrôles de routage que vous créez sur le cluster sont ajoutés au panneau de configuration par défaut. Vous pouvez également créer vos propres panneaux de commande pour regrouper les commandes de routage associées.

Règle de sécurité

Les règles de sécurité sont des règles que vous ajoutez au contrôle du routage pour garantir que les actions de restauration ne compromettent pas accidentellement la disponibilité de votre application. Par exemple, vous pouvez créer une règle de sécurité qui crée un contrôle de routage qui agit comme un interrupteur global « on/off » afin que vous puissiez activer ou désactiver un ensemble d'autres contrôles de routage.

Endpoint (point de terminaison du cluster)

Chaque cluster de Route 53 ARC possède cinq points de terminaison régionaux que vous pouvez utiliser pour définir et récupérer les états de contrôle du routage. Votre processus d'accès aux points de terminaison doit partir du principe que Route 53 ARC active et arrête régulièrement les points de terminaison pour des raisons de maintenance. Vous devez donc essayer chaque point de terminaison l'un après l'autre jusqu'à ce que vous vous connectiez à l'un d'entre eux. Vous accédez aux points de terminaison pour connaître l'état actuel des contrôles de routage (Activé ou Désactivé) et pour déclencher des basculements pour vos applications en modifiant l'état des contrôles de routage.

Plans de données et de contrôle pour le contrôle du routage

Lorsque vous planifiez le basculement et la reprise après sinistre, évaluez la résilience de vos mécanismes de basculement. Nous vous recommandons de vous assurer que les mécanismes sur lesquels vous comptez lors du basculement sont hautement disponibles, afin de pouvoir les utiliser lorsque vous en avez besoin en cas de sinistre. En règle générale, vous devez utiliser les fonctions du plan de données pour vos mécanismes chaque fois que vous le pouvez, pour une fiabilité et une tolérance aux pannes optimales. Dans cette optique, il est important de comprendre comment les fonctionnalités d'un service sont réparties entre les plans de contrôle et les plans de données, et de comprendre dans quels cas vous pouvez compter sur une fiabilité extrême en ce qui concerne le plan de données d'un service.

Comme pour la plupart des AWS services, la fonctionnalité de contrôle du routage est prise en charge par les plans de contrôle et les plans de données. Bien que les deux soient conçus pour être fiables, un plan de contrôle est optimisé pour la cohérence des données, tandis qu'un plan de données est optimisé pour la disponibilité. Un plan de données est conçu pour être résilient afin de maintenir sa disponibilité même en cas d'événements perturbateurs, lorsqu'un plan de contrôle peut devenir indisponible.

En général, un plan de contrôle vous permet d'exécuter des fonctions de gestion de base, telles que la création, la mise à jour et la suppression de ressources dans le service. Un plan de données fournit les fonctionnalités de base d'un service. C'est pourquoi nous vous recommandons d'utiliser les opérations du plan de données lorsque la disponibilité est importante, par exemple lorsque vous devez rediriger le trafic vers une réplique de secours lors d'une panne.

Pour le contrôle du routage, les plans de contrôle et les plans de données sont répartis comme suit :

- L'API du plan de contrôle pour le contrôle du routage est l'API Recovery Control Configuration, prise en charge dans la région USA Ouest (Oregon) (us-west-2). Vous utilisez ces opérations d'API ou les AWS Management Console pour créer ou supprimer des clusters, des panneaux de commande et des contrôles de routage, afin de vous préparer à un événement de reprise après sinistre lorsque vous devrez peut-être rediriger le trafic pour votre application. Le plan de contrôle de configuration du contrôle de routage n'est pas hautement disponible.
- Le plan de données de contrôle du routage est un cluster dédié à cinq régions géographiquement isolées AWS . Chaque client crée un ou plusieurs clusters à l'aide du plan de contrôle de routage. Le cluster héberge des panneaux de commande et des commandes de routage. Vous utilisez ensuite l'API Routing Control (Recovery Cluster) pour obtenir, répertorier et mettre à jour les états

du contrôle de routage lorsque vous souhaitez rediriger le trafic pour votre application. Le plan de données de contrôle de routage EST hautement disponible.

Le plan de données de contrôle de routage étant hautement disponible, nous vous recommandons de prévoir d'utiliser le AWS Command Line Interface pour effectuer des appels d'API afin de fonctionner avec les états du contrôle de routage lorsque vous souhaitez basculer pour récupérer après un événement. Pour plus d'informations sur les principales considérations à prendre en compte lors de la préparation et de la réalisation d'une opération de restauration avec contrôle de routage, consultezMeilleures pratiques pour le contrôle du routage dans Route 53 ARC.

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

Balisage pour le contrôle du routage dans Amazon Route 53 Application Recovery Controller

Les balises sont des mots ou des phrases (métadonnées) que vous utilisez pour identifier et organiser vos AWS ressources. Vous pouvez ajouter plusieurs balises à une ressource, chacune de ces balises étant composée d'une clé et d'une valeur que vous définissez. Par exemple, la clé peut être l'environnement et la valeur peut être la production. Vous pouvez rechercher et filtrer vos ressources en fonction des balises que vous ajoutez.

Vous pouvez étiqueter les ressources suivantes dans le contrôle du routage dans Route 53 ARC :

- Clusters
- Panneaux de commande
- Règles de sécurité

Le balisage dans Route 53 ARC n'est disponible que via l'API, par exemple en utilisant le AWS CLI.

Vous trouverez ci-dessous des exemples de balisage dans le contrôle du routage à l'aide du AWS CLI.

```
aws route53-recovery-control-config --region us-west-2 create-cluster --
cluster-name example1-cluster --tags Region=PDX,Stage=Prod
```

```
aws route53-recovery-control-config --region us-west-2 create-control-panel
--control-panel-name example1-control-panel --cluster-arn arn:aws:route53-
recovery-control::111122223333:cluster/5678abcd-abcd-5678-abcd-5678abcdefgh
--tags Region=PDX,Stage=Prod
```

Pour plus d'informations, consultez TagResourcele Guide de référence de l'API de configuration de Recovery Control pour Amazon Route 53 Application Recovery Controller.

Tarification du contrôle du routage dans Route 53 ARC

Avec Amazon Route 53 Application Recovery Controller, vous ne payez que pour ce que vous configurez pour être utilisé dans le service. Pour le contrôle du routage dans Route 53 ARC, vous payez un coût horaire par cluster que vous créez. Chaque cluster peut héberger plusieurs contrôles de routage, que vous pouvez utiliser pour déclencher le basculement des applications.

Pour aider à gérer les coûts et à améliorer l'efficacité, vous pouvez configurer le partage entre comptes pour un cluster, afin de partager un cluster avec plusieurs AWS comptes. Pour plus d'informations, consultez Support multi-comptes pour les clusters dans Route 53 ARC.

Pour obtenir des informations détaillées sur les tarifs de Route 53 ARC et des exemples de tarification, consultez les tarifs d'Amazon Route 53 Application Recovery Controller et faites défiler la page vers le bas jusqu'à Amazon Route 53 Application Recovery Controller.

Commencer à utiliser la restauration multirégionale dans Amazon Route 53 Application Recovery Controller

Pour faire basculer vos applications à l'aide du contrôle de routage dans Amazon Route 53 Application Recovery Controller, vous devez disposer d' AWS applications multiples Régions AWS. Pour commencer, assurez-vous d'abord que vos applications sont configurées dans des répliques cloisonnées dans chaque région, afin de pouvoir passer de l'une à l'autre lors d'un événement. Vous pouvez ensuite créer des contrôles de routage pour rediriger le trafic de l'application afin de le faire basculer d'une application principale vers une application secondaire, afin de garantir la continuité pour vos utilisateurs.

> **Note**
>
> Si votre application est cloisonnée par zones de disponibilité, pensez à utiliser le décalage de zone ou le décalage automatique de zone pour la reprise après incident. Aucune

configuration n'est requise pour utiliser le décalage de zone ou le décalage automatique de zone afin de restaurer de manière fiable les applications en cas de détérioration de la zone de disponibilité. Pour plus d'informations, consultez Utilisez le décalage de zone et le décalage automatique de zone pour restaurer les applications dans Amazon Route 53 Application Recovery Controller.

Afin que vous puissiez utiliser le contrôle de routage ARC de Route 53 pour récupérer des applications lors d'un événement, nous vous recommandons de configurer au moins deux applications qui soient des répliques l'une de l'autre. Chaque réplique, ou cellule, représente un Région AWS. Après avoir configuré les ressources de votre application pour qu'elles s'alignent sur les régions, assurez-vous que votre application est configurée pour une restauration réussie en suivant les étapes suivantes.

Conseil : Pour simplifier la configuration, nous fournissons AWS CloudFormation des modèles HashiCorp Terraform qui créent une application avec des répliques redondantes qui échouent indépendamment les unes des autres. Pour en savoir plus et télécharger les modèles, consultezConfiguration d'un exemple d'application.

Pour vous préparer à utiliser le contrôle de routage, assurez-vous que votre application est configurée pour être résiliente en procédant comme suit :

1. Créez des copies indépendantes de votre pile d'applications (couche réseau et couche informatique) qui sont des répliques les unes des autres dans chaque région afin de pouvoir transférer le trafic de l'une à l'autre en cas d'événement. Assurez-vous que le code de votre application ne comporte aucune dépendance entre régions susceptible d'avoir un impact sur l'autre en cas de défaillance d'une réplique. Pour réussir à passer de l'une à l' Régions AWS autre, les limites de votre pile doivent se situer dans une région.
2. Dupliquez toutes les données dynamiques requises pour votre application sur les répliques. Vous pouvez utiliser les services AWS de base de données pour vous aider à répliquer vos données.

Commencez à contrôler le routage pour le basculement du trafic

Le contrôle du routage dans Amazon Route 53 Application Recovery Controller vous permet de déclencher le basculement de votre trafic entre des copies d'applications redondantes, ou répliques, exécutées séparément. Régions AWS Le basculement est effectué avec le DNS, à l'aide du plan de données Amazon Route 53.

Après avoir configuré vos répliques dans chaque région, comme décrit dans la section suivante, vous pouvez associer chacune d'elles à un contrôle de routage. Tout d'abord, vous associez les contrôles de routage aux noms de domaine de premier niveau de vos répliques dans chaque région. Vous ajoutez ensuite une vérification de l'état du contrôle de routage au contrôle de routage afin qu'il puisse activer et désactiver le flux de trafic. Cela vous permet de contrôler le routage du trafic entre les répliques de votre application.

Vous pouvez mettre à jour les états du contrôle de routage dans le AWS Management Console pour faire basculer le trafic, mais nous vous recommandons plutôt d'utiliser les actions ARC Route 53, en utilisant l'API ou AWS CLI pour les modifier. Les actions d'API ne dépendent pas de la console, elles sont donc plus résilientes.

Par exemple, pour passer d'une région à une autre, de us-west-1 à us-east-1, vous pouvez `update-routing-control-state` utiliser l'action de l'API pour définir l'état de to et de to. `us-west-1` `Off` `us-east-1` `On`

Avant de créer des composants de contrôle de routage pour configurer le basculement de votre application, assurez-vous que celle-ci est cloisonnée en répliques régionales, afin de pouvoir basculer de l'une à l'autre. Pour en savoir plus et commencer à cloisonner une nouvelle application ou à créer un exemple de stack, consultez les sections suivantes.

Configuration d'un exemple d'application

Pour vous aider à comprendre le fonctionnement du contrôle de routage, nous vous proposons un exemple d'application appelé`TicTacToe`. L'exemple utilise des AWS CloudFormation modèles pour simplifier le processus, ainsi que des modèles téléchargeables AWS CloudFormation et HashiCorp Terraform avec un exemple d'application afin que vous puissiez rapidement explorer vous-même la configuration et l'utilisation de Route 53 ARC.

Après avoir déployé l'exemple d'application, vous pouvez utiliser les modèles pour créer des composants ARC Route 53, puis explorer l'utilisation de contrôles de routage pour gérer le flux de trafic vers l'application. Vous pouvez adapter les modèles et le processus à votre propre scénario et à vos propres applications.

- AWS CloudFormation: Pour commencer avec un exemple d'application et des AWS CloudFormation modèles, consultez les instructions README ici sur ce compartiment Amazon S3. Pour en savoir plus sur l'utilisation AWS CloudFormation des modèles, consultez AWS CloudFormation les concepts du Guide de AWS CloudFormation l'utilisateur.

- HashiCorp Terraform : pour commencer avec un exemple d'application et des modèles Terraform, consultez les instructions README ici sur ce compartiment Amazon S3. Vous pouvez en savoir plus sur l'utilisation des modèles Terraform en lisant la HashiCorp documentation.

Meilleures pratiques pour le contrôle du routage dans Route 53 ARC

Nous recommandons les meilleures pratiques suivantes en matière de préparation à la restauration et au basculement pour le contrôle du routage dans Amazon Route 53 Application Recovery Controller.

Rubriques

Conservez les informations d' AWS identification spécialement conçues et durables, sécurisées et toujours accessibles

Dans un scénario de reprise après sinistre (DR), réduisez au minimum les dépendances du système en utilisant une approche simple pour accéder aux tâches de restauration AWS et les exécuter. Créez des informations d'identification IAM à longue durée de vie spécifiques aux tâches de reprise après sinistre, et conservez-les en toute sécurité dans un coffre-fort physique sur site ou un coffre-fort virtuel, pour y accéder en cas de besoin. Avec IAM, vous pouvez gérer de manière centralisée les informations d'identification de sécurité, telles que les clés d'accès et les autorisations d'accès aux AWS ressources. Pour les tâches autres que la reprise après sinistre, nous vous recommandons de continuer à utiliser l'accès fédéré, en utilisant AWS des services tels que l'authentification AWS unique.

Pour effectuer des tâches de basculement dans Route 53 ARC à l'aide de l'API du plan de données du cluster de restauration, vous pouvez associer une politique IAM Route 53 ARC à votre utilisateur. Pour en savoir plus, veuillez consulter la section Exemples de politiques basées sur l'identité dans Amazon Route 53 Application Recovery Controller.

Choisissez des valeurs TTL inférieures pour les enregistrements DNS impliqués dans le basculement

Pour les enregistrements DNS que vous devrez peut-être modifier dans le cadre de votre mécanisme de basculement, en particulier les enregistrements dont l'état est vérifié, l'utilisation de valeurs TTL inférieures est appropriée. La définition d'une TTL de 60 ou 120 secondes est un choix courant pour ce scénario.

Le paramètre DNS TTL (time to live) indique aux résolveurs DNS combien de temps ils doivent mettre en cache un enregistrement avant d'en demander un nouveau. Lorsque vous choisissez un TTL, vous faites un compromis entre latence, fiabilité et réactivité face au changement. Lorsque le TTL d'un enregistrement est plus court, les résolveurs DNS remarquent les mises à jour de l'enregistrement plus rapidement, car le TTL indique qu'ils doivent effectuer des requêtes plus fréquemment.

Pour plus d'informations, consultez Choisir des valeurs TTL pour les enregistrements DNS dans Meilleures pratiques pour le DNS Amazon Route 53.

Limitez le temps pendant lequel les clients restent connectés à vos terminaux

Lorsque vous utilisez des contrôles de routage pour passer de l'un Région AWS à l'autre, le mécanisme utilisé par Amazon Route 53 Application Recovery Controller pour déplacer le trafic de votre application est une mise à jour DNS. Cette mise à jour entraîne le renvoi de toutes les nouvelles connexions hors de la zone affectée.

Cependant, les clients disposant de connexions ouvertes préexistantes peuvent continuer à faire des demandes concernant l'emplacement altéré jusqu'à ce qu'ils se reconnectent. Pour garantir un rétablissement rapide, nous vous recommandons de limiter la durée pendant laquelle les clients restent connectés à vos terminaux.

Si vous utilisez un Application Load Balancer, vous pouvez utiliser `keepalive` cette option pour configurer la durée des connexions. Pour plus d'informations, consultez la section Durée de conservation du client HTTP dans le guide de l'utilisateur d'Application Load Balancer.

Par défaut, les équilibreurs de charge d'application définissent la durée de conservation du client HTTP sur 3 600 secondes, soit 1 heure. Nous vous suggérons de réduire la valeur pour qu'elle corresponde à votre objectif de temps de restauration pour votre application, par exemple 300

secondes. Lorsque vous choisissez une durée de conservation d'un client HTTP, considérez que cette valeur représente un compromis entre une reconnexion plus fréquente en général, ce qui peut affecter la latence, et le déplacement plus rapide de tous les clients loin d'une zone ou d'une région altérée.

Ajoutez à vos favoris ou codez en dur vos cinq points de terminaison du cluster régional et les ARN de contrôle de routage

Nous vous recommandons de conserver une copie locale des points de terminaison de votre cluster régional Route 53 ARC, dans des favoris ou de l'enregistrer dans le code d'automatisation que vous utilisez pour réessayer vos points de terminaison. En cas de panne, il se peut que vous ne puissiez pas accéder à certaines opérations d'API, notamment les opérations d'API ARC Route 53 qui ne sont pas hébergées sur le cluster de plans de données extrêmement fiable. Vous pouvez répertorier les points de terminaison de vos clusters Route 53 ARC à l'aide de l'opération DescribeClusterAPI.

Choisissez l'un de vos points de terminaison au hasard pour mettre à jour vos états de contrôle de routage

Lorsque vous devez basculer, nous vous recommandons de mettre à jour (et de récupérer) les états du contrôle de routage à l'aide d'un point de terminaison aléatoire parmi les cinq points de terminaison de votre cluster régional. Si ce point de terminaison échoue, réessayez chacun de vos autres points de terminaison régionaux. Pour plus d'informations sur l'utilisation d'exemples de code avec le AWS SDK, notamment pour essayer des points de terminaison de cluster, consultez. Exemples de code pour Application Recovery Controller utilisant des AWS SDK

Utilisez l'API extrêmement fiable du plan de données pour répertorier et mettre à jour les états de contrôle du routage, et non la console

À l'aide de l'API du plan de données ARC Route 53, visualisez vos contrôles et états de routage à l'aide de l'opération ListRoutingControls et mettez à jour les états des contrôles de routage pour rediriger le trafic en cas de basculement avec l'UpdateRoutingControlStateopération. Vous pouvez utiliser le AWS CLI (comme dans ces exemples) ou le code que vous avez écrit à l'aide de l'un des AWS SDK. Route 53 ARC offre une fiabilité extrême grâce à l'API intégrée au plan de données qui permet de contourner le trafic. Nous vous recommandons d'utiliser l'API plutôt que de modifier les états de contrôle de routage dans le AWS Management Console.

Connectez-vous à l'un des points de terminaison de votre cluster régional pour Route 53 ARC afin d'utiliser l'API du plan de données. Si le point de terminaison n'est pas disponible, essayez de vous connecter à un autre point de terminaison du cluster.

Si une règle de sécurité bloque une mise à jour de l'état du contrôle de routage, vous pouvez la contourner pour effectuer la mise à jour et inverser le trafic. Pour plus d'informations, consultez Dérogation aux règles de sécurité pour réacheminer le trafic.

Testez le basculement avec Route 53 ARC

Testez régulièrement le basculement avec le contrôle de routage ARC Route 53, afin de passer de votre pile d'applications principale à une pile d'applications secondaire. Il est important de vous assurer que les structures ARC de la Route 53 que vous avez ajoutées sont alignées sur les bonnes ressources de votre pile et que tout fonctionne comme prévu. Vous devez le tester après avoir configuré Route 53 ARC pour votre environnement, et continuer à effectuer des tests périodiques, afin que votre environnement de basculement soit préparé, avant que vous ne subissiez une situation de panne dans laquelle vous auriez besoin que votre système secondaire soit rapidement opérationnel afin d'éviter les temps d'arrêt pour vos utilisateurs.

Opérations de l'API de contrôle du routage

Cette section inclut des tableaux répertoriant les opérations d'API que vous pouvez utiliser pour configurer et utiliser le contrôle de routage dans Amazon Route 53 Application Recovery Controller, ainsi que des liens vers la documentation pertinente.

Pour des exemples d'utilisation des opérations d'API de configuration de contrôle de routage courantes avec le AWS Command Line Interface, voir Exemples d'utilisation des opérations de l'API de contrôle de routage ARC Route 53 avec AWS CLI.

Le tableau suivant répertorie les opérations de l'API ARC Route 53 que vous pouvez utiliser pour la configuration du contrôle de routage, avec des liens vers la documentation pertinente.

Action	Utilisation de la console Route 53 ARC	Utilisation de l'API ARC Route 53
Créer un cluster	Consultez Création de composants de contrôle de routage dans Route 53 ARC .	Consultez CreateCluster
Décrire un cluster	Consultez Création de composants de contrôle de routage dans Route 53 ARC .	Consultez DescribeCluster

Action	Utilisation de la console Route 53 ARC	Utilisation de l'API ARC Route 53
Supprimer un cluster	Consultez Création de composants de contrôle de routage dans Route 53 ARC .	Consultez DeleteCluster
Répertorier les clusters d'un compte	Consultez Création de composants de contrôle de routage dans Route 53 ARC .	Consultez ListClusters
Création d'un contrôle de routage	Consultez Création de composants de contrôle de routage dans Route 53 ARC .	Voir CreateRoutingControl
Décrire un contrôle de routage	Consultez Création de composants de contrôle de routage dans Route 53 ARC .	Voir DescribeRoutingControl
Mettre à jour un contrôle de routage	Consultez Création de composants de contrôle de routage dans Route 53 ARC .	Voir UpdateRoutingControl
Supprimer un contrôle de routage	Consultez Création de composants de contrôle de routage dans Route 53 ARC .	Voir DeleteRoutingControl
Lister les contrôles de routage	Consultez Création de composants de contrôle de routage dans Route 53 ARC .	Voir ListRoutingContrôles
Création d'un panneau de commande	Consultez Création de composants de contrôle de routage dans Route 53 ARC .	Voir le CreateControlpanneau
Décrire un panneau de commande	Consultez Création de composants de contrôle de routage dans Route 53 ARC .	Voir le DescribeControlpanneau

Action	Utilisation de la console Route 53 ARC	Utilisation de l'API ARC Route 53
Mettre à jour un panneau de commande	Consultez Création de composants de contrôle de routage dans Route 53 ARC .	Voir le UpdateControlpanneau
Supprimer un panneau de commande	Consultez Création de composants de contrôle de routage dans Route 53 ARC .	Voir le DeleteControlpanneau
Lister les panneaux de commande	Consultez Création de composants de contrôle de routage dans Route 53 ARC .	Voir les ListControlpanneaux
Création d'une règle de sécurité	Consultez Création de règles de sécurité pour le contrôle du routage .	Voir la CreateSafetyrègle
Décrire une règle de sécurité	Consultez Création de règles de sécurité pour le contrôle du routage .	Voir la DescribeSafetyrègle
Mettre à jour une règle de sécurité	Consultez Création de règles de sécurité pour le contrôle du routage .	Voir la UpdateSafetyrègle
Supprimer une règle de sécurité	Consultez Création de règles de sécurité pour le contrôle du routage .	Voir la DeleteSafetyrègle
Énumérer les règles de sécurité	Consultez Création de règles de sécurité pour le contrôle du routage .	Voir les ListSafetyrègles
Répertorier les bilans de santé associés à Route 53	Consultez Création d'un contrôle de santé du contrôle de routage dans Route 53 ARC .	Voir ListAssociatedRoute 53 HealthChecks

Action	Utilisation de la console Route 53 ARC	Utilisation de l'API ARC Route 53
Répertorier les politiques de AWS RAM ressources pour le partage de clusters	Consultez Support multi-comptes pour les clusters dans Route 53 ARC.	Voir la GetResourcepolitique

Le tableau suivant répertorie les opérations courantes de l'API ARC Route 53 que vous pouvez utiliser pour gérer le basculement du trafic avec le plan de données de contrôle du routage, avec des liens vers la documentation pertinente.

Action	Utilisation de la console Route 53 ARC	Utilisation de l'API ARC Route 53
Obtenir un état de contrôle de routage	Consultez Obtenir et mettre à jour les états de contrôle de routage dans AWS Management Console.	Voir GetRoutingControlState
Lister les contrôles de routage	N/A	Voir ListRoutingContrôles
Mettre à jour un état de contrôle de routage	Consultez Obtenir et mettre à jour les états de contrôle de routage dans AWS Management Console.	Voir UpdateRoutingControlState
Mettre à jour plusieurs états de contrôle de routage	Consultez Obtenir et mettre à jour les états de contrôle de routage dans AWS Management Console.	Voir UpdateRoutingControlStates

Utilisation de ce service avec un AWS SDK

AWS des kits de développement logiciel (SDK) sont disponibles pour de nombreux langages de programmation populaires. 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 for C++	AWS SDK for C++ exemples de code
AWS CLI	AWS CLI exemples de code
AWS SDK for Go	AWS SDK for Go exemples de code
AWS SDK for Java	AWS SDK for Java exemples de code
AWS SDK for JavaScript	AWS SDK for JavaScript exemples de code
Kit AWS SDK pour Kotlin	Kit AWS SDK pour Kotlin exemples de code
AWS SDK for .NET	AWS SDK for .NET exemples de code
AWS SDK for PHP	AWS SDK for PHP exemples de code
AWS Tools for PowerShell	Outils pour des exemples PowerShell de code
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto3) exemples de code
AWS SDK for Ruby	AWS SDK for 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 voir des exemples spécifiques à ce service, consultez Exemples de code pour Application Recovery Controller utilisant des AWS SDK.

Exemple de disponibilité

Vous n'avez pas trouvé ce dont vous avez besoin ? Demandez un exemple de code en utilisant le lien Faire un commentaire en bas de cette page.

Exemples d'utilisation des opérations de l'API de contrôle de routage ARC Route 53 avec AWS CLI

Cette section présente des exemples d'applications simples illustrant l'utilisation du contrôle de routage, en utilisant la AWS Command Line Interface fonctionnalité de contrôle de routage d'Amazon Route 53 Application Recovery Controller à l'aide d'opérations d'API. Les exemples sont destinés à vous aider à acquérir une compréhension de base de la manière d'utiliser le contrôle de routage à l'aide de la CLI.

Grâce au contrôle du routage dans Amazon Route 53 Application Recovery Controller, vous pouvez déclencher des basculements de trafic entre des copies d'applications redondantes, ou répliques, exécutées dans des zones distinctes Régions AWS ou des zones de disponibilité.

Vous organisez les contrôles de routage en groupes appelés panneaux de commande qui sont provisionnés sur un cluster. Un cluster ARC Route 53 est un ensemble régional de points de terminaison déployés dans le monde entier. Les points de terminaison du cluster fournissent une API hautement disponible que vous pouvez utiliser pour définir et récupérer les états de contrôle du routage. Pour plus d'informations sur les composants de la fonction de contrôle de routage, consultezComposants de contrôle de routage .

> **Note**
>
> Route 53 ARC est un service mondial qui prend en charge plusieurs Régions AWS points de terminaison. Toutefois, vous devez spécifier la région USA Ouest (Oregon), c'est-à-dire spécifier le paramètre`--region us-west-2`, dans la plupart des commandes de la Route 53 ARC CLI. Par exemple, utilisez le `region` paramètre lorsque vous créez des groupes de récupération, des panneaux de commande et des clusters.
> Lorsque vous créez un cluster, Route 53 ARC vous fournit un ensemble de points de terminaison régionaux. Pour obtenir ou mettre à jour les états du contrôle de routage, vous devez spécifier le point de terminaison régional (le point de terminaison Région AWS et l'URL du point de terminaison) dans votre commande CLI.

Pour plus d'informations sur l'utilisation du AWS CLI, consultez la référence des AWS CLI commandes. Pour obtenir la liste des actions de l'API de contrôle du routage, reportez-vous Opérations de l'API de contrôle du routage aux sections et Opérations de l'API de contrôle du routage.

Nous allons commencer par créer les composants dont vous avez besoin pour gérer le basculement à l'aide des contrôles de routage, en commençant par créer un cluster.

Configuration des composants de contrôle de routage

Notre première étape consiste à créer un cluster. Un cluster ARC Route 53 est un ensemble de cinq points de terminaison, un dans chacun des cinq points différents Régions AWS. L'infrastructure Route 53 ARC permet à ces terminaux de fonctionner de manière coordonnée afin de garantir la haute disponibilité et la cohérence séquentielle des opérations de basculement.

1. Créer un cluster

1a. Créer un cluster.

```
aws route53-recovery-control-config --region us-west-2 create-cluster --cluster-name
 NewCluster
```

```
{
    "Cluster": {
        "ClusterArn": "arn:aws:route53-recovery-control::111122223333:cluster/5678abcd-
abcd-5678-abcd-5678abcdefgh",
        "Name": "NewCluster",
        "Status": "PENDING"
    }
}
```

Lorsque vous créez une ressource ARC Route 53 pour la première fois, son statut est « `PENDING` pendant la création du cluster ». Vous pouvez suivre son évolution en appelant`describe-cluster`.

1b. Décrivez un cluster.

```
aws route53-recovery-control-config --region us-west-2 \
    describe-cluster --cluster-arn arn:aws:route53-recovery-
control::111122223333:cluster/5678abcd-abcd-5678-abcd-5678abcdefgh
```

```
{
    "Cluster":{
        "ClusterArn": "arn:aws:route53-recovery-control::111122223333:cluster/5678abcd-
abcd-5678-abcd-5678abcdefgh",
```

```
        "ClusterEndpoints":[
            {"Endpoint": "https://host-aaaaaa.us-east-1.example.com", "Region":"us-
east-1"},
            {"Endpoint": "https://host-bbbbbb.ap-southeast-2.example.com",
 "Region":"ap-southeast-2"},
            {"Endpoint": "https://host-cccccc.eu-west-1.example.com", "Region":"eu-
west-1"},
            {"Endpoint": "https://host-dddddd.us-west-2.example.com", "Region":"us-
west-2"},
            {"Endpoint": "https://host-eeeeee.ap-northeast-1.example.com",
 "Region":"ap-northeast-1"}
        ]
        "Name": "NewCluster",
        "Status": "DEPLOYED"
    }
}
```

Lorsque le statut est DÉPLOYÉ, Route 53 ARC a créé avec succès le cluster avec l'ensemble de points de terminaison avec lesquels vous pouvez interagir. Vous pouvez répertorier tous vos clusters en appelant`list-clusters`.

1 c. Répertoriez vos clusters.

```
aws route53-recovery-control-config --region us-west-2 list-clusters
```

```
{
    "Clusters": [
        {
            "ClusterArn": "arn:aws:route53-recovery-
control::111122223333:cluster/1234abcd-abcd-1234-abcd-1234abcdefgh",
            "ClusterEndpoints":[
                {"Endpoint": "https://host-aaaaaa.us-east-1.example.com", "Region":"us-
east-1"},
                {"Endpoint": "https://host-bbbbbb.ap-southeast-2.example.com",
 "Region":"ap-southeast-2"},
                {"Endpoint": "https://host-cccccc.eu-west-1.example.com", "Region":"eu-
west-1"},
                {"Endpoint": "https://host-dddddd.us-west-2.example.com", "Region":"us-
west-2"},
                {"Endpoint": "https://host-eeeeee.ap-northeast-1.example.com",
 "Region":"ap-northeast-1"}
            ],
```

```
            "Name": "AnotherCluster",
            "Status": "DEPLOYED"
        },
        {
            "ClusterArn": "arn:aws:route53-recovery-
control::111122223333:cluster/5678abcd-abcd-5678-abcd-5678abcdefgh",
            "ClusterEndpoints": [
                {"Endpoint": "https://host-ffffff.us-east-1.example.com", "Region":"us-
east-1"},
                {"Endpoint": "https://host-gggggg.ap-southeast-2.example.com",
 "Region":"ap-southeast-2"},
                {"Endpoint": "https://host-hhhhhh.eu-west-1.example.com", "Region":"eu-
west-1"},
                {"Endpoint": "https://host-iiiiii.us-west-2.example.com", "Region":"us-
west-2"},
                {"Endpoint": "https://host-jjjjjj.ap-northeast-1.example.com",
 "Region":"ap-northeast-1"}
            ],
            "Name": "NewCluster",
            "Status": "DEPLOYED"
        }
    ]
}
```

2. Création d'un panneau de commande

Un panneau de commande est un regroupement logique permettant d'organiser vos contrôles de routage Route 53 ARC. Lorsque vous créez un cluster, Route 53 ARC fournit automatiquement un panneau de commande pour vous appeler`DefaultControlPanel`. Vous pouvez utiliser ce panneau de commande immédiatement.

Un panneau de commande ne peut exister que dans un seul cluster. Si vous souhaitez déplacer un panneau de configuration vers un autre cluster, vous devez le supprimer puis le créer dans le second cluster. Vous pouvez voir tous les panneaux de commande de votre compte en appelant`list-control-panels`. Pour afficher uniquement les panneaux de commande d'un cluster spécifique, ajoutez le `--cluster-arn` champ.

2a. Répertoriez les panneaux de commande.

```
aws route53-recovery-control-config --region us-west-2 \
    list-control-panels --cluster-arn arn:aws:route53-recovery-
control::111122223333:cluster/eba23304-1a51-4674-ae32-b4cf06070bdd
```

```
{
    "ControlPanels": [
        {
            "ControlPanelArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/1234567dddddd1234567dddddd1234567",
            "ClusterArn": "arn:aws:route53-recovery-
control::111122223333:cluster/5678abcd-abcd-5678-abcd-5678abcdefgh",
            "DefaultControlPanel": true,
            "Name": "DefaultControlPanel",
            "RoutingControlCount": 0,
            "Status": "DEPLOYED"
        }
    ]
}
```

Vous pouvez éventuellement créer votre propre panneau de commande en appelant`create-control-panel`.

2 b. Créez un panneau de commande.

```
aws route53-recovery-control-config --region us-west-2 create-control-panel \
        --control-panel-name NewControlPanel2 \
        --cluster-arn arn:aws:route53-recovery-control::111122223333:cluster/5678abcd-
abcd-5678-abcd-5678abcdefgh
```

```
{
    "ControlPanel": {
        "ControlPanelArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456",
        "ClusterArn": "arn:aws:route53-recovery-control::111122223333:cluster/5678abcd-
abcd-5678-abcd-5678abcdefgh",
        "DefaultControlPanel": false,
        "Name": "NewControlPanel2",
        "RoutingControlCount": 0,
        "Status": "PENDING"
    }
}
```

Lorsque vous créez une ressource ARC Route 53 pour la première fois, son statut est « `PENDING` en cours de création ». Vous pouvez vérifier les progrès en appelant`describe-control-panel`.

2 c. Décrivez un panneau de commande.

```
aws route53-recovery-control-config --region us-west-2 describe-control-panel \
    --control-panel-arn arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456
```

```
{
    "ControlPanel": {
        "ControlPanelArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456",
        "ClusterArn": "arn:aws:route53-recovery-control::111122223333:cluster/5678abcd-
abcd-5678-abcd-5678abcdefgh",
        "DefaultControlPanel": true,
        "Name": "DefaultControlPanel",
        "RoutingControlCount": 0,
        "Status": "DEPLOYED"
    }
}
```

3. Création d'un contrôle de routage

Maintenant que vous avez configuré le cluster et examiné les panneaux de commande, vous pouvez commencer à créer des contrôles de routage. Lorsque vous créez un contrôle de routage, vous devez au moins spécifier le nom de ressource Amazon (ARN) du cluster dans lequel vous souhaitez placer le contrôle de routage. Vous pouvez également spécifier l'ARN d'un panneau de commande pour le contrôle du routage. Vous devez également spécifier le cluster dans lequel se trouve le panneau de commande.

Si vous ne spécifiez pas de panneau de commande, votre contrôle de routage est ajouté au panneau de commande créé automatiquement,`DefaultControlPanel`.

Créez un contrôle de routage en appelant`create-routing-control`.

3a. Créez un contrôle de routage.

```
aws route53-recovery-control-config --region us-west-2 create-routing-control \
    --routing-control-name NewRc1 \
    --cluster-arn arn:aws:route53-recovery-control::111122223333:cluster/5678abcd-
abcd-5678-abcd-5678abcdefgh
```

```
{
    "RoutingControl": {
```

```
        "ControlPanelArn": " arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456",
        "Name": "NewRc1",
        "RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567",
        "Status": "PENDING"
    }
}
```

Les contrôles de routage suivent le même modèle de création que les autres ressources ARC Route 53. Vous pouvez donc suivre leur progression en appelant une opération de description.

3b. Décrivez le contrôle du routage.

```
aws route53-recovery-control-config --region us-west-2 describe-routing-control \
       --routing-control-arn arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567
```

```
{
    "RoutingControl": {
        "ControlPanelArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456",
        "Name": "NewRc1",
        "RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567",
        "Status": "DEPLOYED"
    }
}
```

Vous pouvez répertorier les commandes de routage dans un panneau de commande en appelant`list-routing-controls`. L'ARN du panneau de commande est requis.

3c. Répertoriez les contrôles de routage.

```
aws route53-recovery-control-config --region us-west-2 list-routing-controls \
        --control-panel-arn arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456
```

```
{
```

```
    "RoutingControls": [
        {
            "ControlPanelArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456",
            "Name": "Rc1",
            "RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567",
            "Status": "DEPLOYED"
        },
        {
            "ControlPanelArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456",
            "Name": "Rc2",
            "RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
hijklmnop987654321",
            "Status": "DEPLOYED"
        }
    ]
}
```

Dans l'exemple suivant, lorsque nous travaillons avec des états de contrôle de routage, nous supposons que vous disposez des deux contrôles de routage répertoriés dans cette section (Rc1 et Rc2). Dans cet exemple, chaque contrôle de routage représente une zone de disponibilité dans laquelle votre application est déployée.

4. Créez des règles de sécurité

Lorsque vous utilisez plusieurs contrôles de routage en même temps, vous pouvez décider de mettre en place certaines mesures de protection lorsque vous les activez et les désactivez, afin d'éviter des conséquences involontaires, telles que la désactivation des deux contrôles de routage et l'arrêt de tout flux de trafic. Pour créer ces garanties, vous devez créer des règles de sécurité pour le contrôle du routage.

Il existe deux types de règles de sécurité : les règles d'assertion et les règles de blocage. Pour en savoir plus sur les règles de sécurité, consultezCréation de règles de sécurité pour le contrôle du routage .

L'appel suivant fournit un exemple de création d'une règle d'assertion qui garantit qu'au moins l'un des deux contrôles de routage est défini sur un 0n moment donné. Pour créer la règle, vous devez exécuter `create-safety-rule` le `assertion-rule` paramètre.

Pour obtenir des informations détaillées sur le fonctionnement de l'API des règles d'assertion, consultez AssertionRulele Guide de référence de l'API de contrôle de routage pour Amazon Route 53 Application Recovery Controller.

4a. Créez une règle d'assertion.

```
aws route53-recovery-control-config --region us-west-2 create-safety-rule \
        --assertion-rule '{"Name": "TestAssertionRule",
        "ControlPanelArn": "arn:aws:route53-recovery-
control::888888888888:controlpanel/zzz123yyy456xxx789zzz123yyy456xxx",
        "WaitPeriodMs": 5000,
        "AssertedControls":
        ["arn:aws:route53-recovery-control::888888888888:controlpanel/
zzz123yyy456xxx789zzz123yyy456xxx/routingcontrol/def123def123def"
        "arn:aws:route53-recovery-control::888888888888:controlpanel/
zzz123yyy456xxx789zzz123yyy456xxx/routingcontrol/ghi456ghi456ghi"],
        "RuleConfig": {"Threshold": 1, "Type": "ATLEAST", "Inverted": false}}'
```

```
{
    "Rule": {
        "ASSERTION": {
            "Arn": "arn:aws:route53-recovery-control::888888888888:controlpanel/
zzz123yyy456xxx789zzz123yyy456xxx/safetyrule/333333444444",
            "AssertedControls": [
                "arn:aws:route53-recovery-control::888888888888:controlpanel/
zzz123yyy456xxx789zzz123yyy456xxx/routingcontrol/def123def123def"
                "arn:aws:route53-recovery-control::888888888888:controlpanel/
zzz123yyy456xxx789zzz123yyy456xxx/routingcontrol/ghi456ghi456ghi"],
            "ControlPanelArn": "arn:aws:route53-recovery-
control::888888888888:controlpanel/zzz123yyy456xxx789zzz123yyy456xxx",
            "Name": "TestAssertionRule",
            "RuleConfig": {
                "Inverted": false,
                "Threshold": 1,
                "Type": "ATLEAST"
            },
            "Status": "PENDING",
            "WaitPeriodMs": 5000
        }
    }
}
```

L'appel suivant fournit un exemple de création d'une règle de blocage qui fournit un commutateur global « activé/désactivé » ou « blocage » pour un ensemble de contrôles de routage cibles dans un panneau de commande. Cela vous permet d'interdire la mise à jour des contrôles de routage cibles afin que, par exemple, l'automatisation ne puisse pas effectuer de mises à jour non autorisées. Dans cet exemple, le commutateur de déclenchement est une commande de routage spécifiée par le `GatingControls` paramètre et les deux commandes de routage contrôlées ou « fermées » sont spécifiées par le `TargetControls` paramètre.

> **Note**
>
> Avant de créer la règle de blocage, vous devez créer le contrôle de routage de blocage, qui n'inclut pas les enregistrements de basculement DNS, et les contrôles de routage cible, que vous configurez avec les enregistrements de basculement DNS.

Pour créer la règle, vous devez exécuter `create-safety-rule` le `gating-rule` paramètre.

Pour obtenir des informations détaillées sur le fonctionnement de l'API des règles d'assertion, consultez GatingRulele Guide de référence de l'API de contrôle de routage pour Amazon Route 53 Application Recovery Controller.

4 b. Créez une règle de blocage.

```
aws route53-recovery-control-config --region us-west-2 create-safety-rule \
        --gating-rule '{"Name": "TestGatingRule",
        "ControlPanelArn": "arn:aws:route53-recovery-
control::888888888888:controlpanel/zzz123yyy456xxx789zzz123yyy456xxx",
        "WaitPeriodMs": 5000,
        "GatingControls": ["arn:aws:route53-recovery-
control::888888888888:controlpanel/zzz123yyy456xxx789zzz123yyy456xxx/routingcontrol/
def123def123def"]
        "TargetControls": ["arn:aws:route53-recovery-
control::888888888888:controlpanel/zzz123yyy456xxx789zzz123yyy456xxx/routingcontrol/
ghi456ghi456ghi",
        "arn:aws:route53-recovery-control::888888888888:controlpanel/
zzz123yyy456xxx789zzz123yyy456xxx/routingcontrol/lmn789lmn789lmn"],
        "RuleConfig": {"Threshold": 0, "Type": "OR", "Inverted": false}}'
```

```
{
    "Rule": {
```

```
        "GATING": {
            "Arn": "arn:aws:route53-recovery-control::888888888888:controlpanel/
zzz123yyy456xxx789zzz123yyy456xxx/safetyrule/444444444444",
            "GatingControls": [
                "arn:aws:route53-recovery-control::888888888888:controlpanel/
zzz123yyy456xxx789zzz123yyy456xxx/routingcontrol/def123def123def"
            ],
            "TargetControls": [
                "arn:aws:route53-recovery-control::888888888888:controlpanel/
zzz123yyy456xxx789zzz123yyy456xxx/routingcontrol/ghi456ghi456ghi"
                "arn:aws:route53-recovery-control::888888888888:controlpanel/
zzz123yyy456xxx789zzz123yyy456xxx/routingcontrol/lmn789lmn789lmn"
            ],
            "ControlPanelArn": "arn:aws:route53-recovery-
control::888888888888:controlpanel/zzz123yyy456xxx789zzz123yyy456xxx",
            "Name": "TestGatingRule",
            "RuleConfig": {
                "Inverted": false,
                "Threshold": 0,
                "Type": "OR"
            },
            "Status": "PENDING",
            "WaitPeriodMs": 5000
        }
    }
}
```

Comme pour les autres ressources de contrôle du routage, vous pouvez décrire, répertorier ou supprimer les règles de sécurité une fois qu'elles se sont propagées au plan de données.

Après avoir défini une ou plusieurs règles de sécurité, vous pouvez continuer à interagir avec le cluster pour définir ou récupérer l'état des contrôles de routage. Si une `set-routing-control-state` opération enfreint une règle que vous avez créée, vous recevrez une exception similaire à la suivante :

```
Cannot modify control state for [0123456bbbbbbb0123456bbbbbb01234560123
abcdefg1234567] due to failed rule evaluation
0123456bbbbbbb0123456bbbbbb01234563333333444444
```

Le premier identifiant est l'ARN du panneau de commande concaténé avec l'ARN du contrôle de routage. Le deuxième identifiant est l'ARN du panneau de commande concaténé avec l'ARN de la règle de sécurité.

5. Créez des bilans de santé

Pour utiliser les contrôles de routage pour faire basculer le trafic, vous devez créer des contrôles de santé dans Amazon Route 53, puis les associer à vos enregistrements DNS. En cas de basculement du trafic, un contrôle de routage ARC Route 53 définit le contrôle de santé sur échec, de sorte que la Route 53 redirige le trafic. (Le bilan de santé ne valide pas l'état de santé de votre application ; il est simplement utilisé comme méthode pour réacheminer le trafic.)

Par exemple, supposons que vous ayez deux cellules (régions ou zones de disponibilité). Vous configurez l'une comme cellule principale de votre application, et l'autre comme cellule secondaire, vers laquelle basculer.

Pour configurer les contrôles de santé en cas de basculement, vous pouvez par exemple effectuer les opérations suivantes :

1. Utilisez la Route 53 ARC CLI pour créer un contrôle de routage pour chaque cellule.
2. Utilisez l'interface de ligne de commande Route 53 pour créer un contrôle de santé de la Route 53 ARC dans Route 53 pour chaque contrôle de routage.
3. Utilisez la CLI Route 53 pour créer deux enregistrements DNS de basculement dans Route 53 et associez un contrôle de santé à chacun d'eux.

5a. Créez un contrôle de routage pour chaque cellule.

```
aws route53-recovery-control-config --region us-west-2 create-routing-control \
        --routing-control-name RoutingControlCell1 \
        --cluster-arn arn:aws:route53-recovery-control::111122223333:cluster/5678abcd-
abcd-5678-abcd-5678abcdefgh
```

```
aws route53-recovery-control-config --region us-west-2 create-routing-control \
        --routing-control-name RoutingControlCell2 \
        --cluster-arn arn:aws:route53-recovery-control::111122223333:cluster/5678abcd-
abcd-5678-abcd-5678abcdefgh
```

5 b. Créez un bilan de santé pour chaque contrôle de routage.

> **Note**
>
> Vous créez des contrôles de santé de Route 53 ARC à l'aide de l'interface de ligne de commande Amazon Route 53.

```
aws route53 create-health-check --caller-reference RoutingControlCell1 \
        --health-check-config \
        Type=RECOVERY_CONTROL,RoutingControlArn=arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567
```

```
{
    "Location": "https://route53.amazonaws.com/2015-01-01/healthcheck/11111aaaa-bbbb-
cccc-dddd-ffffff22222",
    "HealthCheck": {
        "Id": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
        "CallerReference": "RoutingControlCell1",
        "HealthCheckConfig": {
            "Type": "RECOVERY_CONTROL",
            "Inverted": false,
            "Disabled": false,
            "RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567"
        },
        "HealthCheckVersion": 1
    }
}
```

```
aws route53 create-health-check --caller-reference RoutingControlCell2 \
    --health-check-config \
    Type=RECOVERY_CONTROL,RoutingControlArn=arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567
```

```
{
    "Location": "https://route53.amazonaws.com/2015-01-01/healthcheck/11111aaaa-bbbb-
cccc-dddd-ffffff22222",
    "HealthCheck": {
```

```
        "Id": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
        "CallerReference": "RoutingControlCell2",
        "HealthCheckConfig": {
            "Type": "RECOVERY_CONTROL",
            "Inverted": false,
            "Disabled": false,
            "RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567"
        },
        "HealthCheckVersion": 1
    }
}
```

5c. Créez deux enregistrements DNS de basculement et associez un contrôle de santé à chacun d'eux.

Vous créez des enregistrements DNS de basculement dans Route 53 à l'aide de la CLI Route 53. Pour créer les enregistrements, suivez les instructions du manuel Amazon Route 53 AWS CLI Command Reference pour la commande change-resource-record-sets. Dans les enregistrements, spécifiez la valeur DNS pour chaque cellule ainsi que la `HealthCheckID` valeur correspondante créée par Route 53 pour le contrôle de santé (voir 6b).

Pour la cellule primaire :

```
{
    "Name": "myapp.yourdomain.com",
    "Type": "CNAME",
    "SetIdentifier": "primary",
    "Failover": "PRIMARY",
    "TTL": 0,
    "ResourceRecords": [
        {
            "Value": "cell1.yourdomain.com"
        }
    ],
    "HealthCheckId": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
}
```

Pour la cellule secondaire :

```
{
```

```
    "Name": "myapp.yourdomain.com",
    "Type": "CNAME",
    "SetIdentifier": "secondary",
    "Failover": "SECONDARY",
    "TTL": 0,
    "ResourceRecords": [
        {
            "Value": "cell2.yourdomain.com"
        }
    ],
    "HealthCheckId": "yyyyyy-yyyy-yyyy-yyyy-yyyyyyyyyyyy"
}
```

Maintenant, pour passer de votre cellule principale à votre cellule secondaire, vous pouvez suivre l'exemple de la CLI à l'étape 4b pour mettre à jour l'état de `RoutingControlCell1` to `OFF` et `RoutingControlCell2` to`ON`.

Répertoriez et mettez à jour les contrôles et les états de routage à l'aide du AWS CLI

Après avoir créé les ressources de votre Amazon Route 53 Application Recovery Controller, telles que le cluster, les contrôles de routage et les panneaux de commande, vous pouvez interagir avec le cluster pour répertorier et mettre à jour les états des contrôles de routage en vue du basculement.

Pour chaque cluster que vous créez, Route 53 ARC vous fournit un ensemble de points de terminaison de cluster, un sur cinq Régions AWS. Vous devez spécifier l'un de ces points de terminaison régionaux (le Région AWS et l'URL du point de terminaison) lorsque vous appelez le cluster pour récupérer ou définir des états de contrôle de routage vers `On` ou`Off`. Lorsque vous utilisez le AWS CLI, pour obtenir ou mettre à jour des états de contrôle de routage, en plus du point de terminaison régional, vous devez également spécifier le point `--region` de terminaison régional, comme indiqué dans les exemples de cette section.

Vous pouvez utiliser n'importe quel point de terminaison du cluster régional. Nous vous recommandons d'alterner vos systèmes entre les points de terminaison régionaux et de vous préparer à réessayer avec chacun des points de terminaison disponibles. Pour des exemples de code illustrant l'essai de points de terminaison d'un cluster en séquence, consultezActions pour Application Recovery Controller à l'aide de AWS kits de développement logiciel.

Pour plus d'informations sur l'utilisation du AWS CLI, consultez la référence des AWS CLI commandes. Pour obtenir la liste des actions de l'API de contrôle du routage et des liens vers des informations supplémentaires, consultez Opérations de l'API de contrôle du routage.

> **Important**
>
> Bien que vous puissiez mettre à jour un état de contrôle de routage sur la console Amazon Route 53, nous vous recommandons de mettre à jour les états de contrôle de routage à l'aide du AWS CLI ou d'un AWS SDK. La Route 53 ARC offre une fiabilité extrême grâce au plan de données de contrôle de routage Route 53 ARC qui permet de réacheminer le trafic et de basculer entre les cellules. Pour plus de recommandations sur l'utilisation de Route 53 ARC pour le basculement, consultezMeilleures pratiques pour le contrôle du routage dans Route 53 ARC.

Lorsque vous créez un contrôle de routage, l'état est défini sur`Off`. Cela signifie que le trafic n'est pas acheminé vers la cellule cible pour ce contrôle de routage. Vous pouvez vérifier l'état du contrôle de routage en exécutant la commande`get-routing-control-state`.

Pour déterminer la région et le point de terminaison à spécifier, exécutez la `describe-clusters` commande pour afficher le`ClusterEndpoints`. Chacune `ClusterEndpoint` inclut une région et un point de terminaison correspondant que vous pouvez utiliser pour obtenir ou mettre à jour les états du contrôle de routage. DescribeClusterest une opération de l'API de configuration du contrôle de restauration. Nous vous recommandons de conserver une copie locale des points de terminaison de votre cluster régional Route 53 ARC, dans des signets ou codée en dur dans du code d'automatisation que vous utilisez pour réessayer vos points de terminaison.

1. Lister les contrôles de routage

Vous pouvez visualiser vos contrôles de routage et leurs états à l'aide des points de terminaison très fiables du plan de données ARC Route 53.

1. Répertoriez les commandes de routage pour un panneau de commande spécifique. Si vous ne spécifiez aucun panneau de configuration, `list-routing-controls` renvoie toutes les commandes de routage du cluster.

```
aws route53-recovery-cluster list-routing-controls --control-panel-arn \
        arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456 \
        --region us-west-2 \
        --endpoint-url https://host-dddddd.us-west-2.example.com/v1
```

```
{
```

```
    "RoutingControls": [{
        "ControlPanelArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456",
        "ControlPanelName": "ExampleControlPanel",
        "RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567",
        "RoutingControlName": "RCOne",
        "RoutingControlState": "On"
    },
    {
        "ControlPanelArn": "arn:aws:route53-recovery-
control::023759465626:controlpanel/0123456bbbbbbb0123456bbbbbb0123456",
        "ControlPanelName": "ExampleControlPanel",
        "RoutingControlArn": "arn:aws:route53-recovery-
control::023759465626:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
zzzzxxxxyyyy123456",
        "RoutingControlName": "RCTwo",
        "RoutingControlState": "Off"
    }
]
```

2. Bénéficiez de contrôles de routage

2. Obtenez un état de contrôle de routage.

```
aws route53-recovery-cluster get-routing-control-state --routing-control-arn \
        arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567 \
        --region us-west-2 \
        --endpoint-url https://host-dddddd.us-west-2.example.com/v1
```

```
{"RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567",
    "RoutingControlName": "RCOne",
    "RoutingControlState": "On"
}
```

2. Mettre à jour les contrôles de routage

Pour acheminer le trafic vers le point de terminaison cible contrôlé par le contrôle de routage, vous mettez à jour l'état du contrôle de routage sur0n. Mettez à jour l'état du contrôle de routage en exécutant la commandeu`pdate-routing-control-state`. (Lorsque la demande aboutit, la réponse est vide.)

2a. Mettez à jour un état de contrôle de routage.

```
aws route53-recovery-cluster update-routing-control-state \
        --routing-control-arn \
        arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567 \
        --routing-control-state On \
        --region us-west-2 \
        --endpoint-url https://host-dddddd.us-west-2.example.com/v1
```

```
{}
```

Vous pouvez mettre à jour plusieurs contrôles de routage en même temps avec un seul appel d'API :`update-routing-control-states`. (Lorsque la demande aboutit, la réponse est vide.)

2 b. Mettez à jour plusieurs états de contrôle de routage à la fois (mises à jour par lots).

```
aws route53-recovery-cluster update-routing-control-states \
        --update-routing-control-state-entries \
        '[{"RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567",
        "RoutingControlState": "Off"}, \
        {"RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
hijklmnop987654321",
        "RoutingControlState": "On"}]' \
        --region us-west-2 \
        --endpoint-url https://host-dddddd.us-west-2.example.com/v1
```

```
{}
```

Utilisation des composants de contrôle de routage dans Route 53 ARC

Rubriques

Création de composants de contrôle de routage dans Route 53 ARC

Cette section explique comment créer un cluster, des contrôles de routage, des bilans de santé et des panneaux de commande pour travailler avec le contrôle de routage dans Amazon Route 53 Application Recovery Controller.

Commencez par créer un cluster pour héberger vos commandes de routage et les panneaux de commande que vous utilisez pour les regrouper. Créez ensuite des contrôles de routage et des bilans de santé afin de pouvoir rediriger le trafic pour qu'il passe d'une cellule à l'autre, afin que le trafic soit dirigé vers votre réplique de sauvegarde, par exemple.

Notez que vous êtes facturé à l'heure pour chaque cluster que vous créez. Vous n'avez généralement besoin que d'un seul cluster pour héberger les commandes de routage et les panneaux de commande pour la gestion du contrôle de restauration d'une application. En outre, vous pouvez configurer le partage des ressources en utilisant AWS Resource Access Manager, afin qu'un cluster puisse héberger des contrôles de routage et d'autres ressources Route 53 ARC détenues par plusieurs Comptes AWS. Pour en savoir plus sur le partage de ressources dans Route 53 ARC, Support multi-comptes pour les clusters dans Route 53 ARC. Pour plus d'informations sur les tarifs, consultez les tarifs d'Amazon Route 53 Application Recovery Controller et faites défiler la page vers le bas jusqu'à Amazon Route 53.

Pour utiliser les contrôles de routage pour faire basculer le trafic, vous devez créer des contrôles de santé de contrôle de routage que vous associez aux enregistrements DNS Amazon Route 53 pour les ressources de votre application. Par exemple, supposons que vous ayez deux cellules, l'une que vous avez configurée comme cellule principale pour votre application, et l'autre comme cellule secondaire, vers laquelle vous pouvez basculer.

Pour configurer les contrôles de santé en cas de basculement, procédez comme suit :

1. Créez un contrôle de routage pour chaque cellule.

2. Créez un bilan de santé pour chaque contrôle de routage.
3. Créez deux enregistrements DNS, par exemple deux enregistrements de basculement DNS, et associez un bilan de santé à chacun d'eux.

Un autre scénario dans lequel vous pouvez créer un contrôle de routage est celui où vous créez une règle de sécurité qui est une règle de blocage. Dans ce cas, vous n'associez pas les contrôles de santé et les enregistrements DNS au contrôle de routage, car vous l'utiliserez comme contrôle de routage de blocage. Pour plus d'informations, consultez Création de règles de sécurité pour le contrôle du routage .

Les étapes de création des composants pour le contrôle du routage sur la console Route 53 ARC sont incluses dans ces sections. Pour en savoir plus sur l'utilisation des opérations de l'API de configuration du contrôle de restauration avec Route 53 ARC, consultez le Opérations de l'API de contrôle du routage.

Création d'un cluster dans Route 53 ARC

Vous devez créer un cluster pour héberger les commandes de routage et les panneaux de commande dans Route 53 ARC.

Un cluster est un ensemble de points de terminaison régionaux redondants sur lesquels vous pouvez exécuter des appels d'API pour mettre à jour ou obtenir l'état d'un ou de plusieurs contrôles de routage. Un seul cluster peut héberger plusieurs contrôles de routage.

> **Important**
>
> Sachez que vous êtes facturé à l'heure pour chaque cluster que vous créez. Un cluster peut héberger un certain nombre de commandes de routage et de panneaux de commande pour la gestion du contrôle de restauration, ce qui est généralement suffisant pour une application.

Pour créer un cluster

1. Ouvrez la console Route 53 ARC à l'adressehttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Choisissez Clusters.
3. Choisissez Create, puis entrez le nom de votre cluster.
4. Choisissez Créer un cluster.

Création d'un contrôle de routage dans Route 53 ARC

Créez un contrôle de routage pour chaque cellule vers laquelle vous souhaitez acheminer le trafic. Par exemple, lorsque vous avez une application dont les ressources sont cloisonnées à des fins de restauration, vous pouvez avoir une cellule pour chacune d'elles et des cellules imbriquées pour chaque Région AWS zone de disponibilité au sein de chaque région. Dans ce scénario, vous devez créer un contrôle de routage pour chaque cellule et chaque cellule imbriquée.

Lorsque vous créez des contrôles de routage, n'oubliez pas que les noms des contrôles de routage doivent être uniques dans chaque panneau de commande.

Après avoir créé des contrôles de routage à utiliser pour rediriger le trafic, vous associez chacun d'eux à un bilan de santé, qui vous permet d'acheminer le trafic vers des cellules, en fonction des enregistrements DNS que vous avez associés à chacune d'elles. Si vous configurez une règle de contrôle comme règle de sécurité et que vous créez un contrôle de routage de portail, vous n'ajoutez pas de contrôle de santé au contrôle de routage.

Pour créer un contrôle de routage

1. Ouvrez la console Route 53 ARC à l'adressehttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Choisissez le contrôle du routage.
3. Sur la page Contrôle de routage, choisissez Créer, puis choisissez un contrôle de routage.
4. Entrez un nom pour votre contrôle de routage, choisissez le cluster auquel ajouter le contrôle et choisissez de l'ajouter à un panneau de commande existant, notamment en utilisant le panneau de configuration par défaut. Vous pouvez également créer un nouveau panneau de commande.
5. Si vous choisissez de créer un nouveau panneau de commande, choisissez un cluster sur lequel créer le panneau de commande, puis entrez un nom pour le panneau.
6. Choisissez Créer un contrôle de routage.
7. Suivez les étapes pour nommer et créer le contrôle de routage.

Création d'un contrôle de santé du contrôle de routage dans Route 53 ARC

Vous associez une vérification de l'état du contrôle de routage à chaque contrôle de routage que vous souhaitez utiliser pour réacheminer le trafic. Vous configurez ensuite chaque contrôle de santé avec un enregistrement DNS Amazon Route 53, par exemple un enregistrement DNS de basculement. Vous pouvez ensuite rediriger le trafic dans Amazon Route 53 Application Recovery

Controller simplement en mettant à jour l'état du contrôle de routage associé, pour le définir sur `On` ou`Off`.

> **Note**
>
> Vous ne pouvez pas modifier un contrôle de santé d'un contrôle de routage existant pour l'associer à un autre contrôle de routage.

Pour créer un bilan de santé du contrôle de routage

1. Ouvrez la console Route 53 ARC à l'adressehttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Choisissez le contrôle du routage.
3. Sur la page Contrôle de routage, choisissez un contrôle de routage.
4. Sur la page détaillée du contrôle de routage, choisissez Create health check.
5. Entrez un nom pour le bilan de santé, puis choisissez Créer.

Ensuite, vous créez des enregistrements DNS Route 53 et associez vos contrôles de santé du contrôle du routage à chacun d'entre eux. Supposons, par exemple, que vous souhaitiez utiliser deux enregistrements de basculement DNS pour associer les vérifications de santé de votre contrôle de routage. Pour que Route 53 ARC fasse correctement basculer le trafic à l'aide des commandes de routage, commencez par créer les deux enregistrements de basculement dans Route 53 : un enregistrement principal et un enregistrement secondaire. Pour plus d'informations sur la configuration des enregistrements de basculement DNS, consultez la section Concepts de vérification de l'état de santé.

Lorsque vous créez l'enregistrement de basculement principal, les valeurs doivent être similaires aux suivantes :

```
Name: myapp.yourdomain.com
Type: CNAME
Set Identifier: Primary
Failover: Primary
TTL: 0
Resource Records:
Value: cell1.yourdomain.com
```

```
Health Check ID: xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
```

Les valeurs des enregistrements de basculement secondaires doivent être similaires aux suivantes :

```
Name: myapp.yourdomain.com
Type: CNAME
Set Identifier: Secondary
Failover: Secondary
TTL: 0
Resource Records:
Value: cell2.yourdomain.com
Health Check ID: xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
```

Supposons maintenant que vous souhaitiez rediriger le trafic en raison d'une panne. Pour ce faire, vous devez mettre à jour les états de contrôle de routage associés pour changer l'état de contrôle de routage principal `OFF` et l'état de contrôle de routage secondaire en`ON`. Dans ce cas, les contrôles de santé associés empêchent le trafic d'atteindre le réplica principal et l'acheminent plutôt vers le réplica secondaire. Pour plus d'informations sur le basculement du trafic à l'aide de contrôles de routage, consultez Obtenir et mettre à jour les états de contrôle du routage à l'aide de l'API Route 53 ARC (recommandé).

Pour voir des exemples de AWS CLI commandes permettant de créer des contrôles de routage et les contrôles de santé associés à l'aide des opérations de l'API Route 53 ARC, consultez Exemples d'utilisation des opérations de l'API de contrôle de routage ARC Route 53 avec AWS CLI.

Création d'un panneau de commande dans Route 53 ARC

Un panneau de configuration intégré à Amazon Route 53 Application Recovery Controller vous permet de regrouper les contrôles de routage connexes. Un panneau de commande peut comporter des contrôles de routage qui représentent un microservice au sein d'une application, une application entière ou un groupe d'applications, selon l'étendue de votre basculement. L'un des avantages du regroupement des contrôles de routage dans un panneau de commande est que vous pouvez utiliser des règles de sécurité associées à un panneau de commande pour protéger les modifications de routage du trafic.

Lorsque vous créez un cluster, Route 53 ARC crée un panneau de configuration par défaut. Vous pouvez utiliser le panneau de configuration par défaut pour vos commandes de routage, ou vous pouvez créer un ou plusieurs panneaux de commande pour regrouper vos commandes de

routage. Notez que seuls les caractères ASCII sont pris en charge pour les noms des panneaux de commande.

Les étapes de création d'un panneau de commande sur la console Route 53 ARC sont incluses dans cette section. Pour plus d'informations sur l'utilisation des opérations de l'API de configuration du contrôle de restauration avec Route 53 ARC, consultez le Opérations de l'API de contrôle du routage.

Pour créer un panneau de commande

1. Ouvrez la console Route 53 ARC à l'adressehttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Choisissez le contrôle du routage.
3. Sur la page de contrôle du routage, choisissez Créer, puis choisissez un panneau de configuration.
4. Choisissez un cluster sur lequel créer le panneau de commande, puis entrez un nom pour le panneau.
5. Choisissez Créer un panneau de configuration.

Affichage et mise à jour des états de contrôle de routage dans Route 53 ARC

Cette section explique comment afficher et mettre à jour les états du contrôle de routage dans Amazon Route 53 Application Recovery Controller. Les commandes de routage sont de simples commutateurs marche-arrêt qui gèrent le flux de trafic vers les cellules de votre groupe de restauration. Les cellules sont généralement Régions AWS, ou parfois des zones de disponibilité, qui incluent vos ressources. Lorsqu'un contrôle de routage est en état0n, le trafic circule vers la cellule contrôlée par ce contrôle de routage.

Vous regroupez les commandes de routage dans des panneaux de commande, qui sont des groupements logiques de basculement. Lorsque vous ouvrez un panneau de configuration sur la console, par exemple, vous pouvez afficher toutes les commandes de routage d'un regroupement en une seule fois, afin de voir où circule le trafic.

Vous pouvez mettre à jour un état de contrôle de routage sur la console Route 53 ARC ou à l'aide de l'API Route 53 ARC. Nous vous recommandons de mettre à jour les états du contrôle de routage à l'aide de l'API. Tout d'abord, Route 53 ARC offre une fiabilité extrême grâce à l'API intégrée au plan de données pour effectuer ces actions. C'est important lorsque vous modifiez ces états, car les changements d'état de routage se répercutent sur les cellules en redirigeant le trafic des applications. En outre, à l'aide de l'API, vous pouvez essayer de vous connecter à différents points de terminaison

du cluster en rotation, selon les besoins, si un point de terminaison du cluster auquel vous essayez de vous connecter n'est pas disponible.

Vous pouvez mettre à jour un état de contrôle de routage ou plusieurs états de contrôle de routage à la fois. Par exemple, vous pouvez définir un état de contrôle de routage pour `0ff` empêcher le trafic de circuler vers une cellule, par exemple une zone de disponibilité dans laquelle une application connaît une latence accrue. Dans le même temps, vous souhaiterez peut-être définir un autre état de contrôle de routage pour que le trafic commence 0n à circuler vers une autre cellule ou une autre zone de disponibilité. Dans ce scénario, vous pouvez mettre à jour les deux états de contrôle de routage en même temps, afin que le trafic continue de circuler.

Rubriques

Obtenir et mettre à jour les états de contrôle du routage à l'aide de l'API Route 53 ARC (recommandé)

Nous vous recommandons d'utiliser les opérations de l'API Amazon Route 53 Application Recovery Controller pour obtenir ou mettre à jour les états de contrôle du routage, à l'aide d'une AWS CLI commande ou d'un code que vous avez développé pour utiliser les opérations de l'API Route 53 ARC avec l'un des AWS SDK. Nous recommandons d'utiliser les opérations d'API, avec la CLI ou dans le code, pour travailler avec les états de contrôle du routage, plutôt que d'utiliser le AWS Management Console.

Route 53 ARC offre une fiabilité extrême pour le basculement entre les cellules (Régions AWS) en mettant à jour les états des contrôles de routage à l'aide de l'API, car les contrôles de routage sont stockés dans un cluster à haute disponibilité. Route 53 ARC garantit qu'au moins trois des cinq points de terminaison du cluster régional sont toujours accessibles pour modifier l'état du contrôle du routage. Pour obtenir ou modifier un état de contrôle de routage à l'aide de l'API, vous devez vous connecter à l'un des points de terminaison de votre cluster régional. Si le point de terminaison n'est pas disponible, vous pouvez essayer de vous connecter à un autre point de terminaison de votre cluster.

Vous pouvez consulter la liste des points de terminaison du cluster régional pour votre cluster dans la console Route 53, ou en utilisant une action d'API, DescribeCluster. Votre processus d'obtention et de modification des états de contrôle de routage doit essayer chaque point de terminaison à tour de

rôle, selon les besoins, car les points de terminaison du cluster passent par des états disponibles et indisponibles pour une maintenance et des mises à jour régulières.

Nous fournissons des informations détaillées et des exemples de code pour utiliser les opérations de l'API Route 53 ARC pour obtenir et mettre à jour les états de contrôle du routage, et pour travailler avec les points de terminaison des clusters régionaux. Pour plus d'informations, consultez les ressources suivantes :

- Pour des exemples de code expliquant comment effectuer une rotation entre les points de terminaison d'un cluster régional pour obtenir et définir des états de contrôle de routage, consultezActions pour Application Recovery Controller à l'aide de AWS kits de développement logiciel.
- Pour plus d'informations sur l'utilisation du AWS CLI pour obtenir et mettre à jour les états de contrôle de routage, consultez Répertoriez et mettez à jour les contrôles et les états de routage à l'aide du AWS CLI.

Obtenir et mettre à jour les états de contrôle de routage dans AWS Management Console

Vous pouvez obtenir et mettre à jour les états de contrôle de routage dans le AWS Management Console. Sachez toutefois que vous ne pouvez pas choisir différents points de terminaison du cluster régional dans la console. En d'autres termes, il n'existe aucun processus permettant de choisir et de faire pivoter les points de terminaison du cluster dans la console, comme vous pouvez le faire en utilisant l'API Amazon Route 53 Application Recovery Controller. De plus, la console n'est pas très disponible alors que le plan de données Route 53 ARC offre une fiabilité extrême. Pour ces raisons, nous vous recommandons d'utiliser l'API ARC Route 53 pour obtenir et mettre à jour les états de contrôle de routage pour les opérations de production.

Pour plus de recommandations sur l'utilisation de Route 53 ARC pour le basculement, consultezMeilleures pratiques pour le contrôle du routage dans Route 53 ARC.

Pour afficher et mettre à jour les contrôles de routage dans la console, suivez les étapes décrites dans les procédures suivantes.

Pour obtenir les états de contrôle du routage

1. Ouvrez la console Route 53 ARC à l'adressehttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Choisissez le contrôle du routage.

3. Dans la liste, choisissez un panneau de commande et visualisez les commandes de routage.

Pour mettre à jour un ou plusieurs états de contrôle de routage

1. Ouvrez la console Amazon Route 53 à l'adresse https://console.aws.amazon.com/route53/home.
2. Sous Application Recovery Controller, choisissez Routing control.
3. Choisissez Action, puis Modifier le routage du trafic.
4. Mettez à jour les états d'un ou de plusieurs contrôles de routage pour qu'`0ff`ils soient ou`0n`, selon l'endroit où vous souhaitez que le trafic circule ou cesse de circuler pour votre application.
5. Saisissez `confirm` dans la zone de texte.
6. Choisissez Mettre à jour le routage du trafic.

Création de règles de sécurité pour le contrôle du routage

Lorsque vous utilisez plusieurs contrôles de routage en même temps, vous pouvez décider de mettre en place des mesures de protection pour éviter des conséquences imprévues. Par exemple, vous souhaiterez peut-être éviter de désactiver par inadvertance toutes les commandes de routage d'une application, ce qui entraînerait un scénario d'ouverture défaillante. Vous pouvez également implémenter un commutateur marche-arrêt principal pour désactiver un ensemble de commandes de routage, par exemple pour empêcher l'automatisation de rediriger le trafic. Pour établir de telles garanties pour le contrôle du routage dans Route 53 ARC, vous devez créer des règles de sécurité.

Vous configurez les règles de sécurité pour le contrôle du routage à l'aide d'une combinaison de contrôles de routage, de règles et d'autres options que vous spécifiez. Chaque règle de sécurité est associée à un seul panneau de commande, mais un panneau de commande peut comporter plusieurs règles de sécurité. Lorsque vous créez des règles de sécurité, n'oubliez pas que les noms des règles de sécurité doivent être uniques dans chaque panneau de commande.

Rubriques

- Types de règles de sécurité
- Création d'une règle de sécurité sur la console
- Modification ou suppression d'une règle de sécurité sur la console
- Dérogation aux règles de sécurité pour réacheminer le trafic

Types de règles de sécurité

Il existe deux types de règles de sécurité, les règles d'assertion et les règles de blocage, que vous pouvez utiliser pour protéger le basculement de différentes manières.

Règle d'assertion

Avec une règle d'assertion, lorsque vous modifiez un ou plusieurs états de contrôle de routage, Route 53 ARC veille à ce que les critères que vous avez définis lors de la configuration de la règle soient respectés, sinon les états du contrôle de routage ne sont pas modifiés.

Cela peut être utile, par exemple, pour empêcher un scénario d'ouverture défaillante, tel qu'un scénario dans lequel vous empêchez le trafic de se diriger vers une cellule mais pas de démarrer le trafic vers une autre cellule. Pour éviter cela, une règle d'assertion garantit qu'au moins un contrôle de routage dans un ensemble de contrôles de routage d'un panneau de commande existe 0n à un moment donné. Cela garantit que le trafic circule vers au moins une région ou une zone de disponibilité pour une application.

Pour voir un exemple de AWS CLI commande qui crée une règle d'assertion pour appliquer ce critère, voir Créer des règles de sécurité dans Exemples d'utilisation des opérations de l'API de contrôle de routage ARC Route 53 avec AWS CLI.

Pour obtenir des informations détaillées sur les propriétés de fonctionnement de l'API des règles d'assertion, consultez AssertionRulele Guide de référence de l'API Routing Control pour Amazon Route 53 Application Recovery Controller.

Règle de blocage

Avec une règle de blocage, vous pouvez appliquer une commutation globale activation/désactivation sur un ensemble de contrôles de routage afin que la modification de ces états de contrôle de routage soit imposée en fonction d'un ensemble de critères que vous spécifiez dans la règle. Le critère le plus simple est de savoir si un seul contrôle de routage que vous spécifiez comme commutateur est défini sur `0N` ou`0FF`.

Pour implémenter cela, vous créez un contrôle de routage par portail, à utiliser comme commutateur global, et des contrôles de routage cibles, pour contrôler le flux de trafic vers différentes régions ou zones de disponibilité. Ensuite, pour empêcher les mises à jour manuelles ou automatisées de l'état des contrôles de routage cibles que vous avez configurés pour la règle de contrôle de routage, vous définissez l'état du contrôle de routage de portail sur. `0ff` Pour autoriser les mises à jour, vous devez le définir sur0n.

Pour voir un exemple de AWS CLI commande qui crée une règle de blocage implémentant ce type de commutateur global, voir Créer des règles de sécurité dans Exemples d'utilisation des opérations de l'API de contrôle de routage ARC Route 53 avec AWS CLI.

Pour obtenir des informations détaillées sur les propriétés de fonctionnement de l'API des règles de blocage, consultez GatingRulele Guide de référence de l'API Routing Control pour Amazon Route 53 Application Recovery Controller.

Création d'une règle de sécurité sur la console

Les étapes décrites dans cette section expliquent comment créer une règle de sécurité sur la console Route 53 ARC. Les étapes sont similaires, que vous créiez une règle d'assertion ou une règle de blocage. Les différences sont notées dans la procédure.

Pour en savoir plus sur l'utilisation des opérations d'API de restauration et de contrôle de routage avec Amazon Route 53 Application Recovery Controller, consultez Opérations de l'API de contrôle du routage.

Pour créer une règle de sécurité

1. Ouvrez la console Route 53 ARC à l'adressehttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Choisissez le contrôle du routage.
3. Sur la page de contrôle du routage, choisissez un panneau de commande.
4. Sur la page des détails du panneau de commande, choisissez Action, puis Ajouter une règle de sécurité.
5. Choisissez le type de règle à ajouter : règle d'assertion ou règle de blocage.
6. Choisissez un nom et modifiez éventuellement le délai d'attente.
7. Spécifiez les options de configuration pour la règle de sécurité.

   - Pour une règle d'assertion, spécifiez les contrôles de routage affirmés.
   - Pour une règle de routage, spécifiez le contrôle de routage de portail et les contrôles de routage cible.

   Pour les deux règles, spécifiez la configuration des règles en choisissant le type et le seuil, et indiquez si la règle est inversée.

> **Note**
>
> Pour en savoir plus sur la spécification d'une règle d'assertion, consultez les informations relatives au AssertionRulefonctionnement fournies dans le Guide de référence de l'API de contrôle de routage pour Amazon Route 53 Application Recovery Controller. Pour en savoir plus sur la spécification d'une règle de blocage, consultez les informations fournies pour l'GatingRuleopération dans le Guide de référence de l'API de contrôle de routage pour Amazon Route 53 Application Recovery Controller.

8. Choisissez Créer.

Modification ou suppression d'une règle de sécurité sur la console

Les étapes décrites dans cette section expliquent comment modifier ou supprimer une règle de sécurité sur la console Route 53 ARC. Vous ne pouvez apporter que des modifications limitées à une règle de sécurité, pour changer le nom ou mettre à jour le délai d'attente. Pour apporter d'autres modifications, supprimez et recréez la règle de sécurité.

Pour en savoir plus sur l'utilisation des opérations d'API avec Amazon Route 53 Application Recovery Controller, consultez le Opérations de l'API de contrôle du routage.

Pour supprimer une règle de sécurité

1. Ouvrez la console Route 53 ARC à l'adressehttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Choisissez le contrôle du routage.
3. Sur la page de contrôle du routage, choisissez un panneau de commande.
4. Sur la page des détails du panneau de commande, choisissez une règle de sécurité, puis choisissez Supprimer ou Modifier.

Dérogation aux règles de sécurité pour réacheminer le trafic

Il existe des scénarios dans lesquels vous souhaiterez peut-être contourner les mesures de contrôle de routage appliquées par les règles de sécurité que vous avez configurées. Par exemple, vous souhaiterez peut-être basculer rapidement pour une reprise après sinistre, et une ou plusieurs règles de sécurité peuvent vous empêcher de manière inattendue de mettre à jour un état de contrôle de routage pour rediriger le trafic. Dans un scénario de « rupture de verre » comme celui-ci, vous pouvez

contourner une ou plusieurs règles de sécurité pour modifier un état de contrôle de routage et faire basculer votre application.

Vous pouvez contourner les règles de sécurité lorsque vous mettez à jour un état de contrôle de routage (ou plusieurs états de contrôle de routage) en utilisant la `update-routing-control-states` AWS CLI commande `update-routing-control-state` ou avec le `safety-rules-to-override` paramètre. Spécifiez le paramètre avec l'Amazon Resource Name (ARN) de la règle de sécurité que vous souhaitez remplacer, ou spécifiez une liste d'ARN séparés par des virgules pour annuler au moins deux règles de sécurité.

Lorsqu'une règle de sécurité bloque une mise à jour de l'état du contrôle de routage, le message d'erreur inclut l'ARN de la règle qui a bloqué la mise à jour. Vous pouvez donc prendre note de l'ARN, puis le spécifier dans une commande CLI de l'état de contrôle du routage avec le paramètre de remplacement des règles de sécurité.

> **Note**
>
> Comme plusieurs règles de sécurité peuvent être en place pour les contrôles de routage que vous mettez à jour, vous pouvez exécuter la commande CLI pour mettre à jour l'état de votre contrôle de routage en annulant une règle de sécurité, mais obtenir un message d'erreur indiquant qu'une autre règle de sécurité bloque la mise à jour. Continuez à ajouter les ARN des règles de sécurité à la liste des règles à remplacer dans la commande de mise à jour, séparés par des virgules, jusqu'à ce que la commande de mise à jour se termine correctement.

Pour en savoir plus sur l'utilisation de la `SafetyRulesToOverride` propriété avec l'API et les SDK, consultez UpdateRoutingControlState.

Voici deux exemples de commandes CLI permettant de contourner les règles de sécurité afin de mettre à jour les états de contrôle du routage.

Ignorer une règle de sécurité

```
aws route53-recovery-cluster --region us-west-2 update-routing-control-state \
    --routing-control-arn \
    arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/
routingcontrol/abcdefg1234567 \
```

```
    --routing-control-state On \
    --safety-rules-to-override arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/safetyrule/
yyyyyyy8888888 \
    --endpoint-url https://host-dddddd.us-west-2.example.com/v1
```

Ignorer deux règles de sécurité

```
aws route53-recovery-cluster --region us-west-2 update-routing-control-state \
    --routing-control-arn \
    arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/
routingcontrol/abcdefg1234567 \
    --routing-control-state On \
    --safety-rules-to-override "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/safetyrule/
yyyyyyy8888888" \
    "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/safetyrule/
qqqqqqq7777777"
    --endpoint-url https://host-dddddd.us-west-2.example.com/v1
```

Support multi-comptes pour les clusters dans Route 53 ARC

Amazon Route 53 Application Recovery Controller s'intègre AWS Resource Access Manager pour permettre le partage des ressources. AWS RAM est un service qui vous permet de partager des ressources avec d'autres personnes Comptes AWS ou par le biais de AWS Organizations. Pour Route 53 ARC, vous pouvez partager la ressource du cluster.

Avec AWS RAM, vous partagez les ressources que vous possédez en créant un partage de ressources. Un partage de ressources indique les ressources à partager et les participants avec lesquels les partager. Les participants peuvent inclure :

- Spécifique Comptes AWS à l'intérieur ou à l'extérieur de l'organisation du propriétaire dans AWS Organizations
- 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.

En partageant AWS Resource Access Manager les ressources du cluster entre les comptes de Route 53 ARC, vous pouvez utiliser un cluster pour héberger des panneaux de contrôle et des contrôles de routage appartenant à plusieurs entités Comptes AWS. Lorsque vous choisissez de partager un cluster, les autres clusters Comptes AWS que vous spécifiez peuvent utiliser le cluster pour héberger leurs propres panneaux de contrôle et contrôles de routage, ce qui permet un contrôle et une flexibilité accrus sur les capacités de routage entre les différentes équipes.

AWS RAM est un service qui aide les AWS clients à partager des ressources en toute sécurité Comptes AWS. Avec AWS RAM, vous pouvez partager des ressources au sein d'une organisation ou d'unités organisationnelles (UO) en AWS Organizations utilisant des rôles et des utilisateurs IAM. AWS RAM est un moyen centralisé et contrôlé de partager un cluster.

Lorsque vous partagez un cluster, vous pouvez réduire le nombre total de clusters dont votre organisation a besoin. Avec un cluster partagé, vous pouvez répartir le coût total de fonctionnement du cluster entre différentes équipes, afin de maximiser les avantages de Route 53 ARC à moindre coût. (La création de ressources hébergées dans un cluster n'entraîne aucun coût supplémentaire, ni pour le propriétaire ni pour les participants.) Le partage de clusters entre comptes peut également faciliter le processus d'intégration de plusieurs applications dans Route 53 ARC, en particulier si vous avez un grand nombre d'applications réparties entre plusieurs comptes et équipes opérationnelles.

Pour commencer à utiliser le partage entre comptes dans Route 53 ARC, vous devez créer un partage de ressources dans AWS RAM. Le partage de ressources indique les participants autorisés à partager le cluster que votre compte possède. Les participants peuvent ensuite créer des ressources, telles que des panneaux de contrôle et des contrôles de routage, dans le cluster, en utilisant AWS Management Console ou en exécutant les opérations de l'API Route 53 ARC à l'aide des AWS SDK AWS Command Line Interface ou.

Cette rubrique explique comment partager les ressources que vous possédez et comment utiliser les ressources partagées avec vous.

Table des matières

- Quotas

Conditions préalables au partage de clusters

- Pour partager un cluster, vous devez en être le propriétaire dans votre Compte AWS. Cela signifie que la ressource doit être allouée ou provisionnée dans votre compte. Vous ne pouvez pas partager un cluster qui a été partagé avec vous.
- Pour partager un cluster avec votre organisation ou une unité organisationnelle AWS Organizations, vous devez activer le partage avec AWS Organizations. Pour de plus amples informations, veuillez consulter Activer le partage avec AWS Organizations dans le Guide de l'utilisateur AWS RAM .

Partage d'un cluster

Lorsque vous partagez un cluster dont vous êtes propriétaire, les participants que vous spécifiez pour partager le cluster peuvent créer et héberger leurs propres ressources ARC Route 53 dans le cluster.

Pour partager un cluster, vous devez l'ajouter à un partage de ressources. Un partage de ressources est une AWS RAM ressource qui vous permet de partager vos ressources entre elles Comptes AWS. Un partage de ressources indique les ressources à partager et les participants avec lesquels elles sont partagées. Pour partager un cluster, vous pouvez créer un nouveau partage de ressources ou ajouter la ressource à un partage de ressources existant. Pour créer un nouveau partage de ressources, vous pouvez utiliser la AWS RAM console ou utiliser des opérations d' AWS RAM API avec le AWS Command Line Interface ou AWS les SDK.

Si vous faites partie d'une organisation AWS Organizations et que le partage au sein de votre organisation est activé, les participants de votre organisation ont automatiquement accès au cluster partagé. Dans le cas contraire, les participants reçoivent une invitation à rejoindre le partage de ressources et ont accès au cluster partagé après avoir accepté l'invitation.

Vous pouvez partager un cluster dont vous êtes propriétaire à l'aide de la AWS RAM console ou en utilisant des opérations d' AWS RAM API avec les SDK AWS CLI ou.

Pour partager un cluster dont vous êtes propriétaire à l'aide de la AWS RAM console

Voir Création d'un partage de ressources dans le guide de AWS RAM l'utilisateur.

Pour partager un cluster dont vous êtes propriétaire à l'aide du AWS CLI

Utilisez la commande create-resource-share.

Annulation du partage d'un cluster partagé

Lorsque vous annulez le partage d'un cluster, les règles suivantes s'appliquent aux participants et aux propriétaires :

- Les ressources actuelles des participants continuent d'exister dans le cluster non partagé.
- Les participants peuvent continuer à mettre à jour les états de contrôle du routage dans le cluster non partagé, afin de gérer le routage en cas de basculement des applications.
- Les participants ne peuvent plus créer de nouvelles ressources dans le cluster non partagé.
- Si les participants disposent toujours de ressources dans un cluster non partagé, le propriétaire ne peut pas supprimer le cluster partagé.

Pour annuler le partage d'un cluster partagé dont vous êtes le propriétaire, supprimez-le du partage de ressources. Vous pouvez le faire en utilisant la AWS RAM console ou en utilisant des opérations AWS RAM d'API avec les SDK AWS CLI ou.

Pour annuler le partage d'un cluster partagé dont vous êtes propriétaire à l'aide de la console AWS RAM

Consultez la section Mise à jour d'un partage de ressources du Guide de l'utilisateur AWS RAM .

Pour annuler le partage d'un cluster partagé dont vous êtes propriétaire à l'aide du AWS CLI

Utilisez la commande disassociate-resource-share.

Identification d'un cluster partagé

Les propriétaires et les participants peuvent identifier les clusters partagés en consultant les informations dans AWS RAM. Ils peuvent également obtenir des informations sur les ressources partagées à l'aide de la console Route 53 ARC et AWS CLI.

En général, pour en savoir plus sur les ressources que vous avez partagées ou qui ont été partagées avec vous, consultez les informations du guide de l' AWS Resource Access Manager utilisateur :

- En tant que propriétaire, vous pouvez consulter toutes les ressources que vous partagez avec d'autres personnes en utilisant AWS RAM. Pour plus d'informations, consultez la section Affichage de vos ressources partagées dans AWS RAM.
- En tant que participant, vous pouvez consulter toutes les ressources partagées avec vous en utilisant AWS RAM. Pour plus d'informations, consultez la section Affichage de vos ressources partagées dans AWS RAM.

En tant que propriétaire, vous pouvez déterminer si vous partagez un cluster en consultant les informations dans AWS Management Console ou en utilisant les opérations AWS Command Line Interface de l'API ARC Route 53.

Pour déterminer si un cluster dont vous êtes propriétaire est partagé à l'aide de la console

Sur la AWS Management Console page de détails d'un cluster, consultez l'état du partage du cluster.

Pour déterminer si un cluster dont vous êtes propriétaire est partagé à l'aide du AWS CLI

Utilisez la commande get-resource-policy. S'il existe une politique de ressources pour un cluster, la commande renvoie des informations sur cette stratégie.

En tant que participant, lorsqu'un cluster est partagé avec vous, vous devez généralement accepter le partage. En outre, le champ Propriétaire du cluster contient le compte du propriétaire du cluster.

Responsabilités et autorisations pour les clusters partagés

Autorisations accordées aux propriétaires

Lorsque vous partagez un cluster dont vous êtes propriétaire avec d'autres personnes Comptes AWS, les participants autorisés à l'utiliser peuvent créer des panneaux de commande, des contrôles de routage et d'autres ressources dans le cluster.

En tant que propriétaire de clusters, vous êtes responsable de la création, de la gestion et de la suppression des clusters. Vous ne pouvez pas modifier ou supprimer les ressources créées par les participants, telles que les contrôles de routage et les règles de sécurité. Par exemple, vous ne pouvez pas mettre à jour un contrôle de routage créé par un participant pour modifier l'état du contrôle de routage.

Toutefois, vous pouvez consulter les détails des contrôles de routage créés par les participants d'un cluster dont vous êtes le propriétaire. Par exemple, vous pouvez afficher les états du contrôle de routage en appelant une opération de l'API de contrôle de routage Route 53 ARC, à l'aide AWS des SDK AWS Command Line Interface ou.

Si vous devez modifier les ressources créées par les participants, ils peuvent configurer un rôle dans IAM avec l'autorisation d'accéder aux ressources et ajouter votre compte à ce rôle.

Autorisations pour les participants

En général, les participants peuvent créer et utiliser des panneaux de contrôle, des contrôles de routage, des règles de sécurité et des bilans de santé qu'ils créent dans un cluster partagé avec eux.

Ils ne peuvent afficher, modifier ou supprimer les ressources du cluster dans le cluster partagé que s'ils en sont propriétaires. Par exemple, les participants peuvent créer et supprimer des règles de sécurité pour les panneaux de commande qu'ils ont créés.

Les restrictions suivantes s'appliquent aux participants :

- Les participants ne peuvent pas afficher, modifier ou supprimer les panneaux de configuration créés par d'autres comptes à l'aide d'un cluster partagé.
- Les participants ne peuvent pas afficher, créer ou modifier les contrôles de routage, y compris les états des contrôles de routage, pour les ressources créées dans un cluster partagé par d'autres comptes.
- Les participants ne peuvent pas créer, modifier ou consulter les règles de sécurité créées par d'autres comptes dans un cluster partagé.
- Les participants ne peuvent pas ajouter de ressources dans le panneau de configuration par défaut d'un cluster partagé car celui-ci appartient au propriétaire du cluster.

Comme indiqué, les participants ne peuvent pas créer de contrôles de routage dans le panneau de configuration par défaut pour un cluster partagé, car le propriétaire du cluster possède le panneau de configuration par défaut. Toutefois, le propriétaire du cluster peut créer un rôle IAM entre comptes qui autorise l'accès au panneau de configuration par défaut du cluster. Le propriétaire peut ensuite accorder à un participant l'autorisation d'assumer le rôle, afin que le participant puisse accéder au panneau de configuration par défaut pour l'utiliser comme le propriétaire l'a spécifié dans les autorisations du rôle.

Coûts de facturation

Le propriétaire d'un cluster dans Route 53 ARC est facturé pour les coûts associés au cluster. Il n'y a aucun coût supplémentaire, pour les propriétaires de clusters ou pour les participants, pour créer des ressources hébergées dans un cluster.

Pour obtenir des informations détaillées sur les tarifs et des exemples, consultez la tarification d'Amazon Route 53 Application Recovery Controller et faites défiler la page vers le bas jusqu'à Amazon Route 53 Application Recovery Controller.

Quotas

Toutes les ressources créées dans un cluster partagé, y compris les ressources créées par tous les participants ayant accès au cluster partagé, sont prises en compte dans les quotas en vigueur pour le cluster et les autres ressources, telles que les contrôles de routage. Si les comptes qui partagent

les ressources du cluster ont un quota supérieur à celui du propriétaire du cluster, les quotas du propriétaire du cluster ont priorité sur les quotas des comptes qui partagent.

Pour mieux comprendre comment cela fonctionne, consultez les exemples suivants. Pour illustrer le fonctionnement des quotas avec le partage de ressources, supposons, dans ces exemples, que le propriétaire du cluster soit propriétaire et qu'un compte avec lequel le cluster a été partagé soit participant.

Quota de panneaux de commande

Des quotas sont appliqués pour le nombre total de panneaux de contrôle du propriétaire par cluster.

Par exemple, supposons que le propriétaire dispose d'un quota de 50 pour le nombre de panneaux de commande par cluster et dispose de 13 panneaux de commande dans le cluster. Supposons maintenant que le quota du participant soit fixé à 150. Dans ce scénario, le participant ne peut créer que 37 panneaux de commande (soit 50 à 13) dans le cluster partagé.

En outre, si d'autres comptes partageant le cluster créent également des panneaux de contrôle, ceux-ci sont également pris en compte dans le quota global de 50 panneaux de contrôle du cluster.

Quotas de contrôle du routage

Les contrôles de routage ont plusieurs quotas : un quota par panneau de configuration, un quota par cluster et un quota par règle de sécurité. Les quotas du propriétaire ont priorité pour tous ces quotas.

Par exemple, supposons que le propriétaire dispose d'un quota de 300 contrôles de routage par cluster et qu'il dispose déjà de 300 contrôles de routage dans le cluster. Supposons maintenant que le quota du participant soit fixé à 500. Dans ce scénario, le participant ne peut pas créer de nouveaux contrôles de routage dans le cluster partagé.

Règles de sécurité et quotas

Les quotas sont appliqués pour les règles de sécurité du propriétaire par quota du panneau de commande.

Par exemple, supposons que le propriétaire dispose d'un quota de 20 règles de sécurité par panneau de commande et que le participant ait ce quota fixé à 80. Dans ce scénario, étant donné que la limite inférieure du propriétaire est prioritaire, le participant ne peut créer que 20 règles de sécurité dans un panneau de commande du cluster partagé.

Pour obtenir la liste des quotas de contrôle de routage, consultezQuotas pour le contrôle du routage.

Journalisation et surveillance pour le contrôle du routage dans Amazon Route 53 Application Recovery Controller

Vous pouvez l'utiliser AWS CloudTrail pour surveiller le contrôle du routage dans Amazon Route 53 Application Recovery Controller, afin d'analyser les modèles et de résoudre les problèmes.

Rubriques

- Journalisation des appels de l'API ARC Route 53 à l'aide de AWS CloudTrail

Journalisation des appels de l'API ARC Route 53 à l'aide de AWS CloudTrail

Amazon Route 53 Application Recovery Controller 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 ARC. CloudTrail capture tous les appels d'API pour Route 53 ARC sous forme d'événements. Les appels capturés incluent des appels provenant de la console Route 53 ARC et des appels de code vers les opérations de l'API Route 53 ARC.

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 ARC. 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 ARC, 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.

Pour en savoir plus CloudTrail, consultez le guide de AWS CloudTrail l'utilisateur.

Informations sur la Route 53 ARC dans CloudTrail

CloudTrail est activé sur votre compte Compte AWS lorsque vous créez le compte. Lorsqu'une activité se produit sur Route 53 ARC, 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 Compte AWS. Pour plus d'informations, consultez la section Utilisation de l'historique des CloudTrail événements.

Pour un enregistrement continu des événements de votre région Compte AWS, y compris ceux de la Route 53 ARC, 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 Régions AWS. 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 les ressources suivantes :

- Présentation de la création d'un journal de suivi
- 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 de Route 53 ARC sont enregistrées CloudTrail et documentées dans le Guide de référence de l'API Recovery Readiness pour Amazon Route 53 Application Recovery Controller, le Guide de référence de l'API de configuration de Recovery Control pour Amazon Route 53 Application Recovery Controller et le Guide de référence de l'API de contrôle du routage pour Amazon Route 53 Application Recovery Controller. Par exemple, les appels au`CreateCluster`, `UpdateRoutingControlState` et les `CreateRecoveryGroup` 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 faite avec les informations d'identification de l'utilisateur root ou AWS Identity and Access Management (IAM).
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la demande a été faite par un autre AWS service.

Pour plus d'informations, consultez l'élément CloudTrail UserIdentity.

Afficher les événements de la Route 53 ARC dans l'historique des événements

CloudTrail vous permet de consulter les événements récents dans l'historique des événements. Pour afficher les événements relatifs aux demandes d'API ARC Route 53, vous devez sélectionner US West (Oregon) dans le sélecteur de région en haut de la console. Pour plus d'informations, consultez

la section Utilisation de l'historique des CloudTrail événements dans le guide de AWS CloudTrail l'utilisateur.

Comprendre les entrées du fichier journal ARC 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'exemple suivant montre une entrée de CloudTrail journal qui illustre l'`CreateCluster`action de configuration du contrôle de routage.


```
{
  "eventVersion": "1.08",
   "userIdentity": {
     "type": "IAMUser",
     "principalId": "A1B2C3D4E5F6G7EXAMPLE",
     "arn": "arn:aws:iam::111122223333:user/smithj",
     "accountId": "111122223333",
     "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
     "sessionContext": {
          "sessionIssuer": {
              "type": "Role",
              "principalId": "A1B2C3D4E5F6G7EXAMPLE",
              "arn": "arn:aws:iam::111122223333:role/smithj",
              "accountId": "111122223333",
              "userName": "smithj"
          },
          "webIdFederationData": {},
          "attributes": {
              "mfaAuthenticated": "false",
              "creationDate": "2021-06-30T04:44:41Z"
          }
      }
  },
  "eventTime": "2021-06-30T04:45:46Z",
  "eventSource": "route53-recovery-control-config.amazonaws.com",
  "eventName": "CreateCluster",
```

```
  "awsRegion": "us-west-2",
  "sourceIPAddress": "192.0.2.50",
  "userAgent": "aws-cli/2.0.0 Python/3.8.2 Darwin/19.6.0 botocore/2.0.0dev7",
  "requestParameters": {
      "ClientToken": "12345abcdef-1234-5678-abcd-12345abcdef",
      "ClusterName": "XYZCluster"
  },
  "responseElements": {
      "Cluster": {
          "Arn": "arn:aws:route53-recovery-control::012345678901:cluster/abc123456-
aa11-bb22-cc33-abc123456",
          "ClusterArn": "arn:aws:route53-recovery-control::012345678901:cluster/
abc123456-aa11-bb22-cc33-abc123456",
          "Name": "XYZCluster",
          "Status": "PENDING"
      }
  },
  "requestID": "6090509a-5a97-4be6-8e6a-7d73example",
  "eventID": "9cab44ef-0777-41e6-838f-f249example",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "111122223333"
}
```


L'exemple suivant montre une entrée de CloudTrail journal illustrant l'`UpdateRoutingControlState`action à effectuer pour le contrôle du routage.


```
{
  "eventVersion": "1.08",
   "userIdentity": {
     "type": "AssumedRole",
     "principalId": "A1B2C3D4E5F6G7EXAMPLE",
     "arn": "arn:aws:sts::111122223333:assumed-role/admin/smithj",
     "accountId": "111122223333",
     "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
     "sessionContext": {
          "sessionIssuer": {
              "type": "Role",
              "principalId": "A1B2C3D4E5F6G7EXAMPLE",
              "arn": "arn:aws:iam::111122223333:role/admin",
              "accountId": "111122223333",
```

```
            "userName": "admin"
        },
        "webIdFederationData": {},
        "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2021-06-30T04:44:41Z"
        }
    }
  },
  "eventTime": "2021-06-30T04:45:46Z",
  "eventSource": "route53-recovery-control-config.amazonaws.com",
  "eventName": "UpdateRoutingControl",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "192.0.2.50",
  "userAgent": "aws-cli/2.0.0 Python/3.8.2 Darwin/19.6.0 botocore/2.0.0dev7",
  "requestParameters": {
      "RoutingControlName": "XYZRoutingControl3",
      "RoutingControlArn": "arn:aws:route53-recovery-
control::012345678:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567"
  },
  "responseElements": {
      "RoutingControl": {
          "ControlPanelArn": "arn:aws:route53-recovery-
control::012345678:controlpanel/0123456bbbbbbb0123456bbbbbb0123456",
          "Name": "XYZRoutingControl3",
          "Status": "DEPLOYED",
          "RoutingControlArn": "arn:aws:route53-recovery-
control::012345678:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567"
      }
  },
  "requestID": "6090509a-5a97-4be6-8e6a-7d73example",
  "eventID": "9cab44ef-0777-41e6-838f-f249example",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "111122223333"
}
```

Identity and Access Management pour le contrôle du routage

AWS Identity and Access Management (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les ressources ARC de la Route 53. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Table des matières

Comment fonctionne le contrôle du routage dans Amazon Route 53 Application Recovery Controller avec IAM

Avant d'utiliser IAM pour gérer l'accès au contrôle du routage dans Amazon Route 53 Application Recovery Controller, découvrez quelles fonctionnalités IAM sont disponibles pour le contrôle du routage.

Fonctionnalités IAM que vous pouvez utiliser avec le contrôle du routage dans Amazon Route 53 Application Recovery Controller

Fonction IAM	Support pour le contrôle du routage
Politiques basées sur l’identité	Oui
Politiques basées sur les ressources	Non
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition d’une politique	Oui
ACL	Non

Fonction IAM	Support pour le contrôle du routage
ABAC (identifications dans les politiques)	Partielle
Informations d'identification temporaires	Oui
Autorisations de principal	Oui
Fonctions du service	Non
Rôles liés à un service	Non

Pour obtenir une vue globale de haut niveau du fonctionnement des AWS services avec la plupart des fonctionnalités IAM, consultez la section AWS Services compatibles avec IAM dans le Guide de l'utilisateur IAM.

Politiques basées sur l'identité pour Route 53 ARC

Prend en charge les politiques basées sur l'identité	Oui

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Création de politiques IAM dans le Guide de l'utilisateur IAM.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Vous ne pouvez pas spécifier le principal dans une politique basée sur une identité car celle-ci s'applique à l'utilisateur ou au rôle auquel elle est attachée. Pour découvrir tous les éléments que vous utilisez dans une politique JSON, consultez Références des éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

Pour consulter des exemples de politiques basées sur l'identité de Route 53 ARC pour le contrôle du routage, consultez. Exemples de politiques basées sur l'identité pour le contrôle du routage dans Amazon Route 53 Application Recovery Controller

Politiques basées sur les ressources dans le cadre du contrôle du routage

Prend en charge les politiques basées sur les ressources	Non

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique.

Actions politiques pour le contrôle du routage

Prend en charge les actions de politique	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Les actions de stratégie portent généralement le même nom que l'opération AWS d'API associée. Il existe quelques exceptions, telles que les actions avec autorisations uniquement qui n'ont pas d'opération API correspondante. Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une stratégie afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour consulter la liste des actions ARC de Route 53 pour le contrôle du routage, consultez les sections Actions définies par Amazon Route 53 Recovery Controls et Actions définies par le cluster de restauration Amazon Route 53 dans le Service Authorization Reference.

Les actions de politique dans Route 53 ARC pour le contrôle du routage utilisent les préfixes suivants avant l'action, en fonction de l'API avec laquelle vous travaillez :

```
route53-recovery-control-config
```

```
route53-recovery-cluster
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules. Par exemple, vous pouvez effectuer les opérations suivantes :

```
"Action": [
      "route53-recovery-control-config:action1",
      "route53-recovery-control-config:action2"
         ]
```

Vous pouvez aussi spécifier plusieurs actions à l'aide de caractères génériques (*). Par exemple, pour spécifier toutes les actions qui commencent par le mot `Describe`, incluez l'action suivante :

```
"Action": "route53-recovery-control-config:Describe*"
```

Pour consulter des exemples de politiques basées sur l'identité de Route 53 ARC pour le contrôle du routage, consultez. Exemples de politiques basées sur l'identité pour le contrôle du routage dans Amazon Route 53 Application Recovery Controller

Ressources politiques pour la Route 53 ARC

Prend en charge les ressources de politique	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

```
"Resource": "*"
```

Dans la référence d'autorisation de service, vous pouvez voir les informations suivantes relatives à Route 53 ARC :

Pour consulter la liste des types de ressources et de leurs ARN, ainsi que les actions que vous pouvez spécifier avec l'ARN de chaque ressource, consultez les rubriques suivantes dans la référence d'autorisation de service :

- Actions définies par Amazon Route 53 Recovery Controls
- Actions définies par Amazon Route 53 Recovery Cluster.

Pour consulter des exemples de politiques basées sur l'identité de Route 53 ARC pour le contrôle du routage, consultez. Exemples de politiques basées sur l'identité pour le contrôle du routage dans Amazon Route 53 Application Recovery Controller

Clés de conditions de politique pour Route 53 ARC

Prend en charge les clés de condition de politique spécifiques au service	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` (ou le bloc `Condition`) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément `Condition` est facultatif. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande.

Si vous spécifiez plusieurs éléments `Condition` dans une instruction, ou plusieurs clés dans un seul élément `Condition`, AWS les évalue à l'aide d'une opération `AND` logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une `OR` opération logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez accorder à un utilisateur IAM l'autorisation d'accéder à une ressource uniquement si elle est balisée avec son nom d'utilisateur IAM. Pour plus d'informations, consultez Éléments d'une politique IAM : variables et identifications dans le Guide de l'utilisateur IAM.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques au service. Pour voir toutes les clés de condition AWS globales, voir les clés de contexte de condition AWS globales dans le guide de l'utilisateur IAM.

Pour consulter la liste des clés de condition ARC de Route 53 pour le contrôle du routage, consultez les rubriques suivantes dans la référence d'autorisation de service :

- Clés de condition pour Amazon Route 53 Recovery Controls
- Clés de condition pour le cluster de restauration Amazon Route 53

Pour connaître les actions et les ressources que vous pouvez utiliser avec une clé de condition, consultez les rubriques suivantes dans la référence d'autorisation de service :

- Pour consulter la liste des types de ressources et de leurs ARN, consultez les sections Actions définies par Amazon Route 53 Recovery Controls et Actions définies par Amazon Route 53 Recovery Cluster.
- Pour consulter la liste des actions que vous pouvez spécifier avec l'ARN de chaque ressource, consultez les sections Ressources définies par Amazon Route 53 Recovery Controls et Ressources définies par Amazon Route 53 Recovery Cluster.

Pour voir des exemples de politiques basées sur l'identité de Route 53 ARC pour le contrôle du routage, voir Exemples de politiques basées sur l'identité pour le contrôle du routage dans Amazon Route 53 Application Recovery Controller

Listes de contrôle d'accès (ACL) dans Route 53 ARC

Prend en charge les listes ACL	Non

Les listes de contrôle d’accès (ACL) vérifient quels principaux (membres de compte, utilisateurs ou rôles) ont l’autorisation d’accéder à une ressource. Les listes de contrôle d’accès sont similaires aux politiques basées sur les ressources, bien qu’elles n’utilisent pas le format de document de politique JSON.

Contrôle d'accès basé sur les attributs (ABAC) avec Route 53 ARC

Prise en charge d’ABAC (identifications dans les politiques)	Partielle

Le contrôle d’accès basé sur les attributs (ABAC) est une politique d’autorisation qui définit des autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et à de nombreuses AWS ressources. L’étiquetage des entités et des ressources est la première étape d’ABAC. Vous concevez ensuite des politiques ABAC pour autoriser des opérations quand l’identification du principal correspond à celle de la ressource à laquelle il tente d’accéder.

L’ABAC est utile dans les environnements qui connaissent une croissance rapide et pour les cas où la gestion des politiques devient fastidieuse.

Pour contrôler l’accès basé sur des étiquettes, vous devez fournir les informations d’étiquette dans l’élément de condition d’une politique utilisant les clés de condition `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d’informations sur l’ABAC, consultez Qu’est-ce que le contrôle d’accès basé sur les attributs (ABAC) ? dans le Guide de l’utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration de l’ABAC, consultez Utilisation du contrôle d’accès par attributs (ABAC) dans le Guide de l’utilisateur IAM.

Le contrôle de routage ARC Route 53 inclut la prise en charge suivante pour ABAC :

- Recovery Control Config est compatible avec ABAC.
- Recovery Cluster ne prend pas en charge l'ABAC.

Utilisation d'informations d'identification temporaires avec Route 53 ARC

Prend en charge les informations d’identification temporaires	Oui

Certains Services AWS ne fonctionnent pas lorsque vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, y compris celles qui Services AWS fonctionnent avec des informations d'identification temporaires, consultez Services AWS la section relative à l'utilisation d'IAM dans le guide de l'utilisateur d'IAM.

Vous utilisez des informations d'identification temporaires si vous vous connectez à l' AWS Management Console aide d'une méthode autre qu'un nom d'utilisateur et un mot de passe. Par exemple, lorsque vous accédez à AWS l'aide du lien d'authentification unique (SSO) de votre entreprise, ce processus crée automatiquement des informations d'identification temporaires. Vous créez également automatiquement des informations d'identification temporaires lorsque vous vous connectez à la console en tant qu'utilisateur, puis changez de rôle. Pour plus d'informations sur le changement de rôle, consultez Changement de rôle (console) dans le Guide de l'utilisateur IAM.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide de l' AWS API AWS CLI or. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour y accéder AWS. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez Informations d'identification de sécurité temporaires dans IAM.

Autorisations principales interservices pour Route 53 ARC

Prend en charge les sessions d'accès direct (FAS)	Oui

Lorsque vous utilisez une entité IAM (utilisateur ou rôle) pour effectuer des actions AWS, vous êtes considéré comme un mandant. Les politiques accordent des autorisations au principal. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui déclenche une autre action dans un autre service. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions.

Pour savoir si une action nécessite des actions dépendantes supplémentaires dans une politique, consultez les rubriques suivantes dans la référence d'autorisation de service :

- Cluster de restauration Amazon Route 53
- Contrôles de restauration Amazon Route 53

Rôles de service pour Route 53 ARC

Prend en charge les fonctions de service	Non

Une fonction du service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du 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.

Rôles liés à un service pour Route 53 ARC

Prend en charge les rôles liés à un service.	Oui

Un rôle lié à un service est un type de rôle lié à un AWS service. Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés au service apparaissent dans votre AWS compte et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Le contrôle du routage n'utilise pas de rôles liés à un service.

Exemples de politiques basées sur l'identité pour le contrôle du routage dans Amazon Route 53 Application Recovery Controller

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier les ressources ARC de la Route 53. Ils ne peuvent pas non plus effectuer de tâches à l'aide de l'API AWS Management Console, AWS Command Line Interface (AWS CLI) ou de AWS l'API. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Pour apprendre à créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, consultez Création de politiques dans l'onglet JSON dans le Guide de l'utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par Route 53 ARC, y compris le format des ARN pour chacun des types de ressources, consultez la section Actions, ressources

et clés de condition pour Amazon Route 53 Application Recovery Controller dans le Service Authorization Reference.

Rubriques

- Bonnes pratiques en matière de politiques
- Exemple : accès à la console Route 53 ARC pour le contrôle du routage
- Exemples : actions de l'API ARC Route 53 pour la configuration du contrôle du routage

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer des ressources Route 53 ARC dans votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez politiques gérées par AWS ou politiques gérées par AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.
- Accorder les autorisations de moindre privilège : lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l'exécution d'une seule tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation de IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utiliser des conditions dans les politiques IAM pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que AWS CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

- Utilisez IAM Access Analyzer pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : IAM Access Analyzer valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez Validation de politique IAM Access Analyzer dans le Guide de l'utilisateur IAM.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue. Compte AWS Pour exiger le MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Configuration de l'accès aux API protégé par MFA dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

Exemple : accès à la console Route 53 ARC pour le contrôle du routage

Pour accéder à la console Amazon Route 53 Application Recovery Controller, vous devez disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et d'afficher les détails des ressources ARC de la Route 53 présentes dans votre Compte AWS. Si vous créez une stratégie basée sur l'identité qui est plus restrictive que l'ensemble minimum d'autorisations requis, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs ou rôles) tributaires de cette stratégie.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement l'API AWS CLI ou l' AWS API. Autorisez plutôt l'accès à uniquement aux actions qui correspondent à l'opération d'API qu'ils tentent d'effectuer.

Pour garantir que les utilisateurs et les rôles peuvent toujours utiliser la console Route 53 ARC lorsque vous n'autorisez l'accès qu'à des opérations d'API spécifiques, associez également une politique `ReadOnly` AWS gérée pour Route 53 ARC aux entités. Pour plus d'informations, consultez la page des politiques gérées par Route 53 ARC Route 53 ARC ou Ajouter des autorisations à un utilisateur dans le guide de l'utilisateur IAM.

Pour donner aux utilisateurs un accès complet à l'utilisation des fonctionnalités de contrôle de routage de Route 53 ARC via la console, associez une politique telle que la suivante à l'utilisateur,

afin de lui donner les autorisations complètes nécessaires pour configurer les ressources et les opérations de contrôle de routage de Route 53 ARC :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                   "route53-recovery-cluster:GetRoutingControlState",
                   "route53-recovery-cluster:UpdateRoutingControlState",
                   "route53-recovery-cluster:UpdateRoutingControlStates",
                   "route53-recovery-control-config:CreateCluster",
                   "route53-recovery-control-config:CreateControlPanel",
                   "route53-recovery-control-config:CreateRoutingControl",
                   "route53-recovery-control-config:CreateSafetyRule",
                   "route53-recovery-control-config:DeleteCluster",
                   "route53-recovery-control-config:DeleteControlPanel",
                   "route53-recovery-control-config:DeleteRoutingControl",
                   "route53-recovery-control-config:DeleteSafetyRule",
                   "route53-recovery-control-config:DescribeCluster",
                   "route53-recovery-control-config:DescribeControlPanel",
                   "route53-recovery-control-config:DescribeSafetyRule",
                   "route53-recovery-control-config:DescribeRoutingControl",
                   "route53-recovery-control-config:ListAssociatedRoute53HealthChecks",
                   "route53-recovery-control-config:ListClusters",
                   "route53-recovery-control-config:ListControlPanels",
                   "route53-recovery-control-config:ListRoutingControls",
                   "route53-recovery-control-config:ListSafetyRules",
                   "route53-recovery-control-config:UpdateControlPanel",
                   "route53-recovery-control-config:UpdateRoutingControl",
                   "route53-recovery-control-config:UpdateSafetyRule"
             ],
            "Resource": "*"
        },
                {
            "Effect": "Allow",
            "Action": [
                   "route53:GetHealthCheck",
                   "route53:CreateHealthCheck",
                   "route53:DeleteHealthCheck",
                   "route53:ChangeTagsForResource"
            ],
```

```
            "Resource": "*"
        }
    ]
}
```

Exemples : actions de l'API ARC Route 53 pour la configuration du contrôle du routage

Pour garantir qu'un utilisateur peut utiliser les actions de l'API Route 53 ARC pour travailler avec la configuration du contrôle de routage Route 53 ARC, associez une politique correspondant aux opérations d'API avec lesquelles l'utilisateur doit travailler, comme décrit ci-dessous.

Pour utiliser les opérations d'API pour la configuration du contrôle de restauration, associez une politique telle que la suivante à l'utilisateur :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                   "route53-recovery-control-config:CreateCluster",
                   "route53-recovery-control-config:CreateControlPanel",
                   "route53-recovery-control-config:CreateRoutingControl",
                   "route53-recovery-control-config:CreateSafetyRule",
                   "route53-recovery-control-config:DeleteCluster",
                   "route53-recovery-control-config:DeleteControlPanel",
                   "route53-recovery-control-config:DeleteRoutingControl",
                   "route53-recovery-control-config:DeleteSafetyRule",
                   "route53-recovery-control-config:DescribeCluster",
                   "route53-recovery-control-config:DescribeControlPanel",
                   "route53-recovery-control-config:DescribeSafetyRule",
                   "route53-recovery-control-config:DescribeRoutingControl",
                   "route53-recovery-control-config:GetResourcePolicy",
                   "route53-recovery-control-config:ListAssociatedRoute53HealthChecks",
                   "route53-recovery-control-config:ListClusters",
                   "route53-recovery-control-config:ListControlPanels",
                   "route53-recovery-control-config:ListRoutingControls",
                   "route53-recovery-control-config:ListSafetyRules",
                   "route53-recovery-control-config:ListTagsForResource",
                   "route53-recovery-control-config:UpdateControlPanel",
                   "route53-recovery-control-config:UpdateRoutingControl",
                   "route53-recovery-control-config:UpdateSafetyRule",
                   "route53-recovery-control-config:TagResource",
```

```
                    "route53-recovery-control-config:UntagResource"
            ],
            "Resource": "*"
        }
    ]
}
```

Pour effectuer des tâches dans le cadre du contrôle de routage ARC Route 53 à l'aide de l'API du plan de données du cluster de restauration, par exemple, mettre à jour les états du contrôle de routage afin de basculer en cas de sinistre, vous pouvez associer une politique IAM de Route 53 ARC telle que la suivante à votre utilisateur IAM.

Le `AllowSafetyRuleOverride` booléen autorise le remplacement des règles de sécurité que vous avez configurées pour protéger les contrôles de routage. Cette autorisation peut être requise dans les scénarios de « bris de verre » afin de contourner les mesures de protection en cas de catastrophe ou dans d'autres scénarios de basculement urgents. Par exemple, un opérateur peut avoir besoin de basculer rapidement en cas de reprise après sinistre, et une ou plusieurs règles de sécurité peuvent empêcher de manière inattendue la mise à jour de l'état du contrôle de routage requise pour rediriger le trafic. Cette autorisation permet à l'opérateur de spécifier les règles de sécurité à contourner lors des appels d'API pour mettre à jour les états du contrôle de routage. Pour plus d'informations, consultez Dérogation aux règles de sécurité pour réacheminer le trafic.

Si vous souhaitez autoriser un opérateur à utiliser l'API du plan de données du cluster de restauration tout en évitant de contourner les règles de sécurité, vous pouvez associer une politique telle que la suivante, avec un `AllowSafetyRuleOverrides` booléen à. `false` Pour permettre à l'opérateur de contourner les règles de sécurité, définissez le `AllowSafetyRuleOverrides` booléen sur. `true`

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53-recovery-cluster:GetRoutingControlState",
                "route53-recovery-cluster:ListRoutingControls"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
```

```
                "route53-recovery-cluster:UpdateRoutingControlStates",
                "route53-recovery-cluster:UpdateRoutingControlState"
            ],
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "route53-recovery-cluster:AllowSafetyRulesOverrides": "false"
                }
            }
        }
    ]
}
```

AWS politiques gérées pour le contrôle du routage dans Amazon Route 53 Application Recovery Controller

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 politique Service AWS est lancée ou lorsque de nouvelles opérations d'API sont disponibles pour les services existants.

Pour plus d'informations, consultez la section Politiques gérées par AWS dans le Guide de l'utilisateur IAM.

AWS politique gérée : AmazonRoute 53 RecoveryControlConfigFullAccess

Vous pouvez attacher `AmazonRoute53RecoveryControlConfigFullAccess` à vos entités IAM. Cette politique accorde un accès complet aux actions permettant d'utiliser la configuration du contrôle

de restauration dans Route 53 ARC. Associez-le aux utilisateurs IAM et aux autres principaux qui ont besoin d'un accès complet aux actions de configuration du contrôle de restauration.

À votre discrétion, vous pouvez ajouter l'accès à des actions Amazon Route 53 supplémentaires afin de permettre aux utilisateurs de créer des bilans de santé pour les contrôles de routage. Par exemple, vous pouvez autoriser une ou plusieurs des actions suivantes :`route53:GetHealthCheck`, `route53:CreateHealthCheckroute53:DeleteHealthCheck`, et`route53:ChangeTagsForResource`.

Pour consulter les autorisations associées à cette politique, reportez-vous à la section AmazonRoute53 du RecoveryControlConfigFullAccess manuel AWS Managed Policy Reference.

AWS politique gérée : AmazonRoute 53 RecoveryControlConfigReadOnlyAccess

Vous pouvez attacher `AmazonRoute53RecoveryControlConfigReadOnlyAccess` à vos entités IAM. C'est utile pour les utilisateurs qui ont besoin de consulter les configurations des règles de sécurité et de contrôle du routage. Cette politique accorde un accès en lecture seule aux actions permettant de travailler avec la configuration du contrôle de restauration dans Route 53 ARC. Ces utilisateurs ne peuvent pas créer, mettre à jour ou supprimer des ressources de contrôle de restauration.

Pour consulter les autorisations associées à cette politique, reportez-vous à la section AmazonRoute53 du RecoveryControlConfigReadOnlyAccess manuel AWS Managed Policy Reference.

AWS politique gérée : AmazonRoute 53 RecoveryClusterFullAccess

Vous pouvez attacher `AmazonRoute53RecoveryClusterFullAccess` à vos entités IAM. Cette politique accorde un accès complet aux actions permettant d'utiliser le plan de données du cluster dans Route 53 ARC. Associez-le aux utilisateurs IAM et aux autres principaux qui ont besoin d'un accès complet à la mise à jour et à la récupération des états de contrôle de routage.

Pour consulter les autorisations associées à cette politique, reportez-vous à la section AmazonRoute53 du RecoveryClusterFullAccess manuel AWS Managed Policy Reference.

AWS politique gérée : AmazonRoute 53 RecoveryClusterReadOnlyAccess

Vous pouvez attacher `AmazonRoute53RecoveryClusterReadOnlyAccess` à vos entités IAM. Cette politique accorde un accès en lecture seule au plan de données du cluster dans Route 53 ARC.

Ces utilisateurs peuvent récupérer les états du contrôle de routage mais ne peuvent pas les mettre à jour.

Pour consulter les autorisations associées à cette politique, reportez-vous à la section AmazonRoute53 du RecoveryClusterReadOnlyAccess manuel AWS Managed Policy Reference.

Mises à jour des politiques AWS gérées pour le contrôle du routage

Pour plus de détails sur les mises à jour des politiques AWS gérées pour le contrôle du routage dans Route 53 ARC depuis que ce service a commencé à suivre ces modifications, consultezMises à jour des politiques AWS gérées pour Amazon Route 53 Application Recovery Controller. Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au fil RSS sur la page d'historique du document ARC Route 53.

Quotas pour le contrôle du routage

Le contrôle du routage dans Amazon Route 53 Application Recovery Controller est soumis aux quotas suivants (anciennement appelés limites).

Entité	Quota
Nombre de clusters par compte	2
Nombre de panneaux de commande par cluster	50
Nombre de commandes de routage par panneau de commande	100
Nombre total de contrôles de routage (dans tous les panneaux de commande) par cluster	300
Nombre de règles de sécurité par panneau de commande	20
Nombre de contrôles de routage par appel UpdateRoutingControlStatesd'opération	10

Entité	Quota
Nombre d'appels d'API mutants vers un point de terminaison du cluster, par seconde	3

Vérification de l'état de préparation dans Amazon Route 53 Application Recovery Controller

Grâce au contrôle du niveau de préparation d'Amazon Route 53 Application Recovery Controller, vous pouvez savoir si vos applications et ressources sont prêtes à être restaurées. Une fois que vous avez modélisé votre AWS application dans Route 53 ARC et créé des contrôles de disponibilité, les contrôles surveillent en permanence les informations relatives à votre application, telles que les quotas de AWS ressources, la capacité et les politiques de routage réseau. Vous pouvez ensuite choisir d'être informé des modifications susceptibles d'affecter votre capacité à basculer vers une réplique de votre application pour vous remettre d'un événement. Les contrôles de préparation permettent de s'assurer, sur une base continue, que vous pouvez maintenir vos applications multirégionales dans un état adapté et configuré pour gérer le trafic de basculement.

Ce chapitre explique comment modéliser votre application dans Route 53 ARC afin de configurer la structure permettant aux contrôles de préparation de fonctionner, en créant un groupe de restauration et des cellules décrivant votre application. Vous pouvez ensuite suivre les étapes pour ajouter des contrôles de préparation et des périmètres de préparation afin que Route 53 ARC puisse vérifier l'état de préparation de votre application.

Après avoir créé des contrôles de disponibilité, vous pouvez surveiller l'état de préparation de vos ressources. Les contrôles de préparation vous permettent de vous assurer qu'une réplique d'application de secours et ses ressources correspondent en permanence à votre réplique de production, en tenant compte de la capacité, des politiques de routage et des autres détails de configuration de votre application de production. Si le réplica ne correspond pas, vous pouvez ajouter de la capacité ou modifier une configuration afin que les répliques de votre application soient à nouveau alignées.

> **Important**
>
> Les contrôles de préparation sont particulièrement utiles pour vérifier, sur une base continue, que les configurations des répliques d'applications et les états d'exécution sont alignés.

Les contrôles de disponibilité ne doivent pas être utilisés pour indiquer si votre réplique de production est saine, et vous ne devez pas non plus vous fier aux contrôles de disponibilité comme principal élément déclencheur du basculement en cas de sinistre.

Qu'est-ce que le contrôle de préparation dans Amazon Route 53 Application Recovery Controller ?

Un contrôle de l'état de préparation effectué dans Route 53 ARC permet de vérifier en permanence (à intervalles d'une minute) les incohérences en termes AWS de capacité allouée, de quotas de service, de limites d'accélérateur et de différences de configuration et de version pour les ressources incluses dans le contrôle. Les contrôles de préparation peuvent vous informer de ces différences afin que vous puissiez vous assurer que chaque réplique possède la même configuration et le même état d'exécution. Bien que les contrôles de préparation garantissent la cohérence des capacités configurées entre les répliques, vous ne devez pas vous attendre à ce qu'ils décident en votre nom de la capacité de votre réplique. Par exemple, vous devez comprendre les exigences de votre application afin de dimensionner vos groupes Auto Scaling avec une capacité de mémoire tampon suffisante dans chaque réplique pour gérer l'indisponibilité d'une autre cellule.

En ce qui concerne les quotas, lorsque Route 53 ARC détecte une incompatibilité lors d'un contrôle de préparation, il peut prendre des mesures pour aligner les quotas des répliques en augmentant le quota inférieur pour qu'il corresponde au quota le plus élevé. Lorsque les quotas correspondent, le statut du contrôle de préparation s'afficheREADY. (Notez qu'il ne s'agit pas d'un processus de mise à jour immédiat et que la durée totale dépend du type de ressource spécifique et d'autres facteurs.)

La première étape consiste à configurer des contrôles de préparation afin de créer un groupe de restauration représentant votre application. Chaque groupe de restauration inclut des cellules pour chaque unité individuelle de confinement des défaillances ou répliques de votre application. Ensuite, vous créez des ensembles de ressources pour chaque type de ressource de votre application et associez des contrôles de préparation aux ensembles de ressources. Enfin, vous associez les ressources à des zones de disponibilité afin de connaître l'état de préparation des ressources d'un groupe de restauration (votre application) ou de cellules individuelles (répliques, qui sont des régions ou des zones de disponibilité (AZ)).

L'état de préparation (c'READYest-à-direNOT READY) est basé sur les ressources concernées par le contrôle de préparation et sur l'ensemble de règles applicables à un type de ressource. Il existe des ensembles de règles de préparation pour chaque type de ressource, que les contrôles ARC de

Route 53 utilisent pour vérifier l'état de préparation des ressources. Le fait qu'une ressource l'est `READY` ou non dépend de la façon dont chaque règle de préparation est définie. Toutes les règles de préparation évaluent les ressources, mais certaines comparent les ressources entre elles et d'autres examinent des informations spécifiques sur chaque ressource de l'ensemble de ressources.

En ajoutant des contrôles de préparation, vous pouvez surveiller l'état de préparation de plusieurs manières : avec EventBridge, dans ou en utilisant les AWS Management Console actions de l'API Route 53 ARC. Vous pouvez également surveiller l'état de préparation des ressources dans différents contextes, notamment l'état de préparation des cellules et l'état de préparation de votre application. Utilisez la fonctionnalité d'autorisation entre comptes de Route 53 ARC pour faciliter la configuration et le suivi des ressources distribuées à partir d'un seul AWS compte.

Surveillance des répliques d'applications à l'aide de contrôles de préparation

Route 53 ARC audite les répliques de vos applications en utilisant des contrôles de préparation pour s'assurer que chacune d'entre elles possède la même configuration et le même état d'exécution. Un contrôle du niveau de préparation permet d'auditer en permanence la capacité des AWS ressources, la configuration, les AWS quotas et les politiques de routage d'une application, informations que vous pouvez utiliser pour vous assurer que les répliques sont prêtes à être basculées. Les contrôles de préparation vous aident à vous assurer que votre environnement de restauration est dimensionné et configuré pour basculer en cas de besoin.

Les sections suivantes fournissent plus de détails sur le fonctionnement de la vérification de l'état de préparation.

Contrôles de préparation et répliques de vos applications

Pour être prêt pour la restauration, vous devez conserver à tout moment une capacité de réserve suffisante dans les répliques, afin d'absorber le trafic de basculement en provenance d'une autre zone de disponibilité ou d'une autre région. Route 53 ARC inspecte en permanence (une fois par minute) votre application pour s'assurer que la capacité allouée correspond à toutes les zones de disponibilité ou régions.

La capacité inspectée par Route 53 ARC inclut, par exemple, le nombre d'instances Amazon EC2, les unités de capacité de lecture et d'écriture Aurora et la taille du volume Amazon EBS. Si vous augmentez la capacité de votre réplique principale en fonction des valeurs des ressources, mais que vous oubliez d'augmenter également les valeurs correspondantes dans votre réplique de secours, Route 53 ARC détecte le décalage afin que vous puissiez augmenter les valeurs de la réplique de réserve.

> **Important**
>
> Les contrôles de préparation sont particulièrement utiles pour vérifier, sur une base continue, que les configurations des répliques d'applications et les états d'exécution sont alignés. Les contrôles de disponibilité ne doivent pas être utilisés pour indiquer si votre réplique de production est saine, et vous ne devez pas non plus vous fier aux contrôles de disponibilité comme principal élément déclencheur du basculement en cas de sinistre.

Dans une configuration en veille active, vous devez prendre la décision de vous éloigner ou non d'une cellule en fonction de vos systèmes de surveillance et de vérification de l'état de santé, et envisager les contrôles de disponibilité comme un service complémentaire à ces systèmes. Les contrôles de disponibilité de la Route 53 ARC ne sont pas hautement disponibles. Vous ne devez donc pas vous fier à ce que les contrôles soient accessibles en cas de panne. En outre, les ressources vérifiées peuvent également ne pas être disponibles lors d'un sinistre.

Vous pouvez surveiller l'état de préparation des ressources de votre application dans des cellules spécifiques (AWS régions ou zones de disponibilité) ou pour l'ensemble de votre application. Vous pouvez être averti lorsque le statut d'un contrôle de préparation change, par exemple en`Not ready`, en créant des règles dans EventBridge. Pour plus d'informations, consultez Utilisation du contrôle de préparation dans Route 53 ARC avec Amazon EventBridge. Vous pouvez également consulter l'état de préparation dans AWS Management Console le ou en utilisant des opérations d'API, telles que`get-recovery-readiness`. Pour plus d'informations, consultez Opérations de l'API de contrôle de préparation.

Comment fonctionne le contrôle de préparation

Route 53 ARC audite les répliques de vos applications en utilisant des contrôles de préparation pour s'assurer que chacune d'entre elles possède la même configuration et le même état d'exécution.

Pour vous préparer à la reprise, par exemple, vous devez maintenir à tout moment une capacité de réserve suffisante pour absorber le trafic de basculement en provenance d'une autre zone de disponibilité ou région. Route 53 ARC inspecte en permanence (une fois par minute) votre application pour s'assurer que la capacité allouée correspond à toutes les zones de disponibilité ou régions. La capacité inspectée par Route 53 ARC inclut, par exemple, le nombre d'instances Amazon EC2, les unités de capacité de lecture et d'écriture Aurora et la taille du volume Amazon EBS. Si vous augmentez la capacité de votre réplique principale en fonction des valeurs des ressources, mais que vous oubliez d'augmenter également les valeurs correspondantes dans votre réplique de secours,

Route 53 ARC détecte le décalage afin que vous puissiez augmenter les valeurs de la réplique de réserve.

> **Important**
>
> Les contrôles de préparation sont particulièrement utiles pour vérifier, sur une base continue, que les configurations des répliques d'applications et les états d'exécution sont alignés. Les contrôles de disponibilité ne doivent pas être utilisés pour indiquer si votre réplique de production est saine, et vous ne devez pas non plus vous fier aux contrôles de disponibilité comme principal élément déclencheur du basculement en cas de sinistre.

Dans une configuration en veille active, vous devez prendre la décision de vous éloigner ou non d'une cellule en fonction de vos systèmes de surveillance et de vérification de l'état de santé, et envisager les contrôles de disponibilité comme un service complémentaire à ces systèmes. Les contrôles de disponibilité de la Route 53 ARC ne sont pas hautement disponibles. Vous ne devez donc pas vous fier à ce que les contrôles soient accessibles en cas de panne. En outre, les ressources vérifiées peuvent également ne pas être disponibles lors d'un sinistre.

Vous pouvez surveiller l'état de préparation des ressources de votre application dans des cellules spécifiques (AWS régions ou zones de disponibilité) ou pour l'ensemble de votre application. Vous pouvez être averti lorsque le statut d'un contrôle de préparation change, par exemple en`Not ready`, en créant des règles dans EventBridge. Pour plus d'informations, consultez Utilisation du contrôle de préparation dans Route 53 ARC avec Amazon EventBridge. Vous pouvez également consulter l'état de préparation dans AWS Management Console le ou en utilisant des opérations d'API, telles que`get-recovery-readiness`. Pour plus d'informations, consultez Opérations de l'API de contrôle de préparation.

Comment les règles de préparation déterminent l'état de préparation

Les contrôles de préparation de la Route 53 ARC déterminent l'état de préparation en fonction des règles prédéfinies pour chaque type de ressource et de la manière dont ces règles sont définies. Route 53 ARC inclut un groupe de règles pour chaque type de ressource qu'il prend en charge. Par exemple, Route 53 ARC comporte des groupes de règles de préparation pour les clusters Amazon Aurora, les groupes Auto Scaling, etc. Certaines règles de préparation comparent les ressources d'un ensemble entre elles, tandis que d'autres examinent des informations spécifiques sur chaque ressource de l'ensemble de ressources.

Vous ne pouvez pas ajouter, modifier ou supprimer des règles de préparation ou des groupes de règles. Cependant, vous pouvez créer une CloudWatch alarme Amazon et créer un contrôle de préparation pour surveiller l'état de l'alarme. Par exemple, vous pouvez créer une CloudWatch alarme personnalisée pour surveiller les services de conteneurs Amazon EKS et créer un contrôle de préparation pour vérifier l'état de préparation de l'alarme.

Vous pouvez consulter toutes les règles de préparation pour chaque type de ressource AWS Management Console lorsque vous créez un ensemble de ressources, ou vous pouvez consulter les règles de préparation ultérieurement en accédant à la page de détails d'un ensemble de ressources. Vous pouvez également consulter les règles de préparation dans la section suivante :Règles de préparation dans Route 53 ARC.

Lorsqu'un test de préparation audite un ensemble de ressources à l'aide d'un ensemble de règles, la façon dont chaque règle est définie détermine si le résultat sera `READY` ou `NOT READY` pour toutes les ressources ou s'il sera différent pour les différentes ressources. En outre, vous pouvez consulter l'état de préparation de différentes manières. Par exemple, vous pouvez consulter l'état de préparation d'un groupe de ressources dans un ensemble de ressources ou consulter un résumé de l'état de préparation d'un groupe de reprise ou d'une cellule (c'est-à-dire une AWS région ou une zone de disponibilité, selon la façon dont vous avez configuré votre groupe de récupération).

Le libellé de chaque description de règle explique comment il évalue les ressources pour déterminer l'état de préparation lorsque cette règle est appliquée. Une règle est définie pour inspecter chaque ressource ou pour inspecter toutes les ressources d'un ensemble de ressources afin de déterminer si elles sont prêtes. Plus précisément, les règles fonctionnent comme suit :

- La règle inspecte chaque ressource de l'ensemble de ressources pour vérifier une condition.
  - Si toutes les ressources réussissent, toutes les ressources sont définies comme`READY`.
  - En cas de défaillance d'une ressource, cette ressource est définie comme telle `NOT READY` et les autres cellules sont conservées`READY`.

  Par exemple : MskClusterState:inspecte chaque cluster Amazon MSK pour s'assurer qu'il est dans un `ACTIVE` état.
- La règle inspecte toutes les ressources de l'ensemble de ressources pour garantir une condition.
  - Si la condition est garantie, toutes les ressources sont définies comme`READY`.
  - Si l'une d'entre elles ne répond pas à cette condition, toutes les ressources sont définies comme`NOT READY`.

Par exemple : VpcSubnetCount:inspecte tous les VPC sous-réseaux pour s'assurer qu'ils possèdent le même nombre de sous-réseaux.

- Règle non critique : la règle inspecte toutes les ressources de l'ensemble de ressources pour garantir une condition.
  - En cas d'échec, l'état de préparation reste inchangé. Une règle présentant ce comportement comporte une note dans sa description.

  Par exemple : ElbV2CheckAzCount:inspecte chaque Network Load Balancer pour s'assurer qu'il est rattaché à une seule zone de disponibilité. Remarque : Cette règle n'a aucune incidence sur l'état de préparation.

En outre, Route 53 ARC franchit une étape supplémentaire en matière de quotas. Si un contrôle de préparation détecte une incompatibilité entre les cellules pour les quotas de service (la valeur maximale pour la création de ressources et les opérations) pour une ressource prise en charge, Route 53 ARC augmente automatiquement le quota pour la ressource dont le quota est le plus bas. Cela s'applique uniquement aux quotas (limites). Pour ce qui est de la capacité, vous devez ajouter de la capacité supplémentaire en fonction des besoins de votre application.

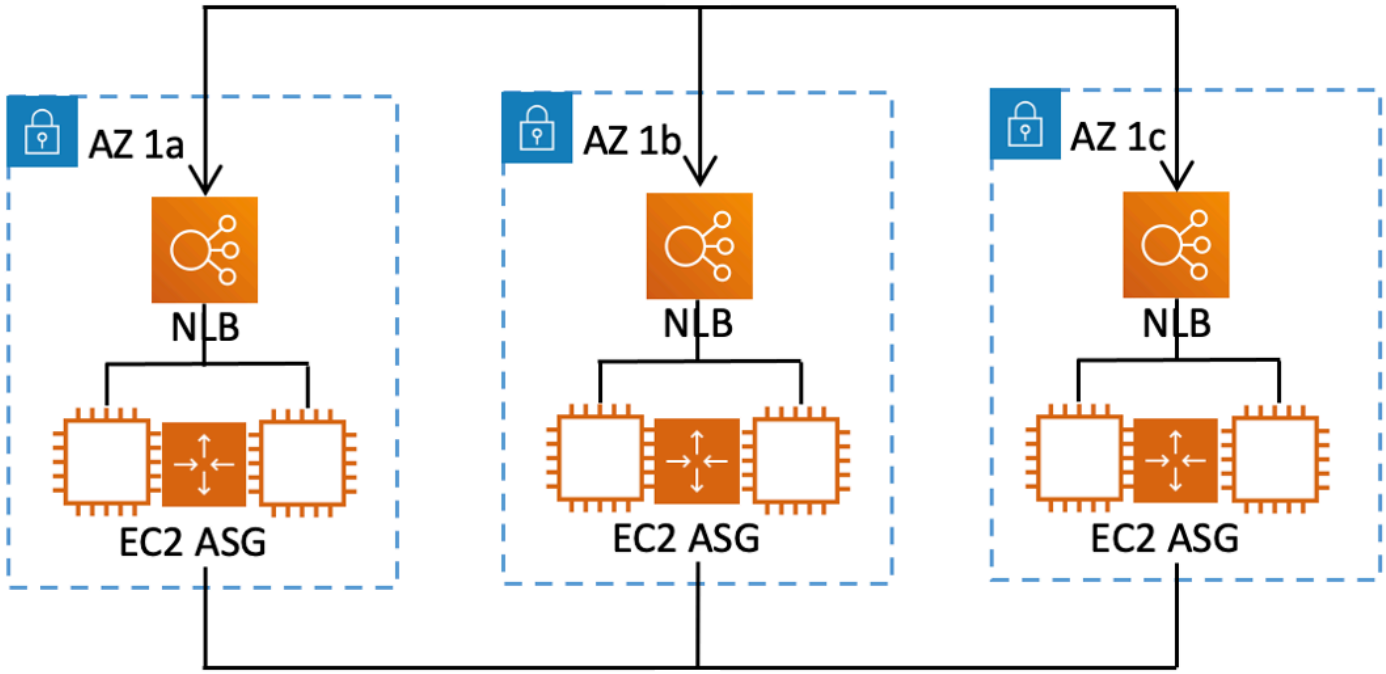
Vous pouvez également configurer une EventBridge notification Amazon pour les contrôles de préparation, par exemple lorsque le statut d'un contrôle de préparation passe à`NOT READY`. Ensuite, lorsqu'une incompatibilité de configuration est détectée, il vous EventBridge envoie une notification et vous pouvez prendre des mesures correctives pour vous assurer que les répliques de vos applications sont alignées et prêtes à être restaurées. Pour plus d’informations, consultez Utilisation du contrôle de préparation dans Route 53 ARC avec Amazon EventBridge.

Comment les contrôles de préparation, les ensembles de ressources et les périmètres de préparation fonctionnent ensemble

Les contrôles de préparation vérifient toujours les groupes de ressources dans les ensembles de ressources. Vous créez des ensembles de ressources (séparément ou pendant que vous créez un contrôle de disponibilité) pour regrouper les ressources qui se trouvent dans les cellules (zones de disponibilité ou AWS régions) de votre groupe de restauration Route 53 ARC, afin de pouvoir définir des contrôles de disponibilité. Un ensemble de ressources est généralement un groupe de ressources du même type (comme les équilibreurs de charge réseau), mais il peut également s'agir de ressources cibles DNS, pour les contrôles de préparation architecturale.

Vous créez généralement un ensemble de ressources et un contrôle de disponibilité pour chaque type de ressource de votre application. Pour vérifier le niveau de préparation de l'architecture, vous créez une ressource cible DNS de premier niveau et un ensemble de ressources global (au niveau du groupe de restauration) pour celle-ci, puis vous créez des ressources cibles DNS au niveau de la cellule, pour un ensemble de ressources distinct.

Le schéma suivant montre un exemple de groupe de restauration composé de trois cellules (Availability Zones), chacune dotée d'un Network Load Balancer (NLB) et d'un groupe Auto Scaling (ASG).



Dans ce scénario, vous devez créer un ensemble de ressources et un contrôle de disponibilité pour les trois Network Load Balancers, ainsi qu'un ensemble de ressources et un contrôle de disponibilité pour les trois groupes Auto Scaling. Vous disposez désormais d'une vérification de l'état de préparation de chaque ensemble de ressources pour votre groupe de restauration, par type de ressource.

En créant des zones de disponibilité pour les ressources, vous pouvez ajouter des résumés des contrôles de préparation pour les cellules ou les groupes de récupération. Pour spécifier le niveau de disponibilité d'une ressource, vous associez l'ARN de la cellule ou du groupe de restauration à chaque ressource d'un ensemble de ressources. Vous pouvez le faire lorsque vous créez un contrôle de disponibilité pour un ensemble de ressources.

Par exemple, lorsque vous ajoutez un contrôle de disponibilité pour un ensemble de ressources pour les équilibreurs de charge réseau pour ce groupe de restauration, vous pouvez ajouter des étendues de préparation à chaque NLB en même temps. Dans ce cas, vous devez associer l'ARN de l'AZ 1a au NLB de l'AZ 1a, l'ARN du `AZ 1b` NLB `AZ 1b` et l'ARN du NLB `AZ 1c` en. `AZ 1c` Lorsque vous créez un test de préparation pour les groupes Auto Scaling, vous devez faire de même, en attribuant des étendues de préparation à chacun d'entre eux lorsque vous créez le test de préparation pour l'ensemble de ressources du groupe Auto Scaling.

Il est facultatif d'associer des étendues de préparation lorsque vous créez un contrôle de préparation, mais nous vous recommandons vivement de les définir. Les zones de préparation permettent à Route 53 ARC d'indiquer le bon état de `NOT READY` préparation `READY` ou l'état de préparation pour les contrôles de préparation sommaires du groupe de reprise et les contrôles de préparation récapitulatifs au niveau des cellules. À moins que vous ne définissiez des périmètres de préparation, Route 53 ARC ne peut pas fournir ces résumés.

Notez que lorsque vous ajoutez une ressource globale ou au niveau de l'application, telle qu'une politique de routage DNS, vous ne choisissez pas de groupe ou de cellule de restauration pour la zone de disponibilité. Vous choisissez plutôt une ressource globale (aucune cellule).

Contrôles de disponibilité des ressources cibles du DNS : audit de l'état de préparation de la résilience

Grâce aux contrôles de disponibilité des ressources cibles du DNS dans Route 53 ARC, vous pouvez vérifier l'état de préparation de votre application en termes d'architecture et de résilience. Ce type de test de préparation analyse en permanence l'architecture de votre application et les politiques de routage d'Amazon Route 53 afin de vérifier les dépendances entre zones et entre régions.

Une application axée sur la restauration possède plusieurs répliques qui sont cloisonnées dans des zones de disponibilité ou des AWS régions, de sorte que les répliques peuvent échouer indépendamment les unes des autres. Si votre application doit être ajustée pour être correctement cloisonnée, Route 53 ARC vous proposera des modifications que vous pouvez apporter, si nécessaire, pour mettre à jour votre architecture afin de garantir sa résilience et sa préparation au basculement.

Route 53 ARC détecte automatiquement le nombre et l'étendue des cellules (représentant des répliques ou des unités de confinement des défaillances) dans votre application, et indique si les cellules sont cloisonnées par zone de disponibilité ou par région. Ensuite, Route 53 ARC identifie et vous fournit des informations sur les ressources d'application présentes dans les cellules, afin

de déterminer si elles sont correctement cloisonnées en zones ou en régions. Par exemple, si vos cellules sont situées dans des zones spécifiques, les contrôles de préparation peuvent vérifier si vos équilibreurs de charge et les cibles situées derrière eux sont également cloisonnés dans ces zones.

Grâce à ces informations, vous pouvez déterminer si des modifications doivent être apportées pour aligner les ressources de vos cellules sur les zones ou régions appropriées.

Pour commencer, vous devez créer des ressources cibles DNS pour votre application, ainsi que des ensembles de ressources et des contrôles de préparation pour celles-ci. Pour plus d'informations, consultez Obtenir des recommandations d'architecture dans Route 53 ARC.

Contrôles de préparation et scénarios de reprise après sinistre

Les contrôles de préparation à la Route 53 ARC vous permettent de savoir si vos applications et vos ressources sont prêtes à être restaurées en vous aidant à vous assurer que vos applications sont dimensionnées pour gérer le trafic de basculement. Les états des tests de disponibilité ne doivent pas être utilisés comme un signal indiquant qu'une réplique de production est saine. Vous pouvez toutefois utiliser des contrôles de préparation en complément de la surveillance de vos applications et de votre infrastructure ou de vos systèmes de vérification de l'état de santé afin de déterminer s'il convient de ne pas s'en remettre à une réplique ou de s'en remettre à une copie.

En cas d'urgence ou de panne, utilisez une combinaison de bilans de santé et d'autres informations pour déterminer si votre veille est étendue, saine et prête à être dépassée par le trafic de production. Par exemple, vérifiez si les canaris qui se heurtent à votre cellule de réserve répondent à vos critères de réussite, en plus de vérifier que le statut du test de préparation pour la mise en veille le est. `READY`

Sachez que les contrôles de disponibilité de la Route 53 ARC sont hébergés dans une seule AWS région, l'ouest des États-Unis (Oregon), et qu'en cas de panne ou de sinistre, les informations des contrôles de disponibilité peuvent devenir périmées ou ne plus être disponibles. Pour plus d'informations, consultez Plans de données et de contrôle pour le contrôle du routage.

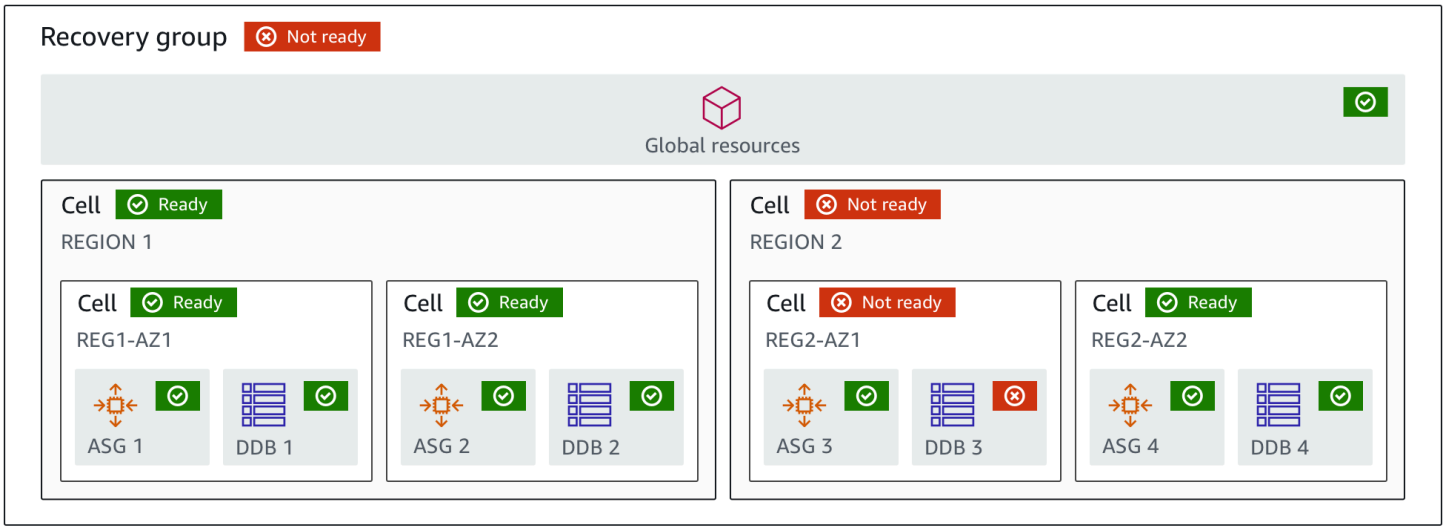
AWS Disponibilité de la région pour le contrôle de préparation

Pour obtenir des informations détaillées sur le support régional et les points de terminaison de service pour Amazon Route 53 Application Recovery Controller, consultez la section Points de terminaison et quotas Amazon Route 53 Application Recovery Controller dans le manuel Amazon Web Services General Reference.

> **Note**
>
> Le contrôle du niveau de préparation dans Amazon Route 53 Application Recovery Controller est une fonctionnalité globale. Cependant, les ressources de vérification de l'état de préparation se trouvent dans la région USA Ouest (Oregon). Vous devez donc spécifier la région USA Ouest (Oregon) (spécifiez le paramètre`--region us-west-2`) dans les AWS CLI commandes ARC de la Route 53 régionale, par exemple, lorsque vous créez des ressources telles que des ensembles de ressources et des contrôles de disponibilité.

Composants de contrôle de préparation

Le schéma suivant illustre un exemple de groupe de récupération configuré pour prendre en charge la fonction de vérification de l'état de préparation. Dans cet exemple, les ressources sont regroupées en cellules (par Région AWS) et en cellules imbriquées (par zones de disponibilité) dans un groupe de récupération. Il existe un état de préparation global pour le groupe de restauration (application), ainsi que des états de préparation individuels pour chaque cellule (région) et cellule imbriquée (zone de disponibilité).



Voici les composants de la fonction de vérification de l'état de préparation de Route 53 ARC.

Cellule

Une cellule définit les répliques ou les unités indépendantes de basculement de votre application. Il regroupe toutes les AWS ressources nécessaires à l'exécution indépendante de votre application au sein de la réplique. Par exemple, vous pouvez avoir un ensemble de ressources dans une cellule principale et un autre dans une cellule de secours. Vous déterminez les limites

du contenu d'une cellule, mais les cellules représentent généralement une zone de disponibilité ou une région. Vous pouvez avoir plusieurs cellules (cellules imbriquées) dans une cellule, par exemple des Z dans une région. Chaque cellule imbriquée représente une unité isolée de basculement.

Groupe de rétablissement

Les cellules sont rassemblées dans un groupe de récupération. Un groupe de restauration représente une application ou un groupe d'applications dont vous souhaitez vérifier l'état de préparation au basculement. Il se compose de deux ou plusieurs cellules, ou répliques, dont les fonctionnalités correspondent. Par exemple, si vous avez une application Web répliquée sur us-east-1a et us-east-1b, où us-east-1b est votre environnement de basculement, vous pouvez représenter cette application dans Route 53 ARC sous la forme d'un groupe de restauration composé de deux cellules : une dans us-east-1a et une dans us-east-1b. Un groupe de restauration peut également inclure une ressource globale, telle qu'un bilan de santé Route 53.

Ressources et identificateurs de ressources

Lorsque vous créez des composants pour les contrôles de préparation dans Route 53 ARC, vous spécifiez une ressource, telle qu'une table Amazon DynamoDB, un Network Load Balancer ou une ressource cible DNS, à l'aide d'un identifiant de ressource. Un identifiant de ressource est soit le Amazon Resource Name (ARN) de la ressource, soit, pour une ressource cible DNS, l'identifiant généré par Route 53 ARC lors de la création de la ressource.

Ressource cible DNS

Une ressource cible DNS est la combinaison du nom de domaine de votre application et d'autres informations DNS, telles que la AWS ressource vers laquelle pointe le domaine. L'inclusion d'une AWS ressource est facultative, mais si vous la fournissez, il doit s'agir d'un enregistrement de ressource Route 53 ou d'un Network Load Balancer. Lorsque vous fournissez la AWS ressource, vous pouvez obtenir des recommandations architecturales plus détaillées qui peuvent vous aider à améliorer la résilience de restauration de votre application. Vous pouvez créer des ensembles de ressources dans Route 53 ARC pour les ressources cibles DNS, puis créer un contrôle de disponibilité pour l'ensemble de ressources afin d'obtenir des recommandations d'architecture pour votre application. Le test de disponibilité surveille également la politique de routage DNS de votre application, en fonction des règles de préparation pour les ressources cibles du DNS.

Ensemble de ressources

Un ensemble de ressources est un ensemble de ressources, y compris AWS des ressources ou des ressources cibles DNS, qui s'étendent sur plusieurs cellules. Par exemple, vous pouvez

avoir un équilibreur de charge dans us-east-1a et un autre dans us-east-1b. Pour contrôler l'état de préparation des équilibreurs de charge à la restauration, vous pouvez créer un ensemble de ressources incluant les deux équilibreurs de charge, puis créer un contrôle de disponibilité pour l'ensemble de ressources. Route 53 ARC vérifiera en permanence l'état de préparation des ressources de l'ensemble. Vous pouvez également ajouter une étendue de disponibilité pour associer les ressources d'un ensemble de ressources au groupe de restauration que vous créez pour votre application.

Règle de préparation

Les règles de préparation sont des audits que Route 53 ARC effectue par rapport à un ensemble de ressources d'un ensemble de ressources. Route 53 ARC dispose d'un ensemble de règles de préparation pour chaque type de ressource pour lequel il prend en charge les contrôles de disponibilité. Chaque règle inclut un identifiant et une description qui expliquent les raisons pour lesquelles Route 53 ARC inspecte les ressources.

Contrôle de préparation

Un contrôle de disponibilité surveille un ensemble de ressources de votre application, tel qu'un ensemble d'instances Amazon Aurora, pour lequel Route 53 ARC vérifie le niveau de préparation à la restauration. Les contrôles de préparation peuvent inclure des audits, par exemple des configurations de capacité, AWS des quotas ou des politiques de routage. Par exemple, si vous souhaitez vérifier l'état de préparation de vos groupes Amazon EC2 Auto Scaling dans deux zones de disponibilité, vous pouvez créer un contrôle de préparation pour un ensemble de ressources avec deux ARN de ressources, un pour chaque groupe Auto Scaling. Ensuite, pour s'assurer que chaque groupe est dimensionné de la même manière, Route 53 ARC surveille en permanence les types d'instances et le nombre d'instances dans les deux groupes.

Périmètre de préparation

Un périmètre de préparation identifie le groupe de ressources inclus dans un contrôle de préparation spécifique. L'étendue d'un contrôle de préparation peut être un groupe de restauration (c'est-à-dire global à l'ensemble de l'application) ou une cellule (c'est-à-dire une région ou une zone de disponibilité). Pour une ressource qui est une ressource globale pour Route 53 ARC, définissez le périmètre de préparation au niveau du groupe de restauration ou de la ressource globale. Par exemple, un bilan de santé de la Route 53 est une ressource globale dans l'ARC de la Route 53 car il n'est pas spécifique à une région ou à une zone de disponibilité.

Plans de données et de contrôle pour le contrôle de l'état de préparation

Lorsque vous planifiez le basculement et la reprise après sinistre, évaluez la résilience de vos mécanismes de basculement. Nous vous recommandons de vous assurer que les mécanismes sur lesquels vous comptez lors du basculement sont hautement disponibles, afin de pouvoir les utiliser lorsque vous en avez besoin en cas de sinistre. En règle générale, vous devez utiliser les fonctions du plan de données pour vos mécanismes chaque fois que vous le pouvez, pour une fiabilité et une tolérance aux pannes optimales. Dans cette optique, il est important de comprendre comment les fonctionnalités d'un service sont réparties entre les plans de contrôle et les plans de données, et de comprendre dans quels cas vous pouvez compter sur une fiabilité extrême en ce qui concerne le plan de données d'un service.

Comme pour la plupart des AWS services, la fonctionnalité de vérification de l'état de préparation est prise en charge par les plans de contrôle et les plans de données. Bien que les deux soient conçus pour être fiables, un plan de contrôle est optimisé pour la cohérence des données, tandis qu'un plan de données est optimisé pour la disponibilité. Un plan de données est conçu pour être résilient afin de maintenir sa disponibilité même en cas d'événements perturbateurs, lorsqu'un plan de contrôle peut devenir indisponible.

En général, un plan de contrôle vous permet d'exécuter des fonctions de gestion de base, telles que la création, la mise à jour et la suppression de ressources dans le service. Un plan de données fournit les fonctionnalités de base d'un service.

Pour le contrôle de l'état de préparation, il existe une seule API, l'API Recovery Readiness, pour le plan de contrôle et le plan de données. Les contrôles de préparation et les ressources de préparation concernent uniquement la région de l'ouest des États-Unis (Oregon) (us-west-2). Le plan de contrôle du niveau de préparation et le plan de données sont fiables mais peu disponibles.

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

Marquage pour vérifier l'état de préparation dans Amazon Route 53 Application Recovery Controller

Les balises sont des mots ou des phrases (métadonnées) que vous utilisez pour identifier et organiser vos AWS ressources. Vous pouvez ajouter plusieurs balises à une ressource, chacune de ces balises étant composée d’une clé et d’une valeur que vous définissez. Par exemple, la clé

peut être l'environnement et la valeur peut être la production. Vous pouvez rechercher et filtrer vos ressources en fonction des balises que vous ajoutez.

Vous pouvez étiqueter les ressources suivantes lors du contrôle de disponibilité dans Route 53 ARC :

- Ensembles de ressources
- Contrôles de préparation

Le balisage dans Route 53 ARC n'est disponible que via l'API, par exemple en utilisant le AWS CLI.

Vous trouverez ci-dessous des exemples de balisage lors de la vérification de l'état de préparation à l'aide du AWS CLI.

```
aws route53-recovery-readiness --region us-west-2 create-resource-
set --resource-set-name dynamodb_resource_set --resource-set-type
AWS::DynamoDB::Table --resources ReadinessScopes=arn:aws:aws-recovery-
readiness::111122223333:cell/PDXCell,ResourceArn=arn:aws:dynamodb:us-
west-2:111122223333:table/PDX_Table ReadinessScopes=arn:aws:aws-recovery-
readiness::111122223333:cell/IADCell,ResourceArn=arn:aws:dynamodb:us-
east-1:111122223333:table/IAD_Table --tags Stage=Prod

aws route53-recovery-readiness --region us-west-2 create-readiness-
check --readiness-check-name dynamodb_readiness_check --resource-set-name
dynamodb_resource_set --tags Stage=Prod
```

Pour plus d'informations, consultez le guide TagResourcede référence de l'API Recovery Readiness pour Amazon Route 53 Application Recovery Controller.

Tarification du contrôle de l'état de préparation sur Route 53 ARC

Avec Amazon Route 53 Application Recovery Controller, vous ne payez que pour ce que vous configurez pour être utilisé dans le service. Pour le contrôle de préparation, vous payez un coût horaire par contrôle de préparation que vous configurez.

Pour obtenir des informations détaillées sur les tarifs de Route 53 ARC et des exemples de tarification, consultez les tarifs d'Amazon Route 53 Application Recovery Controller et faites défiler la page vers le bas jusqu'à Amazon Route 53 Application Recovery Controller.

Configurez un processus de restauration résilient pour votre application

Pour utiliser Amazon Route 53 Application Recovery Controller avec AWS des applications situées dans plusieurs AWS régions, vous devez suivre des directives pour configurer vos applications en termes de résilience, afin de garantir une préparation efficace à la restauration. Vous pouvez ensuite créer des contrôles de préparation pour votre application et configurer des contrôles de routage pour rediriger le trafic en cas de basculement. Vous pouvez également consulter les recommandations de Route 53 ARC concernant l'architecture de votre application qui peuvent améliorer la résilience.

> **Note**
>
> Si votre application est cloisonnée par zones de disponibilité, pensez à utiliser le décalage de zone ou le décalage automatique de zone pour la reprise après incident. Aucune configuration n'est requise pour utiliser le décalage de zone ou le décalage automatique de zone afin de restaurer de manière fiable les applications en cas de détérioration de la zone de disponibilité.
>
> Pour déplacer le trafic hors d'une zone de disponibilité pour les ressources de l'équilibreur de charge, lancez un changement de zone dans la console Route 53 ARC ou dans la console Elastic Load Balancing. Vous pouvez également utiliser le AWS SDK AWS Command Line Interface ou avec les actions de l'API Zonal Shift. Pour plus d'informations, consultez Changement de zone dans Amazon Route 53 Application Recovery Controller.

Pour en savoir plus sur la mise en route des configurations de basculement résilientes, consultezCommencer à utiliser la restauration multirégionale dans Amazon Route 53 Application Recovery Controller.

Meilleures pratiques en matière de vérification de l'état de préparation sur Route 53 ARC

Nous recommandons de suivre les bonnes pratiques suivantes pour vérifier l'état de préparation dans Amazon Route 53 Application Recovery Controller.

Ajouter des notifications pour les modifications de l'état de préparation

Définissez une règle dans Amazon EventBridge pour envoyer une notification chaque fois que le statut d'un contrôle de préparation passe, par exemple de `READY` à`NOT READY`. Lorsque vous

recevez une notification, vous pouvez examiner le problème et le résoudre, afin de vous assurer que votre application et vos ressources sont prêtes à être basculées au moment prévu.

Vous pouvez définir des EventBridge règles pour envoyer des notifications pour plusieurs modifications de l'état de préparation, notamment pour votre groupe de récupération (pour votre application), pour une cellule (telle qu'une AWS région) ou pour un contrôle de disponibilité pour un ensemble de ressources.

Pour plus d’informations, consultez Utilisation du contrôle de préparation dans Route 53 ARC avec Amazon EventBridge.

Opérations de l'API de contrôle de préparation

Le tableau suivant répertorie les opérations ARC de la Route 53 que vous pouvez utiliser pour vous préparer à la reprise (vérification de l'état de préparation), avec des liens vers la documentation pertinente.

Pour des exemples d'utilisation des opérations d'API courantes de préparation à la restauration avec le AWS Command Line Interface, voir Exemples d'utilisation des opérations de l'API de vérification de l'état de préparation ARC Route 53 avec le AWS CLI.

Action	Utilisation de la console Route 53 ARC	Utilisation de l'API ARC Route 53
Création d'une cellule	Consultez Création, mise à jour et suppression de groupes de récupération dans Route 53 ARC.	Consultez CreateCell
Obtenez un téléphone portable	Consultez Création, mise à jour et suppression de groupes de récupération dans Route 53 ARC.	Consultez GetCell
Supprimer une cellule	Consultez Création, mise à jour et suppression de groupes de récupération dans Route 53 ARC.	Consultez DeleteCell

Action	Utilisation de la console Route 53 ARC	Utilisation de l'API ARC Route 53
Mettre à jour une cellule	N/A	Consultez UpdateCell.
Répertorier les cellules d'un compte	Consultez Création, mise à jour et suppression de groupes de récupération dans Route 53 ARC.	Consultez ListCells
Création d'un groupe de récupération	Consultez Création, mise à jour et suppression de groupes de récupération dans Route 53 ARC.	Voir le CreateRecoverygroupe
Obtenez un groupe de rétablissement	Consultez Création, mise à jour et suppression de groupes de récupération dans Route 53 ARC.	Voir le GetRecoverygroupe
Mettre à jour un groupe de récupération	Consultez Création, mise à jour et suppression de groupes de récupération dans Route 53 ARC.	Voir le UpdateRecoverygroupe
Supprimer un groupe de récupération	Consultez Création, mise à jour et suppression de groupes de récupération dans Route 53 ARC.	Voir le DeleteRecoverygroupe
Lister les groupes de restauration	Consultez Création, mise à jour et suppression de groupes de récupération dans Route 53 ARC.	Voir les ListRecoverygroupes
Création d'un ensemble de ressources	Consultez Création et mise à jour des contrôles de préparation dans Route 53 ARC.	Voir CreateResourceSet

Action	Utilisation de la console Route 53 ARC	Utilisation de l'API ARC Route 53
Obtenir un ensemble de ressources	Consultez Création et mise à jour des contrôles de préparation dans Route 53 ARC.	Voir GetResourceSet
Mettre à jour un ensemble de ressources	Consultez Création et mise à jour des contrôles de préparation dans Route 53 ARC.	Voir UpdateResourceSet
Supprimer un ensemble de ressources	Consultez Création et mise à jour des contrôles de préparation dans Route 53 ARC.	Voir DeleteResourceSet
Lister les ensembles de ressources	Consultez Création et mise à jour des contrôles de préparation dans Route 53 ARC.	Voir les ListResourceensembles
Créer une vérification de l'état de préparation	Consultez Création et mise à jour des contrôles de préparation dans Route 53 ARC.	Voir CreateReadinessCheck
Faites une vérification de l'état de préparation	Consultez Création et mise à jour des contrôles de préparation dans Route 53 ARC.	Voir GetReadinessCheck
Mettre à jour un test de préparation	Consultez Création et mise à jour des contrôles de préparation dans Route 53 ARC.	Voir UpdateReadinessCheck
Supprimer une vérification de l'état de préparation	Consultez Création et mise à jour des contrôles de préparation dans Route 53 ARC.	Voir DeleteReadinessCheck
Lister les contrôles de préparation	Consultez Création et mise à jour des contrôles de préparation dans Route 53 ARC.	Voir les ListReadinesschèques

Action	Utilisation de la console Route 53 ARC	Utilisation de l'API ARC Route 53
Règles de préparation de la liste	Consultez Descriptions des règles de préparation dans Route 53 ARC.	Consultez ListRules
Vérifier l'état d'un contrôle de préparation complet	Consultez Surveillance de l'état de préparation sur Route 53 ARC.	Voir GetReadinessCheckStatus
Vérifier le statut d'une ressource	Consultez Surveillance de l'état de préparation sur Route 53 ARC.	Voir le GetReadinessCheckResourcestatut
Vérifier l'état d'une cellule	Consultez Surveillance de l'état de préparation sur Route 53 ARC.	Voir GetCellReadinessSummary
Vérifier l'état d'un groupe de restauration	Consultez Surveillance de l'état de préparation sur Route 53 ARC.	Voir le GetRecoveryGroupReadinessrésumé

Exemples d'utilisation des opérations de l'API de vérification de l'état de préparation ARC Route 53 avec le AWS CLI

Cette section présente des exemples d'applications simples utilisant les fonctionnalités de vérification AWS Command Line Interface de l'état de préparation d'Amazon Route 53 Application Recovery Controller à l'aide d'opérations d'API. Les exemples sont destinés à vous aider à acquérir une compréhension de base de la manière d'utiliser les fonctionnalités de vérification de l'état de préparation à l'aide de la CLI.

Vérifiez l'état de préparation dans le cadre des audits ARC de la Route 53 pour détecter les incohérences entre les ressources présentes dans les répliques de vos applications. Pour configurer les contrôles de préparation de votre application, vous devez configurer (ou modéliser) les ressources de votre application dans les cellules ARC de la Route 53 qui s'alignent sur les répliques que vous avez créées pour votre application. Vous configurez ensuite des contrôles de préparation qui auditent

ces répliques, afin de vous assurer que la réplique de votre application de secours et ses ressources correspondent à votre réplique de production, sur une base continue

Prenons un cas simple où vous avez une application nommée Simple-Service qui s'exécute actuellement dans la région USA Est (Virginie du Nord) (us-east-1). Vous disposez également d'une copie de réserve de l'application dans la région USA Ouest (Oregon) (us-west-2). Dans cet exemple, nous allons configurer des contrôles de disponibilité pour comparer ces deux versions de l'application. Cela nous permet de nous assurer que la région en veille, dans l'ouest des États-Unis (Oregon), est prête à recevoir du trafic, si nécessaire en cas de basculement.

Pour plus d'informations sur l'utilisation du AWS CLI, consultez la référence des AWS CLI commandes. Pour obtenir la liste des actions de l'API de préparation et des liens vers des informations supplémentaires, consultez Opérations de l'API de contrôle de préparation.

Les cellules de Route 53 ARC représentent les limites des failles (comme les zones de disponibilité ou les régions) et sont rassemblées dans des groupes de restauration. Un groupe de restauration représente une application dont vous souhaitez vérifier l'état de préparation au basculement. Pour plus d'informations sur les composants de la vérification de l'état de préparation, consultezComposants de contrôle de préparation .

> **Note**
>
> Route 53 ARC est un service mondial qui prend en charge plusieurs points de terminaison Régions AWS , mais vous devez spécifier la région USA Ouest (Oregon) (c'est-à-dire spécifier le paramètre`--region us-west-2`) dans la plupart des commandes de la CLI Route 53 ARC. Par exemple, pour créer des ressources telles que des groupes de restauration ou des contrôles de préparation.

Pour notre exemple d'application, nous allons commencer par créer une cellule pour chaque région où nous avons des ressources. Nous allons ensuite créer un groupe de restauration, puis terminer la configuration pour une vérification de l'état de préparation.

1. Création de cellules

1a. Créez une cellule us-east-1.

```
aws route53-recovery-readiness --region us-west-2 create-cell \
    --cell-name east-cell
```

```
{
    "CellArn": "arn:aws:route53-recovery-readiness::111122223333:cell/east-cell",
    "CellName": "east-cell",
    "Cells": [],
    "ParentReadinessScopes": [],
    "Tags": {}
}
```

1b. Créez une cellule us-west-1.

```
aws route53-recovery-readiness --region us-west-2 create-cell \
    --cell-name west-cell
```

```
{
    "CellArn": "arn:aws:route53-recovery-readiness::111122223333:cell/west-cell",
    "CellName": "west-cell",
    "Cells": [],
    "ParentReadinessScopes": [],
    "Tags": {}
}
```

1 c. Nous avons maintenant deux cellules. Vous pouvez vérifier leur existence en appelant l'`list-cells`API.

```
aws route53-recovery-readiness --region us-west-2 list-cells
```

```
{
    "Cells": [
        {
            "CellArn": "arn:aws:route53-recovery-readiness::111122223333:cell/east-
cell",
            "CellName": "east-cell",
            "Cells": [],
            "ParentReadinessScopes": [],
            "Tags": {}
        },
        {
            "CellArn": "arn:aws:route53-recovery-readiness::111122223333:cell/west-
cell",
            "CellName": "west-cell"
            "Cells": [],
```

```
            "ParentReadinessScopes": [],
            "Tags": {}
        }
    ]
}
```

2. Création d'un groupe de récupération

Les groupes de rétablissement constituent la principale ressource en matière de préparation au rétablissement dans Route 53 ARC. Un groupe de restauration représente une application dans son ensemble. Au cours de cette étape, nous allons créer un groupe de récupération pour modéliser une application globale, puis ajouter les deux cellules que nous avons créées.

2a. Créez un groupe de récupération.

```
aws route53-recovery-readiness --region us-west-2 create-recovery-group \
    --recovery-group-name simple-service-recovery-group \
       --cells "arn:aws:route53-recovery-readiness::111122223333:cell/east-cell"\
       "arn:aws:route53-recovery-readiness::111122223333:cell/west-cell"
```

```
{
    "Cells": [],
    "RecoveryGroupArn": "arn:aws:route53-recovery-readiness::111122223333:recovery-
group/simple-service-recovery-group",
    "RecoveryGroupName": "simple-service-recovery-group",
    "Tags": {}
}
```

2 b. (Facultatif) Vous pouvez vérifier que votre groupe de récupération a été créé correctement en appelant l'`list-recovery-groups` API.

```
aws route53-recovery-readiness --region us-west-2 list-recovery-groups
```

```
{
    "RecoveryGroups": [
        {
            "Cells": [
                "arn:aws:route53-recovery-readiness::111122223333:cell/east-cell",
                "arn:aws:route53-recovery-readiness::111122223333:cell/west-cell"
            ],
```

```
            "RecoveryGroupArn": "arn:aws:route53-recovery-
readiness::111122223333:recovery-group/simple-service-recovery-group",
            "RecoveryGroupName": "simple-service-recovery-group",
            "Tags": {}
        }
    ]
}
```

Maintenant que nous avons un modèle pour notre application, ajoutons les ressources à surveiller. Dans Route 53 ARC, un groupe de ressources que vous souhaitez surveiller est appelé ensemble de ressources. Les ensembles de ressources contiennent des ressources qui sont toutes du même type. Nous comparons les ressources d'un ensemble de ressources entre elles afin de déterminer si une cellule est prête à faire face au basculement.

3. Création d'un ensemble de ressources

Supposons que notre Simple-Service application soit en effet très simple et n'utilise que des tables DynamoDB. Il possède une table DynamoDB dans us-east-1 et une autre dans us-west-2. Un ensemble de ressources contient également une étendue de disponibilité, qui identifie la cellule dans laquelle se trouve chaque ressource.

3a. Créez un ensemble de ressources qui reflète les ressources de notre Simple-Service application.

```
aws route53-recovery-readiness --region us-west-2 create-resource-set \
    --resource-set-name ImportantInformationTables \
    --resource-set-type AWS::DynamoDB::Table \
    --resources
    ResourceArn="arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsWest2",ReadinessScopes="arn:aws:route53-recovery-readiness::111122223333:cell/
west-cell"
    ResourceArn="arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsEast1",ReadinessScopes="arn:aws:route53-recovery-readiness::111122223333:cell/
east-cell"
```

```
{
    "ResourceSetArn": "arn:aws:route53-recovery-readiness::111122223333:resource-set/
sample-resource-set",
    "ResourceSetName": "ImportantInformationTables",
    "Resources": [
        {
            "ReadinessScopes": [
```

```
                "arn:aws:route53-recovery-readiness::111122223333:cell/west-cell"
            ],
            "ResourceArn": "arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsWest2"
        },
        {
            "ReadinessScopes": [
                "arn:aws:route53-recovery-readiness::111122223333:cell/east-cell"
            ],
            "ResourceArn": "arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsEast1"
        }
    ],
    "Tags": {}
}
```

3b. (Facultatif) Vous pouvez vérifier ce qui est inclus dans l'ensemble de ressources en appelant l'`list-resource-sets`API. Cela répertorie tous les ensembles de ressources d'un AWS compte. Ici, vous pouvez voir que nous n'avons qu'un seul ensemble de ressources créé ci-dessus.

```
aws route53-recovery-readiness --region us-west-2 list-resource-sets
```

```
{
    "ResourceSets": [
        {
            "ResourceSetArn": "arn:aws:route53-recovery-
readiness::111122223333:resource-set/ImportantInformationTables",
            "ResourceSetName": "ImportantInformationTables",
            "Resources": [
                {
                    "ReadinessScopes": [
                        "arn:aws:route53-recovery-readiness::111122223333:cell/west-
cell"
                    ],
                    "ResourceArn": "arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsWest2"
                },
                {
                    "ReadinessScopes": [
                        "arn:aws:route53-recovery-readiness::111122223333:cell/east-
cell"
                    ],
```

```
                    "ResourceArn": "arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsEast1"
                }
            ],
            "Tags": {}
        }
    ]
}{
    "ResourceSets": [
        {
            "ResourceSetArn": "arn:aws:route53-recovery-
readiness::111122223333:resource-set/ImportantInformationTables",
            "ResourceSetName": "ImportantInformationTables",
            "Resources": [
                {
                    "ReadinessScopes": [
                        "arn:aws:route53-recovery-readiness::111122223333:cell/west-
cell"
                    ],
                    "ResourceArn": "arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsWest2"
                },
                {
                    "ReadinessScopes": [
                        "arn:aws:route53-recovery-
readiness::&ExampleAWSAccountNo1;:cell/east-cell"
                    ],
                    "ResourceArn": "arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsEast1"
                }
            ],
            "Tags": {}
        }
    ]
}
```

Nous avons maintenant créé les cellules, le groupe de récupération et le jeu de ressources pour modéliser l'Simple-Serviceapplication dans Route 53 ARC. Ensuite, nous allons mettre en place des contrôles de préparation afin de contrôler l'état de préparation des ressources en cas de basculement.

4. Créer une vérification de l'état de préparation

Une vérification de l'état de préparation applique un ensemble de règles à chaque ressource de l'ensemble de ressources associé à la vérification. Les règles sont spécifiques à chaque type de ressource. C'est-à-dire qu'il existe des règles différentes pour `AWS::DynamoDB::TableAWS::EC2::Instance`, et ainsi de suite. Les règles vérifient diverses dimensions d'une ressource, notamment la configuration, la capacité (le cas échéant), les limites (le cas échéant) et les configurations de routage.

> **Note**
>
> Pour voir les règles appliquées à une ressource lors d'un contrôle de disponibilité, vous pouvez utiliser l'`get-readiness-check-resource-status`API, comme décrit à l'étape 5. Pour consulter la liste de toutes les règles de préparation de Route 53 ARC, utilisez `list-rules` ou consultezDescriptions des règles de préparation dans Route 53 ARC. Route 53 ARC dispose d'un ensemble de règles spécifiques qu'il exécute pour chaque type de ressource ; elles ne sont pas personnalisables pour le moment.

4a. Créez une vérification de l'état de préparation de l'ensemble de ressources,ImportantInformationTables.

```
aws route53-recovery-readiness --region us-west-2 create-readiness-check \
    --readiness-check-name ImportantInformationTableCheck --resource-set-name
 ImportantInformationTables
```

```
{
    "ReadinessCheckArn": "arn:aws:route53-recovery-readiness::111122223333:readiness-
check/ImportantInformationTableCheck",
    "ReadinessCheckName": "ImportantInformationTableCheck",
    "ResourceSet": "ImportantInformationTables",
    "Tags": {}
}
```

4 b. (Facultatif) Pour vérifier que le contrôle de préparation a bien été créé, exécutez l'`list-readiness-checks`API. Cette API affiche tous les contrôles de préparation d'un compte.

```
aws route53-recovery-readiness --region us-west-2 list-readiness-checks
```

```
{
    "ReadinessChecks": [
        {
            "ReadinessCheckArn": "arn:aws:route53-recovery-
readiness::111122223333:readiness-check/ImportantInformationTableCheck",
            "ReadinessCheckName": "ImportantInformationTableCheck",
            "ResourceSet": "ImportantInformationTables",
            "Tags": {}
        }
    ]
}
```

5. Surveiller les contrôles de préparation

Maintenant que nous avons modélisé l'application et ajouté un test de disponibilité, nous sommes prêts à surveiller les ressources. Vous pouvez modéliser le niveau de préparation de votre application à quatre niveaux : le niveau de vérification de l'état de préparation (un groupe de ressources), le niveau des ressources individuelles, le niveau de la cellule (toutes les ressources d'une zone de disponibilité ou d'une région) et le niveau du groupe de restauration (l'application dans son ensemble). Les commandes permettant d'obtenir chacun de ces types d'états de préparation sont fournies ci-dessous.

5a. Consultez l'état de votre test de préparation.

```
aws route53-recovery-readiness --region us-west-2 get-readiness-check-status\
    --readiness-check-name ImportantInformationTableCheck
```

```
{
    "Readiness": "READY",
    "Resources": [
        {
            "LastCheckedTimestamp": "2021-01-07T00:53:39Z",
            "Readiness": "READY",
            "ResourceArn": "arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsWest2"
        },
        {
            "LastCheckedTimestamp": "2021-01-07T00:53:39Z",
            "Readiness": "READY",
            "ResourceArn": "arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsEast2"
```

```
    ]
}
```

5 b. Consultez l'état de préparation détaillé d'une seule ressource lors d'un contrôle de disponibilité, y compris le statut de chaque règle vérifiée.

```
aws route53-recovery-readiness --region us-west-2 get-readiness-check-resource-status \
    --readiness-check-name ImportantInformationTableCheck \
    --resource-identifier "arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsWest2"
```

```
{"Readiness": "READY",
    "Rules": [
        {
            "LastCheckedTimestamp": "2021-01-07T00:55:41Z",
            "Messages": [],
            "Readiness": "READY",
            "RuleId": "DynamoTableStatus"
        },
        {
            "LastCheckedTimestamp": "2021-01-07T00:55:41Z",
            "Messages": [],
            "Readiness": "READY",
            "RuleId": "DynamoCapacity"
        },
        {
            "LastCheckedTimestamp": "2021-01-07T00:55:41Z",
            "Messages": [],
            "Readiness": "READY",
            "RuleId": "DynamoPeakRcuWcu"
        },
        {
            "LastCheckedTimestamp": "2021-01-07T00:55:41Z",
            "Messages": [],
            "Readiness": "READY",
            "RuleId": "DynamoGSIsPeakRcuWcu"
        },
        {
            "LastCheckedTimestamp": "2021-01-07T00:55:41Z",
            "Messages": [],
            "Readiness": "READY",
            "RuleId": "DynamoGSIsConfig"
        },
```

```
        {
            "LastCheckedTimestamp": "2021-01-07T00:55:41Z",
            "Messages": [],
            "Readiness": "READY",
            "RuleId": "DynamoGSIsStatus"
        },
        {
            "LastCheckedTimestamp": "2021-01-07T00:55:41Z",
            "Messages": [],
            "Readiness": "READY",
            "RuleId": "DynamoGSIsCapacity"
        },
        {
            "LastCheckedTimestamp": "2021-01-07T00:55:41Z",
            "Messages": [],
            "Readiness": "READY",
            "RuleId": "DynamoReplicationLatency"
        },
        {
            "LastCheckedTimestamp": "2021-01-07T00:55:41Z",
            "Messages": [],
            "Readiness": "READY",
            "RuleId": "DynamoAutoScalingConfiguration"
        },
        {
            "LastCheckedTimestamp": "2021-01-07T00:55:41Z",
            "Messages": [],
            "Readiness": "READY",
            "RuleId": "DynamoLimits"
        }
    ]
}
```

5c. Vérifiez l'état de préparation global d'une cellule.

```
aws route53-recovery-readiness --region us-west-2 get-cell-readiness-summary \
    --cell-name west-cell
```

```
{
    "Readiness": "READY",
    "ReadinessChecks": [
        {
            "Readiness": "READY",
```

```
            "ReadinessCheckName": "ImportantTableCheck"
        }
    ]
}
```

5d. Enfin, vérifiez le niveau de préparation de haut niveau de votre application, au niveau du groupe de restauration.

```
aws route53-recovery-readiness --region us-west-2 get-recovery-group-readiness-summary
 \
    --recovery-group-name simple-service-recovery-group
```

```
{
    "Readiness": "READY",
    "ReadinessChecks": [
        {
            "Readiness": "READY",
            "ReadinessCheckName": "ImportantTableCheck"
        }
    ]
}
```

Travailler avec des groupes de rétablissement et vérifier l'état de préparation

Cette section décrit et fournit des procédures pour les groupes de restauration et les contrôles de préparation, y compris la création, la mise à jour et la suppression de ces ressources.

Création, mise à jour et suppression de groupes de récupération dans Route 53 ARC

Un groupe de récupération représente votre application dans Amazon Route 53 Application Recovery Controller. Il se compose généralement de deux cellules ou plus qui sont des répliques les unes des autres en termes de ressources et de fonctionnalités, de sorte que vous pouvez passer de l'une à l'autre. Chaque cellule inclut les Amazon Resource Names (ARN) pour les ressources actives d'une AWS région ou d'une zone de disponibilité. Les ressources peuvent être un équilibreur de charge Elastic Load Balancing, un groupe Auto Scaling ou d'autres ressources. Une cellule correspondante représentant une autre zone ou région possède des ressources de secours du même type que celles présentes dans votre cellule active : un équilibreur de charge, un groupe Auto Scaling, etc.

Une cellule représente des répliques de votre application. Les contrôles de préparation effectués dans Route 53 ARC vous aident à déterminer si votre application est prête à passer d'une réplique à une autre. Cependant, vous devez prendre la décision de ne pas utiliser ou non une réplique en fonction de vos systèmes de surveillance et de vérification de l'état de santé, et envisager les contrôles de disponibilité comme un service complémentaire à ces systèmes.

L'état de préparation vérifie les ressources d'audit afin de déterminer leur état de préparation sur la base d'un ensemble de règles prédéfinies pour ce type de ressource. Une fois que vous avez créé votre groupe de restauration avec les répliques, vous ajoutez des contrôles de préparation à Route 53 ARC pour les ressources de votre application. Route 53 ARC peut ainsi vous aider à garantir que les répliques ont la même configuration au fil du temps.

Rubriques

Création de groupes de récupération

Les étapes décrites dans cette section expliquent comment créer un groupe de récupération sur la console Route 53 ARC. Pour en savoir plus sur l'utilisation des opérations d'API de préparation à la restauration avec Amazon Route 53 Application Recovery Controller, consultez Opérations de l'API de contrôle de préparation.

Pour créer un groupe de récupération

1. Ouvrez la console Route 53 ARC à l'adressehttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Choisissez Readiness check.
3. Sur la page Préparation à la restauration, choisissez Create, puis choisissez un groupe de restauration.
4. Entrez le nom de votre groupe de restauration, puis choisissez Next.
5. Choisissez Créer des cellules, puis Ajouter une cellule.
6. Entrez le nom de la cellule. Par exemple, si vous avez une réplique d'application dans l'ouest des États-Unis (Californie du Nord), vous pouvez ajouter une cellule nomméeMyApp-us-west-1.

7. Choisissez Ajouter une cellule, puis attribuez un nom à une deuxième cellule. Par exemple, si vous avez une réplique dans l'est des États-Unis (Ohio), vous pouvez ajouter une cellule nommée `MyApp-us-east-2`.
8. Si vous souhaitez ajouter des cellules imbriquées (répliques dans des zones de disponibilité au sein des régions), choisissez Action, choisissez Ajouter une cellule imbriquée, puis entrez un nom.
9. Lorsque vous avez ajouté toutes les cellules et les cellules imbriquées pour les répliques de votre application, choisissez Next.
10. Passez en revue votre groupe de récupération, puis choisissez Créer un groupe de récupération.

Mise à jour et suppression de groupes et de cellules de récupération

Les étapes décrites dans cette section expliquent comment mettre à jour et supprimer un groupe de récupération, et comment supprimer une cellule sur la console Route 53 ARC. Pour en savoir plus sur l'utilisation des opérations d'API de préparation à la restauration avec Amazon Route 53 Application Recovery Controller, consultez Opérations de l'API de contrôle de préparation.

Pour mettre à jour ou supprimer un groupe de récupération, ou supprimer une cellule

1. Ouvrez la console Route 53 ARC à l'adressehttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Choisissez Readiness check.
3. Sur la page Préparation à la restauration, choisissez un groupe de restauration.
4. Pour travailler avec un groupe de récupération, choisissez Action, puis choisissez Modifier le groupe de récupération ou Supprimer le groupe de récupération.
5. Lorsque vous modifiez un groupe de récupération, vous pouvez ajouter ou supprimer des cellules ou des cellules imbriquées.

   - Pour ajouter une cellule, choisissez Ajouter une cellule.
   - Pour supprimer une cellule, sous l'étiquette Action située à côté de la cellule, choisissez Supprimer la cellule.

Création et mise à jour des contrôles de préparation dans Route 53 ARC

Cette section fournit des procédures pour les contrôles de préparation et les ensembles de ressources, y compris la création, la mise à jour et la suppression de ces ressources.

Création et mise à jour d'un contrôle de préparation

Les étapes décrites dans cette section expliquent comment créer un contrôle de préparation sur la console Route 53 ARC. Pour en savoir plus sur l'utilisation des opérations d'API de préparation à la restauration avec Amazon Route 53 Application Recovery Controller, consultez Opérations de l'API de contrôle de préparation.

Pour mettre à jour un contrôle de disponibilité, vous pouvez modifier l'ensemble de ressources pour le contrôle de préparation, pour ajouter ou supprimer des ressources ou pour modifier le périmètre de préparation d'une ressource.

Pour créer un contrôle de préparation

1. Ouvrez la console Route 53 ARC à l'adressehttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Choisissez Readiness check.
3. Sur la page Préparation, choisissez Créer, puis choisissez un contrôle de préparation.
4. Entrez un nom pour votre test de disponibilité, choisissez le type de ressource que vous souhaitez vérifier, puis cliquez sur Suivant.
5. Ajoutez un ensemble de ressources pour votre vérification de l'état de préparation. Un ensemble de ressources est un groupe de ressources du même type dans différentes répliques. Sélectionnez l'une des méthodes suivantes :

   - Créez un test de préparation avec les ressources d'un ensemble de ressources que vous avez déjà créé.
   - Créez un nouvel ensemble de ressources.

   Si vous choisissez de créer un nouvel ensemble de ressources, donnez-lui un nom et choisissez Ajouter.
6. Copiez et collez les Amazon Resource Names (ARN) un par un pour chaque ressource que vous souhaitez inclure dans l'ensemble, puis choisissez Next.

> **Tip**
>
> Pour des exemples et plus d'informations sur le format ARN attendu par Route 53 ARC pour chaque type de ressource, consultezTypes de ressources et formats ARN dans Route 53 ARC.

7. Si vous le souhaitez, consultez les règles de préparation qui seront utilisées lorsque Route 53 ARC vérifiera le type de ressource que vous avez inclus dans cette vérification de disponibilité. Ensuite, sélectionnez Suivant.
8. (Facultatif) Sous Nom du groupe de restauration, choisissez un groupe de récupération auquel associer le contrôle de disponibilité, puis, pour chaque ARN de ressource, choisissez une cellule (région ou zone de disponibilité) dans le menu déroulant dans lequel se trouve la ressource. S'il s'agit d'une ressource au niveau de l'application, telle qu'une politique de routage DNS, choisissez une ressource globale (aucune cellule).

   Cela spécifie les limites de disponibilité des ressources dans le cadre du contrôle de préparation.

   > **Important**
   >
   > Bien que cette étape soit facultative, des zones de préparation doivent être ajoutées pour obtenir des informations récapitulatives sur l'état de préparation de votre groupe de restauration et de vos cellules. Si vous ignorez cette étape et que vous n'associez pas le contrôle de préparation aux ressources de votre groupe de restauration en choisissant des zones de préparation ici, Route 53 ARC ne peut pas renvoyer d'informations récapitulatives sur l'état de préparation du groupe ou des cellules de restauration.
9. Choisissez Suivant.
10. Consultez les informations de la page de confirmation, puis choisissez Créer un contrôle de préparation.

Pour supprimer un contrôle de préparation

1. Ouvrez la console Route 53 ARC à l'adressehttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Choisissez Readiness check.
3. Choisissez une vérification de l'état de préparation, puis sous Actions, choisissez Supprimer.

Création et modification d'ensembles de ressources

Généralement, vous créez un ensemble de ressources dans le cadre d'un contrôle de disponibilité, mais vous pouvez également créer un ensemble de ressources séparément. Vous pouvez également modifier un ensemble de ressources pour ajouter ou supprimer des ressources. Les étapes décrites dans cette section expliquent comment créer ou modifier un ensemble de ressources sur la

console Route 53 ARC. Pour en savoir plus sur l'utilisation des opérations d'API de préparation à la restauration avec Amazon Route 53 Application Recovery Controller, consultez Opérations de l'API de contrôle de préparation.

Pour créer un ensemble de ressources

1. Ouvrez la console Route 53 à l'adresse https://console.aws.amazon.com/route53/home.
2. Sous Application Recovery Controller, sélectionnez Resource sets.
3. Choisissez Créer.
4. Entrez un nom pour le jeu de ressources, puis choisissez le type de ressource à inclure dans l'ensemble.
5. Choisissez Ajouter, puis entrez le nom de ressource Amazon (ARN) de la ressource à ajouter à l'ensemble.
6. Une fois que vous avez terminé d'ajouter des ressources, choisissez Créer un ensemble de ressources.

Pour modifier un ensemble de ressources

1. Ouvrez la console Route 53 ARC à l'adressehttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Choisissez Readiness check.
3. Sous Ensembles de ressources, choisissez Action, puis Modifier.
4. Effectuez l’une des actions suivantes :
   - Pour supprimer une ressource de l'ensemble, choisissez Supprimer.
   - Pour ajouter une ressource à l'ensemble, choisissez Ajouter, puis entrez le nom Amazon Resource Name (ARN) de la ressource.
5. Vous pouvez également modifier l'étendue de disponibilité de la ressource, afin d'associer la ressource à une autre cellule pour le contrôle de disponibilité.
6. Choisissez Enregistrer.

Surveillance de l'état de préparation sur Route 53 ARC

Vous pouvez vérifier l'état de préparation de votre application dans Amazon Route 53 Application Recovery Controller aux niveaux suivants :

- Le niveau de vérification de l'état de préparation des ressources d'un ensemble de ressources
- Le niveau de ressource individuel
- Le niveau de cellule (réplique de l'application) pour toutes les ressources d'une zone de disponibilité ou d'une AWS région
- Le niveau du groupe de restauration pour l'application dans son ensemble

Vous pouvez être informé des modifications de l'état de préparation, ou vous pouvez surveiller les modifications de l'état de préparation dans la console Route 53 ou en utilisant les commandes de la Route 53 ARC CLI.

Notification de l'état de préparation

Vous pouvez utiliser Amazon EventBridge pour configurer des règles basées sur les événements afin de surveiller les ressources ARC de la Route 53 et de vous informer des modifications de l'état de préparation. Pour plus d'informations, consultez Utilisation du contrôle de préparation dans Route 53 ARC avec Amazon EventBridge.

Surveillance de l'état de préparation dans la console Route 53 ARC

La procédure suivante décrit comment contrôler l'état de préparation à la restauration dans le AWS Management Console.

1. Ouvrez la console Route 53 ARC à l'adressehttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Choisissez Readiness check.
3. Sur la page Préparation, sous Groupe de restauration, consultez l'état de préparation du groupe de restauration pour chaque groupe de restauration (application).

   Vous pouvez également vérifier l'état de préparation de cellules spécifiques ou de ressources individuelles.

Surveillance de l'état de préparation à l'aide des commandes CLI

Cette section fournit des exemples de AWS CLI commandes à utiliser pour connaître l'état de préparation de votre application et de vos ressources à différents niveaux.

Préparation à un ensemble de ressources

État d'un contrôle de préparation que vous avez créé pour un ensemble de ressources (un groupe de ressources).

```
aws route53-recovery-readiness --region us-west-2 get-readiness-check-status --readiness-check-name ReadinessCheckName
```

Préparation à une ressource unique

Pour connaître le statut d'une seule ressource lors d'un contrôle de disponibilité, y compris le statut de chaque règle de disponibilité vérifiée, spécifiez le nom du contrôle de disponibilité et un ARN de ressource. Par exemple :

```
aws route53-recovery-readiness --region us-west-2 get-readiness-check-status --readiness-check-name ReadinessCheckName --resource-arn "arn:aws:dynamodb:us-west-2:111122223333:table/TableName"
```

Préparation à une cellule

État d'une seule cellule, c'est-à-dire d'une région ou d'une zone de disponibilité.

```
aws route53-recovery-readiness --region us-west-2 get-cell-readiness-summary --cell-name CellName
```

Préparation à une candidature

État de l'application globale, au niveau du groupe de restauration.

```
aws route53-recovery-readiness --region us-west-2 get-recovery-group-readiness-summary --recovery-group-name RecoveryGroupName
```

Obtenir des recommandations d'architecture dans Route 53 ARC

Si vous possédez une application existante, Amazon Route 53 Application Recovery Controller peut évaluer l'architecture de votre application et les politiques de routage afin de fournir des recommandations pour modifier la conception afin d'améliorer la résilience de restauration de votre application. Après avoir créé un groupe de récupération dans Route 53 ARC qui représente votre application, suivez les étapes décrites dans cette section pour obtenir des recommandations concernant l'architecture de votre application.

Nous vous recommandons de spécifier une ressource cible pour la ressource cible DNS de votre groupe de restauration, si vous ne l'avez pas encore spécifiée, afin que nous puissions fournir

des recommandations plus détaillées. Lorsque vous fournissez des informations supplémentaires, Route 53 ARC peut vous fournir de meilleures recommandations. Par exemple, si vous entrez un enregistrement de ressource Amazon Route 53 ou un Network Load Balancer comme ressource cible, Route 53 ARC peut fournir des informations indiquant si vous avez créé le nombre optimal de cellules pour votre groupe de récupération.

Notez ce qui suit pour les ressources cibles DNS :

- Spécifiez uniquement un enregistrement de ressource Route 53 ou un Network Load Balancer pour une ressource cible.
- Créez une seule ressource cible DNS pour chaque groupe de restauration.
- Recommandé : créez une ressource cible DNS pour chaque cellule.
- Regroupez les ressources cibles du DNS en un seul ensemble de ressources avec un contrôle de disponibilité.

La procédure suivante explique comment créer des ressources cibles DNS et obtenir des recommandations d'architecture pour votre application.

Pour obtenir des recommandations concernant la mise à jour de votre architecture

1. Ouvrez la console Route 53 ARC à l'adressehttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Choisissez Readiness check.
3. Sous Nom du groupe de restauration, choisissez le groupe de restauration qui représente votre application.
4. Sur la page des détails du groupe de restauration, dans le menu Action, choisissez Obtenir les recommandations d'architecture pour ce groupe de restauration.
5. Si vous n'avez pas encore créé de test de disponibilité des ressources cibles DNS, créez-en un afin que Route 53 ARC puisse fournir des recommandations d'architecture. Choisissez Créer une ressource cible DNS.

   Pour plus d'informations sur les ressources cibles DNS, consultezComposants de contrôle de préparation .
6. Pour créer un ensemble de ressources pour une ressource cible DNS, vous devez créer un contrôle de disponibilité. Entrez un nom pour le contrôle de disponibilité, puis, pour le type de contrôle de préparation, choisissez la ressource cible DNS.

7. Entrez un nom pour l'ensemble de ressources.
8. Entrez les attributs de votre application, notamment le nom DNS, l'ARN de la zone hébergée et l'ID du jeu d'enregistrements.

   > **Tip**
   >
   > Pour connaître le format de l'ARN d'une zone hébergée, consultez la section Format de l'ARN de la zone hébergée dans Types de ressources et formats ARN dans Route 53 ARC.

   Facultativement, mais fortement recommandé, choisissez Add optional attribute et fournissez un Network Load Balancer ARN ou l'enregistrement de ressource Route 53 de votre domaine.
9. (Facultatif) Dans la configuration du groupe de restauration, choisissez une cellule pour votre ressource cible DNS afin de définir le niveau de disponibilité.
10. Choisissez Créer un ensemble de ressources.
11. Sur la page des détails du groupe de restauration, choisissez Obtenir des recommandations d'architecture. Route 53 ARC affiche un ensemble de recommandations sur la page.

Consultez la liste des recommandations. Vous pouvez ensuite décider si et comment apporter des modifications pour améliorer la résilience de restauration de votre application.

Création d'autorisations entre comptes dans Route 53 ARC

Vos ressources peuvent être réparties sur plusieurs AWS comptes, ce qui peut compliquer l'obtention d'une vue complète de l'état de santé de votre application. Il peut également être difficile d'obtenir les informations nécessaires pour prendre des décisions rapides. Pour rationaliser cette procédure de vérification de l'état de préparation dans Amazon Route 53 Application Recovery Controller, vous pouvez utiliser l'autorisation entre comptes.

L'autorisation entre comptes dans Route 53 ARC fonctionne avec la fonction de vérification de l'état de préparation. Avec l'autorisation entre comptes, vous pouvez utiliser un AWS compte central pour surveiller vos ressources situées dans plusieurs AWS comptes. Dans chaque compte contenant des ressources que vous souhaitez surveiller, vous autorisez le compte central à accéder à ces ressources. Le compte central peut ensuite créer des contrôles de disponibilité pour les ressources de tous les comptes et, à partir du compte central, vous pouvez contrôler l'état de préparation en cas de basculement.

> **Note**
>
> La configuration des autorisations entre comptes n'est pas disponible dans la console. Utilisez plutôt les opérations de l'API ARC Route 53 pour configurer et utiliser l'autorisation entre comptes. Pour vous aider à démarrer, cette section fournit des exemples de AWS CLI commandes.

Supposons qu'une application possède un compte contenant des ressources dans la région USA Ouest (Oregon) (us-west-2), et qu'il existe également un compte contenant des ressources que vous souhaitez surveiller dans la région USA Est (Virginie du Nord) (us-east-1). Route 53 ARC peut vous permettre de surveiller les deux ensembles de ressources à partir d'un seul compte, us-west-2, en utilisant l'autorisation entre comptes.

Imaginons, par exemple, que vous possédez les AWS comptes suivants :

- Compte US-West : 999999999999
- Compte US-Est : 111111111111

Dans le compte us-east-1 (111111111111), nous pouvons activer l'autorisation multi-comptes pour autoriser l'accès par le compte us-west-2 (99999999999999) en spécifiant le nom de ressource Amazon (ARN) pour l'utilisateur (root) dans le compte IAM us-west-2 :. `arn:aws:iam::999999999999:root` Une fois l'autorisation créée, le compte us-west-2 peut ajouter des ressources appartenant à us-east-1 aux ensembles de ressources et créer des contrôles de préparation à exécuter sur les ensembles de ressources.

L'exemple suivant illustre la configuration de l'autorisation entre comptes pour un compte. Vous devez activer l'autorisation entre comptes dans chaque compte supplémentaire contenant AWS des ressources que vous souhaitez ajouter et surveiller dans Route 53 ARC.

> **Note**
>
> Route 53 ARC est un service mondial qui prend en charge les points de terminaison dans plusieurs AWS régions, mais vous devez spécifier la région USA Ouest (Oregon) (c'est-à-dire spécifier le paramètre`--region us-west-2`) dans la plupart des commandes de la CLI Route 53 ARC.

La AWS CLI commande suivante montre comment configurer l'autorisation entre comptes pour cet exemple :

```
aws route53-recovery-readiness --region us-west-2 --profile profile-in-us-east-1-
account \
    create-cross-account-authorization --cross-account-authorization
 arn:aws:iam::999999999999:root
```

Pour désactiver cette autorisation, procédez comme suit :

```
aws route53-recovery-readiness --region us-west-2 --profile profile-in-us-east-1-
account \
    delete-cross-account-authorization --cross-account-authorization
 arn:aws:iam::999999999999:root
```

Pour enregistrer un compte spécifique pour tous les comptes pour lesquels vous avez fourni une autorisation multicompte, utilisez la `list-cross-account-authorizations` commande. Notez qu'à l'heure actuelle, vous ne pouvez pas vérifier dans l'autre sens. En d'autres termes, il n'existe aucune opération d'API que vous pouvez utiliser avec un profil de compte pour répertorier tous les comptes pour lesquels il a été autorisé à ajouter et à surveiller des ressources entre comptes.

```
aws route53-recovery-readiness --region us-west-2 --profile profile-in-us-east-1-
account \
    list-cross-account-authorizations
```

```
{
    "CrossAccountAuthorizations": [
        "arn:aws:iam::999999999999:root"
    ]
}
```

Règles de préparation, types de ressources et ARNS

Cette section inclut des informations de référence sur les descriptions des règles de préparation, les types de ressources pris en charge et le format des Amazon Resource Names (ARN) que vous utilisez pour les ensembles de ressources.

Descriptions des règles de préparation dans Route 53 ARC

Cette section répertorie les descriptions des règles de préparation pour tous les types de ressources pris en charge par Amazon Route 53 Application Recovery Controller. Pour consulter la liste des types de ressources pris en charge par Route 53 ARC, consultezTypes de ressources et formats ARN dans Route 53 ARC.

Vous pouvez également consulter les descriptions des règles de préparation sur la console Route 53 ARC ou à l'aide d'une opération d'API, en procédant comme suit :

- Pour afficher les règles de préparation dans la console, suivez les étapes de la procédure suivante :Afficher les règles de préparation sur la console.
- Pour consulter les règles de préparation à l'aide de l'API, consultez l'ListRulesopération.

Rubriques

Règles de préparation dans Route 53 ARC

Cette section répertorie l'ensemble des règles de préparation pour chaque type de ressource pris en charge par Route 53 ARC.

En parcourant les descriptions des règles, vous pouvez constater que la plupart d'entre elles incluent les termes Inspecte tout ou Inspecte chacune. Pour comprendre comment ces termes expliquent le fonctionnement d'une règle dans le contexte d'un contrôle de préparation, et pour obtenir d'autres informations sur la manière dont Route 53 ARC définit l'état de préparation, voir Comment les règles de préparation déterminent l'état de préparation.

Règles de préparation

Route 53 ARC audite les ressources en utilisant les règles de préparation suivantes.

Étapes de la version 1 d'Amazon API Gateway

- ApiGwV1ApiKeyCount: inspecte toutes les étapes d'API Gateway pour s'assurer qu'elles sont associées au même nombre de clés d'API.
- ApiGwV1ApiKeySource: Inspecte toutes les étapes d'API Gateway pour s'assurer qu'elles ont la même valeur pour`API Key Source`.

- ApiGwV1BasePath: Inspecte toutes les étapes d'API Gateway pour s'assurer qu'elles sont liées au même chemin de base.
- ApiGwV1BinaryMediaTypes: inspecte tous les stages d'API Gateway pour s'assurer qu'ils prennent en charge les mêmes types de supports binaires.
- ApiGwV1CacheClusterEnabled: inspecte toutes les étapes de l'API Gateway pour s'assurer qu'elles sont toutes `Cache Cluster` activées ou qu'aucune ne l'est.
- ApiGwV1CacheClusterSize: inspecte toutes les étapes de l'API Gateway pour s'assurer qu'elles sont identiques`Cache Cluster Size`. Si l'un d'entre eux a une valeur supérieure, les autres sont marqués comme NON PRÊTS.
- ApiGwV1CacheClusterStatus: Inspecte toutes les étapes de l'API Gateway pour s'assurer qu'elles `Cache Cluster` sont dans l'état AVAILABLE.
- ApiGwV1DisableExecuteApiEndpoint: inspecte toutes les étapes de l'API Gateway pour s'assurer qu'elles sont toutes `Execute API Endpoint` désactivées ou qu'aucune ne l'est.
- ApiGwV1DomainName: inspecte toutes les étapes de l'API Gateway pour s'assurer qu'elles sont liées au même nom de domaine.
- ApiGwV1EndpointConfiguration: Inspecte toutes les étapes d'API Gateway pour s'assurer qu'elles sont liées à un domaine avec la même configuration de point de terminaison.
- ApiGwV1EndpointDomainNameStatus: Inspecte toutes les étapes de l'API Gateway pour s'assurer que le nom de domaine auquel elles sont liées est à l'état DISPONIBLE.
- ApiGwV1MethodSettings: Inspecte toutes les étapes d'API Gateway pour s'assurer qu'elles ont la même valeur pour`Method Settings`.
- ApiGwV1MutualTlsAuthentication: Inspecte toutes les étapes d'API Gateway pour s'assurer qu'elles ont la même valeur pour`Mutual TLS Authentication`.
- ApiGwV1Policy: inspecte toutes les étapes d'API Gateway pour s'assurer qu'elles utilisent toutes des politiques au niveau de l'API ou qu'aucune ne le fait.
- ApiGwV1RegionalDomainName: Inspecte toutes les étapes de l'API Gateway pour s'assurer qu'elles sont liées au même nom de domaine régional. Remarque : Cette règle n'a aucune incidence sur l'état de préparation.
- ApiGwV1ResourceMethodConfigs: inspecte toutes les étapes d'API Gateway pour s'assurer qu'elles possèdent une hiérarchie de ressources similaire, y compris les configurations associées.
- ApiGwV1SecurityPolicy: Inspecte toutes les étapes d'API Gateway pour s'assurer qu'elles ont la même valeur pour`Security Policy`.

- ApiGwV1Quotas: Inspecte tous les groupes API Gateway pour s'assurer qu'ils sont conformes aux quotas (limites) gérés par Service Quotas.
- ApiGwV1UsagePlans: Inspecte toutes les étapes d'API Gateway pour s'assurer qu'elles sont liées `Usage Plans` à la même configuration.

Amazon API Gateway version 2 étapes

- ApiGwV2ApiKeySelectionExpression: inspecte toutes les étapes d'API Gateway pour s'assurer qu'elles ont la même valeur pour`API Key Selection Expression`.
- ApiGwV2ApiMappingSelectionExpression: Inspecte toutes les étapes d'API Gateway pour s'assurer qu'elles ont la même valeur pour`API Mapping Selection Expression`.
- ApiGwV2CorsConfiguration: Inspecte toutes les étapes d'API Gateway pour s'assurer qu'elles ont la même configuration liée au CORS.
- ApiGwV2DomainName: inspecte toutes les étapes de l'API Gateway pour s'assurer qu'elles sont liées au même nom de domaine.
- ApiGwV2DomainNameStatus: Inspecte toutes les étapes de l'API Gateway pour s'assurer que le nom de domaine est à l'état DISPONIBLE.
- ApiGwV2EndpointType: Inspecte toutes les étapes d'API Gateway pour s'assurer qu'elles ont la même valeur pour`Endpoint Type`.
- ApiGwV2Quotas: Inspecte tous les groupes API Gateway pour s'assurer qu'ils sont conformes aux quotas (limites) gérés par Service Quotas.
- ApiGwV2MutualTlsAuthentication: Inspecte toutes les étapes d'API Gateway pour s'assurer qu'elles ont la même valeur pour`Mutual TLS Authentication`.
- ApiGwV2ProtocolType: Inspecte toutes les étapes d'API Gateway pour s'assurer qu'elles ont la même valeur pour`Protocol Type`.
- ApiGwV2RouteConfigs: Inspecte toutes les étapes d'API Gateway pour s'assurer qu'elles possèdent la même hiérarchie de routes avec la même configuration.
- ApiGwV2RouteSelectionExpression: Inspecte toutes les étapes d'API Gateway pour s'assurer qu'elles ont la même valeur pour`Route Selection Expression`.
- ApiGwV2RouteSettings: Inspecte toutes les étapes d'API Gateway pour s'assurer qu'elles ont la même valeur pour`Default Route Settings`.
- ApiGwV2SecurityPolicy: Inspecte toutes les étapes d'API Gateway pour s'assurer qu'elles ont la même valeur pour`Security Policy`.
- ApiGwV2StageVariables: Inspecte toutes les étapes d'API Gateway pour s'assurer qu'elles sont toutes identiques `Stage Variables` aux autres étapes.

- ApiGwV2ThrottlingBurstLimit: Inspecte toutes les étapes d'API Gateway pour s'assurer qu'elles ont la même valeur pour`Throttling Burst Limit`.
- ApiGwV2ThrottlingRateLimit: Inspecte toutes les étapes d'API Gateway pour s'assurer qu'elles ont la même valeur pour`Throttling Rate Limit`.

Clusters Amazon Aurora

- RdsClusterStatus: Inspecte chaque cluster Aurora pour s'assurer qu'il possède un statut de l'un `AVAILABLE` ou `BACKING-UP` de l'autre.
- RdsEngineMode: Inspecte tous les clusters Aurora pour s'assurer qu'ils ont la même valeur pour`Engine Mode`.
- RdsEngineVersion: Inspecte tous les clusters Aurora pour s'assurer qu'ils ont la même valeur pour`Major Version`.
- RdsGlobalReplicaLag: Inspecte chaque cluster Aurora pour s'assurer qu'il dispose `Global Replica Lag` d'une durée inférieure à 30 secondes.
- RdsNormalizedCapacity: inspecte tous les clusters Aurora pour s'assurer qu'ils ont une capacité normalisée inférieure à 15 % du maximum de l'ensemble de ressources.
- RdsInstanceType: Inspecte tous les clusters Aurora pour s'assurer qu'ils possèdent les mêmes types d'instances.
- RdsQuotas: Inspecte tous les clusters Aurora pour s'assurer qu'ils sont conformes aux quotas (limites) gérés par Service Quotas.

Groupes Auto Scaling

- AsgMinSizeAndMaxSize: Inspecte tous les groupes Auto Scaling pour s'assurer qu'ils ont les mêmes tailles de groupe minimale et maximale.
- AsgAZCount: Inspecte tous les groupes Auto Scaling pour s'assurer qu'ils possèdent le même nombre de zones de disponibilité.
- AsgInstanceTypes: Inspecte tous les groupes Auto Scaling pour s'assurer qu'ils possèdent les mêmes types d'instances. Remarque : Cette règle n'a aucune incidence sur l'état de préparation.
- AsgInstanceSizes: Inspecte tous les groupes Auto Scaling pour s'assurer qu'ils ont les mêmes tailles d'instance.
- AsgNormalizedCapacity: Inspecte tous les groupes Auto Scaling pour s'assurer qu'ils ont une capacité normalisée inférieure à 15 % du maximum de l'ensemble de ressources.
- AsgQuotas: Inspecte tous les groupes Auto Scaling pour s'assurer qu'ils sont conformes aux quotas (limites) gérés par Service Quotas.

CloudWatch alarmes

- CloudWatchAlarmState: Inspecte les CloudWatch alarmes pour s'assurer que chacune d'elles n'est pas à l'`INSUFFICIENT_DATA`état `ALARM` OR.

Passerelles pour clients

- CustomerGatewayIpAddress: inspecte toutes les passerelles des clients pour s'assurer qu'elles possèdent la même adresse IP.
- CustomerGatewayState: Inspecte les passerelles des clients pour s'assurer que chacune d'entre elles est conforme à l'`AVAILABLE`état.
- CustomerGatewayVPNType: inspecte toutes les passerelles des clients pour s'assurer qu'elles disposent du même type de VPN.

DNS target resources

- DnsTargetResourceHostedZoneConfigurationRule: inspecte toutes les ressources cibles DNS pour s'assurer qu'elles ont le même identifiant de zone hébergée Amazon Route 53 et que chaque zone hébergée n'est pas privée. Remarque : Cette règle n'a aucune incidence sur l'état de préparation.
- DnsTargetResourceRecordSetConfigurationRule: inspecte toutes les ressources cibles DNS pour s'assurer qu'elles ont la même durée de vie du cache d'enregistrement des ressources (TTL) et que les TTL sont inférieurs ou égaux à 300.
- DnsTargetResourceRoutingRule: inspecte chaque ressource cible DNS associée à un ensemble d'enregistrements de ressources d'alias pour s'assurer qu'elle achemine le trafic vers le nom DNS configuré sur la ressource cible. Remarque : Cette règle n'a aucune incidence sur l'état de préparation.
- DnsTargetResourceHealthCheckRule: Inspecte toutes les ressources cibles du DNS pour s'assurer que les contrôles de santé sont associés à leurs ensembles d'enregistrements de ressources, le cas échéant et non autrement. Remarque : Cette règle n'a aucune incidence sur l'état de préparation.

Tables Amazon DynamoDB

- DynamoConfiguration: inspecte toutes les tables DynamoDB pour s'assurer qu'elles possèdent les mêmes clés, attributs, chiffrement côté serveur et configurations de flux.
- DynamoTableStatus: inspecte chaque table DynamoDB pour s'assurer qu'elle a le statut ACTIF.
- DynamoCapacity: inspecte toutes les tables DynamoDB pour s'assurer que leurs capacités de lecture et d'écriture allouées se situent dans les 20 % des capacités maximales de l'ensemble de ressources.

- DynamoPeakRcuWcu: inspecte chaque table DynamoDB pour s'assurer qu'elle a connu un pic de trafic similaire à celui des autres tables, afin de garantir la capacité allouée.
- DynamoGsiPeakRcuWcu: inspecte chaque table DynamoDB pour s'assurer qu'elle possède une capacité maximale de lecture et d'écriture similaire à celle des autres tables, afin de garantir la capacité allouée.
- DynamoGsiConfig: inspecte toutes les tables DynamoDB dotées d'index secondaires globaux pour s'assurer qu'elles utilisent le même index, le même schéma de clé et la même projection.
- DynamoGsiStatus: inspecte toutes les tables DynamoDB dotées d'index secondaires globaux pour s'assurer que les index secondaires globaux ont le statut ACTIF.
- DynamoGsiCapacity: inspecte toutes les tables DynamoDB dotées d'index secondaires globaux pour s'assurer que les tables ont des capacités de lecture et d'écriture GSI allouées dans des limites de 20 % des capacités maximales de l'ensemble de ressources.
- DynamoReplicationLatency: inspecte toutes les tables DynamoDB qui sont des tables globales pour s'assurer qu'elles ont la même latence de réplication.
- DynamoAutoScalingConfiguration: Inspecte toutes les tables DynamoDB sur lesquelles Auto Scaling est activé pour s'assurer qu'elles ont les mêmes capacités de lecture et d'écriture minimales, maximales et cibles.
- DynamoQuotas: inspecte toutes les tables DynamoDB pour s'assurer qu'elles sont conformes aux quotas (limites) gérés par Service Quotas.

Elastic Load Balancing (équilibreurs de charge classiques)

- ElbV1CheckAzCount: Inspecte chaque Classic Load Balancer pour s'assurer qu'il est rattaché à une seule zone de disponibilité. Remarque : Cette règle n'a aucune incidence sur l'état de préparation.
- ElbV1AnyInstances: inspecte tous les équilibreurs de charge classiques pour s'assurer qu'ils disposent d'au moins une instance EC2.
- ElbV1AnyInstancesHealthy: inspecte tous les équilibreurs de charge classiques pour s'assurer qu'ils disposent d'au moins une instance EC2 saine.
- ElbV1Scheme: inspecte tous les équilibreurs de charge classiques pour s'assurer qu'ils utilisent le même schéma d'équilibrage de charge.
- ElbV1HealthCheckThreshold: inspecte tous les équilibreurs de charge classiques pour s'assurer qu'ils ont la même valeur de seuil de contrôle de santé.
- ElbV1HealthCheckInterval: Inspecte tous les équilibreurs de charge classiques pour s'assurer qu'ils ont la même valeur d'intervalle de contrôle de santé.

- ElbV1CrossZoneRoutingEnabled: Inspecte tous les équilibreurs de charge classiques pour s'assurer qu'ils ont la même valeur pour l'équilibrage de charge entre zones (ACTIVÉ ou DÉSACTIVÉ).
- ElbV1AccessLogsEnabledAttribute: Inspecte tous les équilibreurs de charge classiques pour s'assurer qu'ils ont la même valeur pour les journaux d'accès (ENABLED ou DISABLED).
- ElbV1ConnectionDrainingEnabledAttribute: Inspecte tous les équilibreurs de charge classiques pour s'assurer qu'ils ont la même valeur pour la vidange de la connexion (ENABLED ou DISABLED).
- ElbV1ConnectionDrainingTimeoutAttribute: Inspecte tous les équilibreurs de charge classiques pour s'assurer qu'ils ont la même valeur de délai d'expiration de la connexion.
- ElbV1IdleTimeoutAttribute: Inspecte tous les équilibreurs de charge classiques pour s'assurer qu'ils ont la même valeur de délai d'inactivité.
- ElbV1ProvisionedCapacityLcuCount: inspecte tous les équilibreurs de charge classiques dotés d'une LCU provisionnée supérieure à 10 pour s'assurer qu'ils se situent dans les 20 % de la LCU provisionnée la plus élevée de l'ensemble de ressources.
- ElbV1ProvisionedCapacityStatus: inspecte l'état de la capacité allouée sur chaque Classic Load Balancer pour s'assurer qu'il n'a pas la valeur DISABLED ou PENDING.

Volumes Amazon EBS

- EbsVolumeEncryption: inspecte tous les EBS volumes pour s'assurer qu'ils ont la même valeur de chiffrement (ENABLED ou DISABLED).
- EbsVolumeEncryptionDefault: inspecte tous les EBS volumes pour s'assurer qu'ils ont la même valeur de chiffrement par défaut (ENABLED ou DISABLED).
- EbsVolumeIops: Inspecte tous les EBS volumes pour s'assurer qu'ils ont les mêmes opérations d'entrée/sortie par seconde (IOPS).
- EbsVolumeKmsKeyId: inspecte tous les EBS volumes pour s'assurer qu'ils possèdent le même identifiant de AWS KMS clé par défaut.
- EbsVolumeMultiAttach: inspecte tous les EBS volumes pour s'assurer qu'ils ont la même valeur pour l'attachement multiple (ENABLED ou DISABLED).
- EbsVolumeQuotas: Inspecte tous les EBS volumes pour s'assurer qu'ils sont conformes aux quotas (limites) définis par Service Quotas.
- EbsVolumeSize: inspecte tous les EBS volumes pour s'assurer qu'ils ont la même taille lisible.
- EbsVolumeState: inspecte tous les EBS volumes pour s'assurer qu'ils ont le même état de volume.

- EbsVolumeType: inspecte tous les EBS volumes pour s'assurer qu'ils ont le même type de volume.

AWS Lambda fonctions

- LambdaMemorySize: inspecte toutes les fonctions Lambda pour s'assurer qu'elles ont la même taille de mémoire. Si l'un d'entre eux possède plus de mémoire, les autres sont marqués`NOT READY`.
- LambdaFunctionTimeout: Inspecte toutes les fonctions Lambda pour s'assurer qu'elles ont la même valeur de délai d'expiration. Si l'un d'eux a une valeur supérieure, les autres sont marqués`NOT READY`.
- LambdaFunctionRuntime: Inspecte toutes les fonctions Lambda pour s'assurer qu'elles ont toutes le même temps d'exécution.
- LambdaFunctionReservedConcurrentExecutions: Inspecte toutes les fonctions Lambda pour s'assurer qu'elles ont toutes la même valeur pour. `Reserved Concurrent Executions` Si l'un d'eux a une valeur supérieure, les autres sont marqués`NOT READY`.
- LambdaFunctionDeadLetterConfig: Inspecte toutes les fonctions Lambda pour s'assurer qu'elles ont toutes `Dead Letter Config` une définition ou qu'aucune d'entre elles n'en a une.
- LambdaFunctionProvisionedConcurrencyConfig: Inspecte toutes les fonctions Lambda pour s'assurer qu'elles ont la même valeur pour. `Provisioned Concurrency`
- LambdaFunctionSecurityGroupCount: Inspecte toutes les fonctions Lambda pour s'assurer qu'elles ont la même valeur pour. `Security Groups`
- LambdaFunctionSubnetIdCount: Inspecte toutes les fonctions Lambda pour s'assurer qu'elles ont la même valeur pour. `Subnet Ids`
- LambdaFunctionEventSourceMappingMatch: Inspecte toutes les fonctions Lambda pour s'assurer que toutes les propriétés `Event Source Mapping` choisies correspondent entre elles.
- LambdaFunctionLimitsRule: Inspecte toutes les fonctions Lambda pour s'assurer qu'elles sont conformes aux quotas (limites) gérés par Service Quotas.

Équilibreurs de charge réseau et équilibreurs de charge d'applications

- ElbV2CheckAzCount: inspecte chaque Network Load Balancer pour s'assurer qu'il est rattaché à une seule zone de disponibilité. Remarque : Cette règle n'a aucune incidence sur l'état de préparation.
- ElbV2TargetGroupsCanServeTraffic: Inspecte chaque Network Load Balancer et Application Load Balancer pour s'assurer qu'il possède au moins une instance Amazon EC2 saine.

- ElbV2State: Inspecte chaque Network Load Balancer et Application Load Balancer pour s'assurer qu'ils sont en bon état. `ACTIVE`
- ElbV2IpAddressType: inspecte tous les équilibreurs de charge réseau et les équilibreurs de charge d'application pour s'assurer qu'ils possèdent les mêmes types d'adresses IP.
- ElbV2Scheme: inspecte tous les équilibreurs de charge réseau et les équilibreurs de charge d'application pour s'assurer qu'ils utilisent le même schéma.
- ElbV2Type: inspecte tous les équilibreurs de charge réseau et les équilibreurs de charge d'application pour s'assurer qu'ils sont du même type.
- ElbV2S3LogsEnabled: inspecte tous les équilibreurs de charge réseau et les équilibreurs de charge d'application pour s'assurer qu'ils ont la même valeur pour les journaux d'accès au serveur Amazon S3 (ENABLED ou DISABLED).
- ElbV2DeletionProtection: inspecte tous les équilibreurs de charge réseau et les équilibreurs de charge d'application pour s'assurer qu'ils ont la même valeur de protection contre la suppression (ENABLED ou DISABLED).
- ElbV2IdleTimeoutSeconds: Inspecte tous les équilibreurs de charge réseau et les équilibreurs de charge d'application pour s'assurer qu'ils ont la même valeur pendant les secondes d'inactivité.
- ElbV2HttpDropInvalidHeaders: Inspecte tous les équilibreurs de charge réseau et les équilibreurs de charge d'application pour s'assurer qu'ils ont la même valeur pour les en-têtes non valides HTTP.
- ElbV2Http2Enabled: inspecte tous les équilibreurs de charge réseau et les équilibreurs de charge d'application pour s'assurer qu'ils ont la même valeur pour le protocole HTTP/2 (ACTIVÉ ou DÉSACTIVÉ).
- ElbV2CrossZoneEnabled: inspecte tous les équilibreurs de charge réseau et les équilibreurs de charge d'application pour s'assurer qu'ils ont la même valeur pour l'équilibrage de charge entre zones (ACTIVÉ ou DÉSACTIVÉ).
- ElbV2ProvisionedCapacityLcuCount: Inspecte tous les équilibreurs de charge réseau et les équilibreurs de charge d'application dotés d'une LCU provisionnée supérieure à 10 pour s'assurer qu'ils se situent dans les 20 % de la LCU la plus élevée de l'ensemble de ressources.
- ElbV2ProvisionedCapacityEnabled: inspecte l'état de capacité de tous les équilibreurs de charge réseau et d'application provisionnés pour s'assurer qu'il n'a pas la valeur DISABLED ou PENDING.

Clusters Amazon MSK

- MskClusterClientSubnet: Inspecte chaque cluster MSK pour s'assurer qu'il ne possède que deux ou trois sous-réseaux clients.
- MskClusterInstanceType: Inspecte tous les clusters MSK pour s'assurer qu'ils possèdent le même type d'instance Amazon EC2.
- MskClusterSecurityGroups: Inspecte tous les clusters MSK pour s'assurer qu'ils possèdent les mêmes groupes de sécurité.
- MskClusterStorageInfo: Inspecte tous les clusters MSK pour s'assurer qu'ils ont la même taille de volume de stockage EBS. Si l'un d'entre eux a une valeur supérieure, les autres sont marqués comme NON PRÊTS.
- MskClusterACMCertificate: Inspecte tous les clusters MSK pour s'assurer qu'ils possèdent la même liste d'ARN de certificats d'autorisation client.
- MskClusterServerProperties: Inspecte tous les clusters MSK pour s'assurer qu'ils ont la même valeur pour. `Current Broker Software Info`
- MskClusterKafkaVersion: Inspecte tous les clusters MSK pour s'assurer qu'ils possèdent la même version de Kafka.
- MskClusterEncryptionInTransitInCluster: Inspecte tous les clusters MSK pour s'assurer qu'ils ont la même valeur pour. `Encryption In Transit In Cluster`
- MskClusterEncryptionInClientBroker: Inspecte tous les clusters MSK pour s'assurer qu'ils ont la même valeur pour. `Encryption In Transit Client Broker`
- MskClusterEnhancedMonitoring: Inspecte tous les clusters MSK pour s'assurer qu'ils ont la même valeur pour. `Enhanced Monitoring`
- MskClusterOpenMonitoringInJmx: Inspecte tous les clusters MSK pour s'assurer qu'ils ont la même valeur pour. `Open Monitoring JMX Exporter`
- MskClusterOpenMonitoringInNode: Inspecte tous les clusters MSK pour s'assurer qu'ils ont la même valeur pour `Open Monitoring Not Exporter.`
- MskClusterLoggingInS3: Inspecte tous les clusters MSK pour s'assurer qu'ils ont la même valeur pour. `Is Logging in S3`
- MskClusterLoggingInFirehose: Inspecte tous les clusters MSK pour s'assurer qu'ils ont la même valeur pour. `Is Logging In Firehose`
- MskClusterLoggingInCloudWatch: Inspecte tous les clusters MSK pour s'assurer qu'ils ont la même valeur pour. `Is Logging Available In CloudWatch Logs`

- MskClusterNumberOfBrokerNodes: Inspecte tous les clusters MSK pour s'assurer qu'ils ont la même valeur pour. `Number of Broker Nodes` Si l'un d'entre eux a une valeur supérieure, les autres sont marqués comme NON PRÊTS.
- MskClusterState: Inspecte chaque cluster MSK pour s'assurer qu'il est dans un état ACTIF.
- MskClusterLimitsRule: Inspecte toutes les fonctions Lambda pour s'assurer qu'elles sont conformes aux quotas (limites) gérés par Service Quotas.

Contrôles de santé d'Amazon Route 53

- R53HealthCheckType: Inspecte chaque bilan de santé de la Route 53 pour s'assurer qu'il n'est pas du type CALCULÉ et que tous les contrôles sont du même type.
- R53HealthCheckDisabled: Inspecte chaque bilan de santé de la Route 53 pour s'assurer qu'il ne présente pas l'état DÉSACTIVÉ.
- R53HealthCheckStatus: Inspecte chaque bilan de santé de la Route 53 pour s'assurer qu'il a le statut SUCCESS.
- R53HealthCheckRequestInterval: Inspecte tous les bilans de santé de la Route 53 pour s'assurer qu'ils ont tous la même valeur pour`Request Interval`.
- R53HealthCheckFailureThreshold: Inspecte tous les bilans de santé de la Route 53 pour s'assurer qu'ils ont tous la même valeur pour `Failure Threshold.`
- R53HealthCheckEnableSNI: Inspecte tous les bilans de santé de la Route 53 pour s'assurer qu'ils ont tous la même valeur pour `Enable SNI.`
- R53HealthCheckSearchString: Inspecte tous les bilans de santé de la Route 53 pour s'assurer qu'ils ont tous la même valeur pour `Search String.`
- R53HealthCheckRegions: Inspecte tous les bilans de santé de la Route 53 pour s'assurer qu'ils comportent tous la même liste de AWS régions.
- R53HealthCheckMeasureLatency: Inspecte tous les bilans de santé de la Route 53 pour s'assurer qu'ils ont tous la même valeur pour`Measure Latency`.
- R53HealthCheckInsufficientDataHealthStatus: Inspecte tous les bilans de santé de la Route 53 pour s'assurer qu'ils ont tous la même valeur pour`Insufficient Data Health Status`.
- R53HealthCheckInverted: Inspecte tous les bilans de santé de la Route 53 pour s'assurer qu'ils sont tous inversés ou qu'ils ne le sont pas.
- R53HealthCheckResourcePath: Inspecte tous les bilans de santé de la Route 53 pour s'assurer qu'ils ont tous la même valeur pour`Resource Path`.

- R53HealthCheckCloudWatchAlarm: Inspecte tous les bilans de santé de la Route 53 pour s'assurer que les CloudWatch alarmes qui leur sont associées ont les mêmes paramètres et configurations.

Abonnements Amazon SNS

- SnsSubscriptionProtocol: inspecte tous les abonnements SNS pour s'assurer qu'ils utilisent le même protocole.
- SnsSubscriptionSqsLambdaEndpoint: inspecte tous les abonnements SNS dotés de points de terminaison Lambda ou SQS pour s'assurer qu'ils ont des points de terminaison différents.
- SnsSubscriptionNonAwsEndpoint: inspecte tous les abonnements SNS dotés d'un type de point de terminaison non lié au AWS service, par exemple un e-mail, pour s'assurer qu'ils ont le même point de terminaison.
- SnsSubscriptionPendingConfirmation: inspecte tous les abonnements SNS pour s'assurer qu'ils ont la même valeur pour les « confirmations en attente ».
- SnsSubscriptionDeliveryPolicy: inspecte tous les abonnements SNS qui utilisent le protocole HTTP/S pour s'assurer qu'ils ont la même valeur pour « Période de livraison effective ».
- SnsSubscriptionRawMessageDelivery: inspecte tous les abonnements SNS pour s'assurer qu'ils ont la même valeur pour « Raw Message Delivery ».
- SnsSubscriptionFilter: Inspecte tous les abonnements SNS pour s'assurer qu'ils ont la même valeur pour « Politique de filtrage ».
- SnsSubscriptionRedrivePolicy: inspecte tous les abonnements SNS pour s'assurer qu'ils ont la même valeur pour « Redrive Policy ».
- SnsSubscriptionEndpointEnabled: inspecte tous les abonnements SNS pour s'assurer qu'ils ont la même valeur pour « Endpoint Enabled ».
- SnsSubscriptionLambdaEndpointValid: inspecte tous les abonnements SNS dotés de points de terminaison Lambda pour s'assurer qu'ils disposent de points de terminaison Lambda valides.
- SnsSubscriptionSqsEndpointValidRule: inspecte tous les abonnements SNS qui utilisent des points de terminaison SQS pour s'assurer qu'ils disposent de points de terminaison SQS valides.
- SnsSubscriptionQuotas: Inspecte tous les abonnements SNS pour s'assurer qu'ils sont conformes aux quotas (limites) gérés par Service Quotas.

Rubriques Amazon SNS

- SnsTopicDisplayName: inspecte toutes les rubriques SNS pour s'assurer qu'elles ont la même valeur pour. `Display Name`

- SnsTopicDeliveryPolicy: inspecte tous les sujets SNS auxquels des abonnés HTTPS sont abonnés pour s'assurer qu'ils ont les mêmes abonnés. `EffectiveDeliveryPolicy`
- SnsTopicSubscription: inspecte tous les sujets SNS pour s'assurer qu'ils ont le même nombre d'abonnés pour chacun de leurs protocoles.
- SnsTopicAwsKmsKey: Inspecte toutes les rubriques du SNS pour s'assurer que toutes les rubriques ou aucune d'entre elles n'ont de clé. AWS KMS
- SnsTopicQuotas: Inspecte toutes les rubriques SNS pour s'assurer qu'elles sont conformes aux quotas (limites) gérés par Service Quotas.

Files d'attente Amazon SQS

- SqsQueueType: inspecte toutes les files d'attente SQS pour s'assurer qu'elles ont toutes la même valeur pour. `Type`
- SqsQueueDelaySeconds: inspecte toutes les files d'attente SQS pour s'assurer qu'elles ont toutes la même valeur pour. `Delay Seconds`
- SqsQueueMaximumMessageSize: inspecte toutes les files d'attente SQS pour s'assurer qu'elles ont toutes la même valeur pour. `Maximum Message Size`
- SqsQueueMessageRetentionPeriod: inspecte toutes les files d'attente SQS pour s'assurer qu'elles ont toutes la même valeur pour. `Message Retention Period`
- SqsQueueReceiveMessageWaitTimeSeconds: inspecte toutes les files d'attente SQS pour s'assurer qu'elles ont toutes la même valeur pour. `Receive Message Wait Time Seconds`
- SqsQueueRedrivePolicyMaxReceiveCount: inspecte toutes les files d'attente SQS pour s'assurer qu'elles ont toutes la même valeur pour. `Redrive Policy Max Receive Count`
- SqsQueueVisibilityTimeout: inspecte toutes les files d'attente SQS pour s'assurer qu'elles ont toutes la même valeur pour. `Visibility Timeout`
- SqsQueueContentBasedDeduplication: inspecte toutes les files d'attente SQS pour s'assurer qu'elles ont toutes la même valeur pour. `Content-Based Deduplication`
- SqsQueueQuotas: Inspecte toutes les files d'attente SQS pour s'assurer qu'elles sont conformes aux quotas (limites) gérés par Service Quotas.

Amazon VPC

- VpcCidrBlock: Inspecte tous les VPC pour s'assurer qu'ils ont tous la même valeur pour la taille du réseau de blocs CIDR.
- VpcCidrBlocksSameProtocolVersion: Inspecte tous les VPC dotés des mêmes blocs CIDR pour s'assurer qu'ils ont la même valeur pour le numéro de version du protocole Internet Stream.

- VpcCidrBlocksStateInAssociationSets: Inspecte tous les ensembles d'associations de blocs CIDR pour tous les VPC afin de s'assurer qu'ils contiennent tous des blocs d'adresse CIDR dans un état. `ASSOCIATED`
- VpcIpv6CidrBlocksStateInAssociationSets: Inspecte tous les ensembles d'associations de blocs CIDR pour tous les VPC afin de s'assurer qu'ils possèdent tous des blocs d'adresse CIDR avec le même nombre d'adresses.
- VpcCidrBlocksInAssociationSets: Inspecte tous les ensembles d'associations de blocs CIDR pour tous les VPC afin de s'assurer qu'ils ont tous la même taille.
- VpcIpv6CidrBlocksInAssociationSets: Inspecte tous les ensembles d'associations de blocs d'adresse CIDR IPv6 pour tous les VPC afin de s'assurer qu'ils ont la même taille.
- VpcState: Inspecte chaque VPC pour s'assurer qu'il est dans `AVAILABLE` un état.
- VpcInstanceTenancy: Inspecte tous les VPC pour s'assurer qu'ils ont tous la même valeur pour. `Instance Tenancy`
- VpcIsDefault: Inspecte tous les VPC pour s'assurer qu'ils ont la même valeur pour `Is Default.`
- VpcSubnetState: Inspecte chaque sous-réseau VPC pour s'assurer qu'il est dans un état DISPONIBLE.
- VpcSubnetAvailableIpAddressCount: Inspecte chaque sous-réseau VPC pour s'assurer qu'il possède un nombre d'adresses IP disponibles supérieur à zéro.
- VpcSubnetCount: Inspecte tous les sous-réseaux VPC pour s'assurer qu'ils possèdent le même nombre de sous-réseaux.
- VpcQuotas: Inspecte tous les sous-réseaux VPC pour s'assurer qu'ils sont conformes aux quotas (limites) gérés par Service Quotas.

AWS VPN connexions

- VpnConnectionsRouteCount: inspecte toutes les connexions VPN pour s'assurer qu'elles comportent au moins un itinéraire, ainsi que le même nombre de routes.
- VpnConnectionsEnableAcceleration: inspecte toutes les connexions VPN pour s'assurer qu'elles ont la même valeur pour`Enable Accelerations`.
- VpnConnectionsStaticRoutesOnly: inspecte toutes les connexions VPN pour s'assurer qu'elles ont la même valeur pour `Static Routes Only.`
- VpnConnectionsCategory: inspecte toutes les connexions VPN pour s'assurer qu'elles correspondent à une catégorie de`VPN`.

- VpnConnectionsCustomerConfiguration: inspecte toutes les connexions VPN pour s'assurer qu'elles ont la même valeur pour`Customer Gateway Configuration`.
- VpnConnectionsCustomerGatewayId: inspecte chaque connexion VPN pour s'assurer qu'une passerelle client y est connectée.
- VpnConnectionsRoutesState: Inspecte toutes les connexions VPN pour s'assurer qu'elles sont en bon `AVAILABLE` état.
- VpnConnectionsVgwTelemetryStatus: inspecte chaque connexion VPN pour s'assurer qu'elle possède un statut VGW de. `UP`
- VpnConnectionsVgwTelemetryIpAddress: Inspecte chaque connexion VPN pour s'assurer qu'elle possède une adresse IP externe différente pour chaque télémétrie VGW.
- VpnConnectionsTunnelOptions: inspecte toutes les connexions VPN pour s'assurer qu'elles disposent des mêmes options de tunnel.
- VpnConnectionsRoutesCidr: inspecte toutes les connexions VPN pour s'assurer qu'elles ont les mêmes blocs d'adresse CIDR de destination.
- VpnConnectionsInstanceType: inspecte toutes les connexions VPN pour s'assurer qu'elles sont identiques`Instance Type`.

AWS VPN passerelles

- VpnGatewayState: Inspecte toutes les passerelles VPN pour s'assurer qu'elles sont dans l'état DISPONIBLE.
- VpnGatewayAsn: inspecte toutes les passerelles VPN pour s'assurer qu'elles ont le même ASN.
- VpnGatewayType: inspecte toutes les passerelles VPN pour s'assurer qu'elles sont du même type.
- VpnGatewayAttachment: inspecte toutes les passerelles VPN pour s'assurer qu'elles ont les mêmes configurations d'attachement.

Afficher les règles de préparation sur la console

Vous pouvez consulter les règles de préparation sur le AWS Management Console, répertoriées par type de ressource.

Pour consulter les règles de préparation sur la console

1. Ouvrez la console Route 53 ARC à l'adressehttps://console.aws.amazon.com/route53recovery/home#/dashboard.

2. Choisissez Readiness check.
3. Sous Type de ressource, choisissez le type de ressource pour lequel vous souhaitez consulter les règles.

Types de ressources et formats ARN dans Route 53 ARC

Lorsque vous créez un ensemble de ressources dans Amazon Route 53 Application Recovery Controller, vous spécifiez le type de ressource à inclure dans l'ensemble et les Amazon Resource Names (ARN) pour chacune des ressources à inclure. Route 53 ARC attend un format d'ARN spécifique pour chaque type de ressource. Cette section répertorie les types de ressources pris en charge par Route 53 ARC et les formats ARN associés pour chacun d'entre eux.

Le format spécifique dépend de la ressource. Lorsque vous fournissez un ARN, remplacez le texte en *italique* par des informations spécifiques à votre ressource.

> **Note**
>
> Sachez que le format ARN requis par Route 53 ARC pour les ressources peut être différent du format ARN dont un service lui-même a besoin pour ses ressources. Par exemple, les formats ARN décrits dans les sections relatives aux types de ressources pour chaque service de la référence d'autorisation de service peuvent ne pas inclure l' Compte AWS ID ou les autres informations dont Route 53 ARC a besoin pour prendre en charge les fonctionnalités du service Route 53 ARC.

AWS::ApiGateway::Stage

Une étape Amazon API Gateway version 1.

- Format de l'ARN : `arn:`*`partition`*`:apigateway:`*`region`*`:`*`account`*`:/restapis/`*`api-id`*`/stages/`*`stage-name`*

  Exemple : `arn:aws:apigateway:us-east-1:111122223333:/restapis/123456789/stages/ExampleStage`

  Pour plus d'informations, consultez la référence API Gateway Amazon Resource Name (ARN).

AWS::ApiGatewayV2::Stage

Une étape Amazon API Gateway version 2.

- Format de l'ARN : `arn:partition:apigateway:region:account:/apis/api-id/stages/stage-name`

  Exemple : `arn:aws:apigateway:us-east-1:111122223333:/apis/123456789/stages/ExampleStage`

  Pour plus d'informations, consultez la référence API Gateway Amazon Resource Name (ARN).

AWS::CloudWatch::Alarm

Une CloudWatch alarme Amazon.

- Format de l'ARN : `arn:partition:cloudwatch:region:account:alarm:alarm-name`

  Exemple : `arn:aws:cloudwatch:us-west-2:111122223333:alarm:test-alarm-1`

  Pour plus d'informations, consultez la section Types de ressources définis par Amazon CloudWatch.

AWS::DynamoDB::Table

Une table Amazon DynamoDB.

- Format de l'ARN : `arn:partition:dynamodb:region:account:table/table-name`

  Exemple : `arn:aws:dynamodb:us-west-2:111122223333:table/BigTable`

  Pour plus d'informations, consultez la section Ressources et opérations DynamoDB.

AWS::EC2::CustomerGateway

Un dispositif de passerelle client.

- Format de l'ARN : `arn:partition:ec2:region:account:customer-gateway/CustomerGatewayId`

  Exemple : `arn:aws:ec2:us-west-2:111122223333:customer-gateway/vcg-123456789`

  Pour plus d'informations, consultez la section Types de ressources définis par Amazon EC2.

AWS::EC2::Volume

Un volume Amazon EBS.

- Format de l'ARN : `arn:partition:ec2:region:account:volume/VolumeId`

Exemple : `arn:aws:ec2:us-west-2:111122223333:volume/volume-of-cylinder-is-pi`

Pour plus d'informations, consultez la référence API Gateway Amazon Resource Name (ARN).

AWS::ElasticLoadBalancing::LoadBalancer

Un Classic Load Balancer.

- Format de l'ARN : `arn:partition:elasticloadbalancing:region:account:loadbalancer/LoadBalancerN`

  Exemple : `arn:aws:elasticloadbalancing:us-west-2:111122223333:loadbalancer/123456789abcbdeCLB`

  Pour plus d'informations, consultez les ressources d'Elastic Load Balancing.

AWS::ElasticLoadBalancingV2::LoadBalancer

Un Network Load Balancer ou un Application Load Balancer.

- Format ARN pour Network Load Balancer : `arn:partition:elasticloadbalancing:region:account:loadbalancer/net/LoadBalancerName`

  Exemple pour Network Load Balancer : `arn:aws:elasticloadbalancing:us-west-2:111122223333:loadbalancer/net/sandbox-net/123456789acbdeNLB`
- Format ARN pour Application Load Balancer : `arn:partition:elasticloadbalancing:region:account:loadbalancer/app/LoadBalancerName`

  Exemple pour Application Load Balancer : `arn:aws:elasticloadbalancing:us-west-2:111122223333:loadbalancer/app/sandbox-alb/123456789acbdeALB`

  Pour plus d'informations, consultez les ressources d'Elastic Load Balancing.

AWS::Lambda::Function

Une AWS Lambda fonction.

- Format de l'ARN : `arn:partition:lambda:region:account:function:FunctionName`

  Exemple : `arn:aws:lambda:us-west-2:111122223333:function:my-function`

Pour plus d'informations, consultez Ressources et conditions pour les actions Lambda.

AWS::MSK::Cluster

Un cluster Amazon MSK.

- Format de l'ARN : `arn:partition:kafka:region:account:cluster/ClusterName/UUID`

  Exemple : `arn:aws:kafka:us-east-1:111122223333:cluster/demo-cluster-1/123456-1111-2222-3333`

  Pour plus d'informations, consultez la section Types de ressources définis par Amazon Managed Streaming for Apache Kafka.

AWS::RDS::DBCluster

Un cluster de base de données Aurora.

- Format de l'ARN : `arn:partition:rds:region:account:cluster:DbClusterInstanceName`

  Exemple : `arn:aws:rds:us-west-2:111122223333:cluster:database-1`

  Pour plus d'informations, consultez Travailler avec les Amazon Resource Names (ARN) dans Amazon RDS.

AWS::Route53::HealthCheck

Un bilan de santé d'Amazon Route 53.

- Format de l'ARN : `arn:partition:route53:::healthcheck/Id`

  Exemple : `arn:aws:route53:::healthcheck/123456-1111-2222-3333`

AWS::SQS::Queue

Une file d'attente Amazon SQS.

- Format de l'ARN : `arn:partition:sqs:region:account:QueueName`

  Exemple : `arn:aws:sqs:us-west-2:111122223333:StandardQueue`

  Pour plus d'informations, consultez les ressources et les opérations d'Amazon Simple Queue Service.

AWS::SNS::Topic

Une rubrique Amazon SNS

- Format de l'ARN : `arn:partition:sns:region:account:TopicName`

  Exemple : `arn:aws:sns:us-west-2:111122223333:TopicName`

  Pour plus d'informations, consultez le format ARN des ressources Amazon SNS.

AWS::SNS::Subscription

Un abonnement Amazon SNS.

- Format de l'ARN : `arn:partition:sns:region:account:TopicName:SubscriptionId`

  Exemple : `arn:aws:sns:us-west-2:111122223333:TopicName:12345678901234567890`

AWS::EC2::VPC

Un Virtual Private Cloud (VPC).

- Format de l'ARN : `arn:partition:ec2:region:account:vpc/VpcId`

  Exemple : `arn:aws:ec2:us-west-2:111122223333:vpc/vpc-123456789`

  Pour plus d'informations, consultez la section Ressources VPC.

AWS::EC2::VPNConnection

Une connexion à un réseau privé virtuel (VPN).

- Format de l'ARN : `arn:partition:ec2:region:account:vpn-connection/VpnConnectionId`

  Exemple : `arn:aws:ec2:us-west-2:111122223333:vpn-connection/vpn-123456789`

  Pour plus d'informations, consultez la section Types de ressources définis par Amazon EC2.

AWS::EC2::VPNGateway

Passerelle de réseau privé virtuel (VPN).

- Format de l'ARN : `arn:partition:ec2:region:account:vpn-gateway/VpnGatewayId`

  Exemple : `arn:aws:ec2:us-west-2:111122223333:vpn-gateway/vgw-123456789acbdefgh`

Pour plus d'informations, consultez la section Types de ressources définis par Amazon EC2.

AWS::Route53RecoveryReadiness::DNSTargetResource

Une ressource cible DNS pour les contrôles de préparation inclut le type d'enregistrement DNS, le nom de domaine, l'ARN de la zone hébergée Route 53 et l'ARN Network Load Balancer ou l'ID du jeu d'enregistrements Route 53.

- Format ARN pour la zone hébergée : `arn:partition:route53::account:hostedzone/Id`

  Exemple de zone hébergée : `arn:aws:route53::111122223333:hostedzone/abcHostedZone`

  REMARQUE : Vous devez inclure l'ID du compte dans les ARN de la zone hébergée, comme indiqué ici. L'ID de compte est requis pour que Route 53 ARC puisse interroger la ressource. Le format est volontairement différent du format ARN requis par Amazon Route 53, décrit dans les types de ressources du service Route 53 dans la référence d'autorisation de service.

- Format ARN pour Network Load Balancer : `arn:partition:elasticloadbalancing:region:account:loadbalancer/net/LoadBalancerName`

  Exemple pour Network Load Balancer : `arn:aws:elasticloadbalancing:us-west-2:111122223333:loadbalancer/net/sandbox-net/123456789acbdefgh`

  Pour plus d'informations, consultez les ressources d'Elastic Load Balancing.

Journalisation et surveillance pour vérifier l'état de préparation dans Amazon Route 53 Application Recovery Controller

Vous pouvez utiliser Amazon CloudWatch et Amazon EventBridge pour contrôler le niveau de préparation dans Amazon Route 53 Application Recovery Controller, afin d'analyser les modèles et de résoudre les problèmes. AWS CloudTrail

> **Note**
>
> Vous devez consulter CloudWatch les métriques et les journaux de la Route 53 ARC dans la région de l'ouest des États-Unis (Oregon), à la fois dans la console et lorsque vous utilisez

le AWS CLI. Lorsque vous utilisez le AWS CLI, spécifiez la région de l'ouest des États-Unis (Oregon) pour votre commande en incluant le paramètre suivant :`--region us-west-2`.

Rubriques

Utilisation d'Amazon CloudWatch avec vérification de l'état de préparation dans Route 53 ARC

Amazon Route 53 Application Recovery Controller publie des points de données sur Amazon CloudWatch pour vos contrôles de préparation. CloudWatch vous permet de récupérer des statistiques sur ces points de données sous la forme d'un ensemble ordonné de séries chronologiques, appelées métriques. Considérez une métrique comme une variable à surveiller, et les points de données comme les valeurs de cette variable au fil du temps. Par exemple, vous pouvez surveiller le trafic AWS dans une région sur une période donnée. Un horodatage et une unité de mesure facultative sont associés à chaque point de données.

Vous pouvez utiliser les métriques pour vérifier que le système fonctionne comme prévu. Par exemple, vous pouvez créer une CloudWatch alarme pour surveiller une métrique spécifiée et lancer une action (telle que l'envoi d'une notification à une adresse e-mail) si la métrique dépasse ce que vous considérez comme une plage acceptable.

Pour plus d'informations, consultez le guide de CloudWatch l'utilisateur Amazon.

Rubriques

Métriques ARC de la Route 53

L'espace de noms `AWS/Route53RecoveryReadiness` inclut les métriques suivantes.

Métrique	Description
`ReadinessChecks`	Représente le nombre de contrôles de préparation traités par Route 53 ARC. La métrique peut être dimensionnée en fonction de ses états, listés ci-dessous. Unité :`Count`. Critères de notification : il existe une valeur différente de zéro. Statistiques : La seule statistique utile est`Sum`. Dimensions • `READY` • `NOT_READY` • `NOT_AUTHORIZED` • `UNKNOWN`
`Resources`	Représente le nombre de ressources traitées par Route 53 ARC, qui peut être dimensionné par leur identifiant de ressource, tel que défini par l'API. Unité :`Count`. Critères de notification : il existe une valeur différente de zéro. Statistiques : La seule statistique utile est`Sum`. Dimensions • `ResourceSetType` : Il s'agit des types de ressources, filtrés en fonction du nombre de ressources par type donné évalués par Route 53 ARC Par exemple : `AWS::CloudWatch::Alarm`

Statistiques relatives aux métriques ARC de la Route 53

CloudWatch fournit des statistiques basées sur les points de données métriques publiés par Route 53 ARC. Les statistiques sont des agrégations de données métriques sur une période donnée. Lorsque vous demandez des statistiques, le flux de données renvoyé est identifié par le nom et la dimension de la métrique. Une dimension est une paire nom/valeur qui identifie une métrique de manière unique.

Voici des exemples de combinaisons de mesures et de dimensions qui pourraient vous être utiles :

- Consultez le nombre de contrôles de préparation évalués par Route 53 ARC.
- Afficher le nombre total de ressources pour un type d'ensemble de ressources donné évalué par Route 53 ARC.

Afficher CloudWatch les statistiques dans Route 53 ARC

Vous pouvez consulter les CloudWatch métriques de Route 53 ARC à l'aide de la CloudWatch console ou du AWS CLI. Dans la console, les métriques sont affichées sous forme de graphiques de surveillance.

Vous devez consulter CloudWatch les statistiques de la Route 53 ARC dans la région USA Ouest (Oregon), à la fois dans la console ou lorsque vous utilisez le AWS CLI. Lorsque vous utilisez le AWS CLI, spécifiez la région de l'ouest des États-Unis (Oregon) pour votre commande en incluant le paramètre suivant :`--region us-west-2`.

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 Métriques.
3. Sélectionnez l'espace de noms Route53 RecoveryReadiness.
4. (Facultatif) Pour afficher une métrique pour toutes les dimensions, saisissez son nom dans le champ de recherche.

Pour consulter les statistiques à l'aide du AWS CLI

Utilisez la commande list-metrics suivante pour répertorier les métriques disponibles :

```
aws cloudwatch list-metrics --namespace AWS/Route53RecoveryReadiness --region us-west-2
```

Pour obtenir les statistiques d'une métrique à l'aide du AWS CLI

Utilisez la get-metric-statisticscommande suivante pour obtenir des statistiques pour une métrique et une dimension spécifiées. Notez que CloudWatch chaque combinaison unique de dimensions est traitée comme une métrique distincte. Vous ne pouvez pas récupérer de statistiques à l'aide de combinaisons de dimensions qui n'ont pas été publiées spécifiquement. Vous devez spécifier les mêmes dimensions que celles utilisées lorsque les mesures ont été créées.

L'exemple suivant répertorie le nombre total de contrôles de préparation évalués, par minute, pour un compte dans Route 53 ARC.

```
aws cloudwatch get-metric-statistics --namespace AWS/Route53RecoveryReadiness \
--metric-name ReadinessChecks \
--region us-west-2 \
--statistics Sum --period 60 \
--dimensions Name=State,Value=READY \
--start-time 2021-07-03T01:00:00Z --end-time 2021-07-03T01:20:00Z
```

Voici un exemple de sortie de la commande :

```
{
    "Label": "ReadinessChecks",
    "Datapoints": [
        {
            "Timestamp": "2021-07-08T18:00:00Z",
            "Sum": 1.0,
            "Unit": "Count"
        },
        {
            "Timestamp": "2021-07-08T18:04:00Z",
            "Sum": 1.0,
            "Unit": "Count"
        },
        {
            "Timestamp": "2021-07-08T18:01:00Z",
            "Sum": 1.0,
            "Unit": "Count"
        },
        {
            "Timestamp": "2021-07-08T18:02:00Z",
            "Sum": 1.0,
            "Unit": "Count"
```

```
        },
        {
            "Timestamp": "2021-07-08T18:03:00Z",
            "Sum": 1.0,
            "Unit": "Count"
        }
    ]
}
```

Journalisation des appels d'API de vérification de l'état de préparation AWS CloudTrail

Amazon Route 53 Application Recovery Controller 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 ARC. CloudTrail capture tous les appels d'API pour Route 53 ARC sous forme d'événements. Les appels capturés incluent des appels provenant de la console Route 53 ARC et des appels de code vers les opérations de l'API Route 53 ARC.

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 ARC. 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 ARC, 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.

Pour en savoir plus CloudTrail, consultez le guide de AWS CloudTrail l'utilisateur.

Informations sur la Route 53 ARC dans CloudTrail

CloudTrail est activé sur votre compte Compte AWS lorsque vous créez le compte. Lorsqu'une activité se produit sur Route 53 ARC, 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 Compte AWS. Pour plus d'informations, consultez la section Utilisation de l'historique des CloudTrail événements.

Pour un enregistrement continu des événements de votre région Compte AWS, y compris ceux de la Route 53 ARC, 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 Régions AWS. 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 les ressources suivantes :

- Présentation de la création d'un journal de suivi
- 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 de Route 53 ARC sont enregistrées CloudTrail et documentées dans le Guide de référence de l'API Recovery Readiness pour Amazon Route 53 Application Recovery Controller, le Guide de référence de l'API de configuration de Recovery Control pour Amazon Route 53 Application Recovery Controller et le Guide de référence de l'API de contrôle du routage pour Amazon Route 53 Application Recovery Controller. Par exemple, les appels au `CreateCluster` `UpdateRoutingControlState` et les `CreateRecoveryGroup` 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 faite avec les informations d'identification de l'utilisateur root ou AWS Identity and Access Management (IAM).
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la demande a été faite par un autre AWS service.

Pour plus d'informations, consultez l'élément CloudTrail UserIdentity.

Afficher les événements de la Route 53 ARC dans l'historique des événements

CloudTrail vous permet de consulter les événements récents dans l'historique des événements. Pour afficher les événements relatifs aux demandes d'API ARC Route 53, vous devez sélectionner US West (Oregon) dans le sélecteur de région en haut de la console. Pour plus d'informations, consultez la section Utilisation de l'historique des CloudTrail événements dans le guide de AWS CloudTrail l'utilisateur.

Comprendre les entrées du fichier journal ARC 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'exemple suivant montre une entrée de CloudTrail journal illustrant l'`CreateRecoveryGroup`action à effectuer pour vérifier l'état de préparation.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:role/admin",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROA33L3W36EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/admin",
                "accountId": "111122223333",
                "userName": "EXAMPLENAME"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2021-07-06T17:38:05Z"
            }
        }
    },
    "eventTime": "2021-07-06T18:08:03Z",
    "eventSource": "route53-recovery-readiness.amazonaws.com",
    "eventName": "CreateRecoveryGroup",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.50",
```

```
    "userAgent": "Boto3/1.17.101 Python/3.8.10 Linux/4.14.231-180.360.amzn2.x86_64
 exec-env/AWS_Lambda_python3.8 Botocore/1.20.102",
    "requestParameters": {
        "recoveryGroupName": "MyRecoveryGroup"
    },
    "responseElements": {
        "Access-Control-Expose-Headers": "x-amzn-errortype,x-amzn-requestid,x-amzn-
errormessage,x-amzn-trace-id,x-amzn-requestid,x-amz-apigw-id,date",
        "cells": [],
        "recoveryGroupName": "MyRecoveryGroup",
        "recoveryGroupArn": "arn:aws:route53-recovery-readiness::111122223333:recovery-
group/MyRecoveryGroup",
        "tags": "***"
    },
    "requestID": "fd42dcf7-6446-41e9-b408-d096example",
    "eventID": "4b5c42df-1174-46c8-be99-d67aexample",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333"
}
```


Utilisation du contrôle de préparation dans Route 53 ARC avec Amazon EventBridge

À l'aide d'Amazon EventBridge, vous pouvez configurer des règles pilotées par des événements qui surveillent vos ressources de contrôle de disponibilité dans Amazon Route 53 Application Recovery Controller, puis lancer des actions cibles utilisant d'autres AWS services. Par exemple, vous pouvez définir une règle pour l'envoi de notifications par e-mail en signalant un sujet Amazon SNS lorsque le statut d'un test de préparation passe de PRÊT à PAS PRÊT.

> **Note**
>
> Route 53 ARC publie uniquement les EventBridge événements destinés à vérifier l'état de préparation dans la région de l'ouest des États-Unis (Oregon) (us-west-2). AWS Pour recevoir des EventBridge événements à des fins de vérification de l'état de préparation, créez des EventBridge règles dans la région de l'ouest des États-Unis (Oregon).

Vous pouvez créer des règles dans Amazon EventBridge pour réagir à l'événement suivant de vérification du niveau de préparation à l'ARC de la Route 53 :

- Vérifier l'état de préparation. L'événement indique si le statut du contrôle de disponibilité change, par exemple, de PRÊT à PAS PRÊT.

Pour capturer des événements ARC spécifiques à la Route 53 qui vous intéressent, définissez des modèles spécifiques à l'événement qui EventBridge peuvent être utilisés pour détecter les événements. Les modèles d'événements ont la même structure que les événements auxquels ils correspondent. Le modèle place entre guillemets les champs que vous voulez faire correspondre et fournit les valeurs que vous recherchez.

Les événements sont générés dans la mesure du possible. Ils sont livrés depuis la Route 53 ARC EventBridge en temps quasi réel dans des circonstances opérationnelles normales. Cependant, des situations peuvent survenir susceptibles de retarder ou d'empêcher la livraison d'un événement.

Pour plus d'informations sur le fonctionnement EventBridge des règles avec les modèles d'événements, consultez la section Événements et modèles d'événements dans EventBridge.

Surveillez une ressource de vérification de l'état de préparation avec EventBridge

Avec EventBridge, vous pouvez créer des règles qui définissent les actions à entreprendre lorsque Route 53 ARC émet des événements pour les ressources de contrôle de disponibilité.

Pour taper ou copier-coller un modèle d'événement dans la EventBridge console, dans la console, sélectionnez l'option Enter my own option. Pour vous aider à déterminer les modèles d'événements susceptibles de vous être utiles, cette rubrique inclut des exemples de modèles d'événements de préparation.

Pour créer une règle pour un événement de ressource

1. Ouvrez la EventBridge console Amazon à l'adresse https://console.aws.amazon.com/events/.
2. Pour Région AWS créer la règle dans, choisissez US West (Oregon). Il s'agit de la région requise pour les événements de préparation.
3. Choisissez Create rule.
4. Entrez un nom et éventuellement une description pour la règle.
5. Pour Event bus, laissez la valeur par défaut, default.
6. Choisissez Suivant.
7. Pour l'étape Créer un modèle d'événement, pour Source d'événement, laissez la valeur par défaut, AWS events.

8. Sous Exemple d'événement, choisissez Enter my own.
9. Pour Exemples d'événements, tapez ou copiez-collez un modèle d'événement. Pour des exemples, reportez-vous à la section suivante.

Exemples de modèles d'événements de préparation

Les modèles d'événements ont la même structure que les événements auxquels ils correspondent. Le modèle place entre guillemets les champs que vous voulez faire correspondre et fournit les valeurs que vous recherchez.

Vous pouvez copier et coller des modèles d'événements depuis cette section EventBridge pour créer des règles que vous pouvez utiliser pour surveiller les actions et les ressources de la Route 53 ARC.

Les modèles d'événements suivants fournissent des exemples que vous pouvez utiliser EventBridge pour la fonctionnalité de vérification de l'état de préparation de Route 53 ARC.

- Sélectionnez tous les événements dans le test de préparation de la Route 53 ARC.

```
{
    "source": [
        "aws.route53-recovery-readiness"
    ]
}
```

- Sélectionnez uniquement les événements liés aux cellules.

```
{
    "source": [
        "aws.route53-recovery-readiness"
    ],
    "detail-type": [
        "Route 53 Application Recovery Controller cell readiness status change"
    ]
}
```

- Sélectionnez uniquement les événements liés à une cellule spécifique appelée *`MyExampleCell`*.

```
{
    "source": [
        "aws.route53-recovery-readiness"
    ],
```

```
    "detail-type": [
        "Route 53 Application Recovery Controller cell readiness status change"
    ],
    "resources": [
        "arn:aws:route53-recovery-readiness::111122223333:cell/MyExampleCell"
    ]
}
```

- Sélectionnez uniquement les événements lorsque l'état d'un groupe de restauration, d'une cellule ou d'une vérification de l'état de préparation devient atteint *NOT READY*.

```
{
   "source":[
      "aws.route53-recovery-readiness"
   ],
   "detail-type":{
      "new-state":{
         "readiness-status":[
            "NOT_READY"
         ]
      }
   }
}
```

- Sélectionnez uniquement les événements lorsqu'un groupe de restauration, une cellule ou une vérification de l'état de préparation devient autre chose *READY*

```
{
   "source":[
      "aws.route53-recovery-readiness"
   ],
   "detail":{
      "new-state":{
         "readiness-status":[
            {
               "anything-but":"READY"
            }
         ]
      }
   }
}
```

Voici un exemple d'événement ARC Route 53 pour une modification de l'état de préparation d'un groupe de restauration :

```
{
    "version": "0",
    "account":"111122223333",
    "detail-type":"Route 53 Application Recovery Controller recovery group readiness
 status change",
    "source":"route53-recovery-readiness.amazonaws.com",
    "time":"2020-11-03T00:31:54Z",
    "id": "1234a678-1b23-c123-12fd3f456e78",
    "region": "us-west-2",
    "resources":[
        "arn:aws:route53-recovery-readiness::111122223333:recovery-group/BillingApp"
    ],
    "detail": {
        "recovery-group-name": "BillingApp",
        "previous-state": {
            "readiness-status": "READY|NOT_READY|UNKNOWN|NOT_AUTHORIZED"
        },
        "new-state": {
            "readiness-status": "READY|NOT_READY|UNKNOWN|NOT_AUTHORIZED"
        }
    }
}
```

Voici un exemple d'événement ARC Route 53 pour une modification de l'état de préparation d'une cellule :

```
{
    "version": "0",
    "account":"111122223333",
    "detail-type":"Route 53 Application Recovery Controller cell readiness status
 change",
    "source":"route53-recovery-readiness.amazonaws.com",
    "time":"2020-11-03T00:31:54Z",
    "id": "1234a678-1b23-c123-12fd3f456e78",
    "region": "us-west-2",
    "resources":[
        "arn:aws:route53-recovery-readiness::111122223333:cell/PDXCell"
    ],
    "detail": {
        "cell-name": "PDXCell",
```

```
        "previous-state": {
            "readiness-status": "READY|NOT_READY|UNKNOWN|NOT_AUTHORIZED"
        },
        "new-state": {
            "readiness-status": "READY|NOT_READY|UNKNOWN|NOT_AUTHORIZED"
        }
    }
}
```

Voici un exemple d'événement ARC de la Route 53 pour un changement de statut de vérification de l'état de préparation :

```
{
    "version": "0",
    "account":"111122223333",
    "detail-type":"Route 53 Application Recovery Controller readiness check status
 change",
    "source":"route53-recovery-readiness.amazonaws.com",
    "time":"2020-11-03T00:31:54Z",
    "id": "1234a678-1b23-c123-12fd3f456e78",
    "region": "us-west-2",
    "resources":[
        "arn:aws:route53-recovery-readiness::111122223333:readiness-check/
UserTableReadinessCheck"
    ],
    "detail": {
    "readiness-check-name": "UserTableReadinessCheck",
        "previous-state": {
            "readiness-status": "READY|NOT_READY|UNKNOWN|NOT_AUTHORIZED"
        },
        "new-state": {
            "readiness-status": "READY|NOT_READY|UNKNOWN|NOT_AUTHORIZED"
        }
    }
}
```

Spécifiez un groupe de CloudWatch journaux à utiliser comme cible

Lorsque vous créez une EventBridge règle, vous devez spécifier la cible vers laquelle les événements correspondant à la règle sont envoyés. Pour obtenir la liste des cibles disponibles pour EventBridge, consultez la section Cibles disponibles dans la EventBridge console. L'une des cibles que vous pouvez ajouter à une EventBridge règle est un groupe de CloudWatch journaux Amazon.

Cette section décrit les exigences relatives à l'ajout de groupes de CloudWatch journaux en tant que cibles et fournit une procédure pour ajouter un groupe de journaux lorsque vous créez une règle.

Pour ajouter un groupe de CloudWatch journaux en tant que cible, vous pouvez effectuer l'une des opérations suivantes :

- Création d'un nouveau groupe de journaux
- Choisissez un groupe de journaux existant

Si vous spécifiez un nouveau groupe de journaux à l'aide de la console lorsque vous créez une règle, le groupe de journaux est EventBridge automatiquement créé pour vous. Assurez-vous que le groupe de journaux que vous utilisez comme cible pour la EventBridge règle commence par`/aws/events`. Si vous souhaitez choisir un groupe de journaux existant, sachez que seuls les groupes de journaux commençant par `/aws/events` apparaissent sous forme d'options dans le menu déroulant. Pour plus d'informations, consultez la section Créer un nouveau groupe de journaux dans le guide de CloudWatch l'utilisateur Amazon.

Si vous créez ou utilisez un groupe de CloudWatch journaux à utiliser comme cible à l'aide d' CloudWatch opérations en dehors de la console, assurez-vous de définir correctement les autorisations. Si vous utilisez la console pour ajouter un groupe de journaux à une EventBridge règle, la politique basée sur les ressources pour le groupe de journaux est automatiquement mise à jour. Toutefois, si vous utilisez le AWS Command Line Interface ou un AWS SDK pour spécifier un groupe de journaux, vous devez mettre à jour la politique basée sur les ressources pour le groupe de journaux. L'exemple de politique suivant illustre les autorisations que vous devez définir dans une stratégie basée sur les ressources pour le groupe de journaux :

```
{
  "Statement": [
    {
      "Action": [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "events.amazonaws.com",
          "delivery.logs.amazonaws.com"
        ]
      },
```

```
      "Resource": "arn:aws:logs:region:account:log-group:/aws/events/*:*",
      "Sid": "TrustEventsToStoreLogEvent"
    }
  ],
  "Version": "2012-10-17"
}
```

Vous ne pouvez pas configurer une politique basée sur les ressources pour un groupe de journaux à l'aide de la console. Pour ajouter les autorisations requises à une politique basée sur les ressources, utilisez l'opération CloudWatch PutResourcePolicy API. Vous pouvez ensuite utiliser la commande de la CLI describe-resource-policies pour vérifier que votre politique a été correctement appliquée.

Pour créer une règle pour un événement de ressource et spécifier une cible de groupe de CloudWatch journaux

1. Ouvrez la EventBridge console Amazon à l'adresse https://console.aws.amazon.com/events/.
2. Choisissez Région AWS celui dans lequel vous souhaitez créer la règle.
3. Choisissez Créer une règle, puis entrez les informations relatives à cette règle, telles que le modèle d'événement ou les détails du calendrier.

   Pour plus d'informations sur la création de EventBridge règles relatives à l'état de préparation, voir Surveiller une ressource de vérification du niveau de préparation avec EventBridge.
4. Sur la page Sélectionner une cible, choisissez CloudWatchcomme cible.
5. Choisissez un groupe de CloudWatch journaux dans le menu déroulant.

Identity and Access Management pour vérifier le niveau de préparation

AWS Identity and Access Management (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les ressources ARC de la Route 53. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Table des matières

- AWS politiques gérées pour le contrôle de l'état de préparation dans Amazon Route 53 Application Recovery Controller

Comment fonctionne le contrôle de l'état de préparation dans ServiceLong ; avec IAM

Avant d'utiliser IAM pour gérer l'accès à Route 53 ARC, découvrez quelles fonctionnalités IAM peuvent être utilisées avec Route 53 ARC.

Avant d'utiliser IAM pour gérer l'accès au contrôle de préparation dans Amazon Route 53 Application Recovery Controller, découvrez quelles fonctionnalités IAM peuvent être utilisées avec le contrôle de préparation.

Fonctionnalités IAM que vous pouvez utiliser avec le contrôle du niveau de préparation dans Amazon Route 53 Application Recovery Controller

Fonction IAM	Assistance pour vérifier l'état de préparation
Politiques basées sur l’identité	Oui
Politiques basées sur les ressources	Non
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition d’une politique	Oui
ACL	Non
ABAC (étiquettes dans les politiques)	Oui
Informations d’identification temporaires	Oui
Autorisations de principal	Oui
Fonctions du service	Non
Rôles liés à un service	Oui

Pour obtenir une vue globale de haut niveau du fonctionnement des AWS services avec la plupart des fonctionnalités IAM, consultez la section AWS Services compatibles avec IAM dans le Guide de l'utilisateur IAM.

Politiques basées sur l'identité pour le contrôle de l'état de préparation

Prend en charge les politiques basées sur l’identité	Oui

Les politiques basées sur l’identité sont des documents de politique d’autorisations JSON que vous pouvez attacher à une identité telle qu’un utilisateur, un groupe d’utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d’actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l’identité, consultez Création de politiques IAM dans le Guide de l’utilisateur IAM.

Avec les politiques IAM basées sur l’identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Vous ne pouvez pas spécifier le principal dans une politique basée sur une identité car celle-ci s’applique à l’utilisateur ou au rôle auquel elle est attachée. Pour découvrir tous les éléments que vous utilisez dans une politique JSON, consultez Références des éléments de politique JSON IAM dans le Guide de l’utilisateur IAM.

Pour consulter des exemples de politiques basées sur l'identité de Route 53 ARC, consultez. Exemples de politiques basées sur l'identité dans Amazon Route 53 Application Recovery Controller

Politiques basées sur les ressources dans le cadre du contrôle de préparation

Prend en charge les politiques basées sur les ressources	Non

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l’accès à une ressource spécifique.

Actions politiques pour le contrôle de l'état de préparation

Prend en charge les actions de politique	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Les actions de stratégie portent généralement le même nom que l'opération AWS d'API associée. Il existe quelques exceptions, telles que les actions avec autorisations uniquement qui n'ont pas d'opération API correspondante. Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une stratégie afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour consulter la liste des actions ARC de Route 53 à des fins de vérification de l'état de préparation, consultez la section Actions définies par Amazon Route 53 Recovery Readiness dans le Service Authorization Reference.

Les actions politiques dans Route 53 ARC pour vérifier l'état de préparation utilisent les préfixes suivants avant l'action :

```
route53-recovery-readiness
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules. Par exemple, ce qui suit :

```
"Action": [
      "route53-recovery-readiness:action1",
      "route53-recovery-readiness:action2"
         ]
```

Vous pouvez aussi spécifier plusieurs actions à l'aide de caractères génériques (*). Par exemple, pour spécifier toutes les actions qui commencent par le mot `Describe`, incluez l'action suivante :

```
"Action": "route53-recovery-readiness:Describe*"
```

Pour consulter des exemples de politiques basées sur l'identité de Route 53 ARC pour le contrôle de l'état de préparation, voir. Exemples de politiques basées sur l'identité pour le contrôle de l'état de préparation dans Amazon Route 53 Application Recovery Controller

Ressources politiques pour le contrôle de l'état de préparation

Prend en charge les ressources de politique	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

```
"Resource": "*"
```

Pour consulter la liste des actions ARC de la Route 53 pour le changement de zone, consultez la section Actions définies par Amazon Route 53 Recovery Readiness.

Pour consulter des exemples de politiques basées sur l'identité de Route 53 ARC pour le contrôle de l'état de préparation, voir. Exemples de politiques basées sur l'identité pour le contrôle de l'état de préparation dans Amazon Route 53 Application Recovery Controller

Clés relatives aux conditions des politiques pour la vérification de l'état

Prend en charge les clés de condition de politique spécifiques au service	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` (ou le bloc `Condition`) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément `Condition` est facultatif. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande.

Si vous spécifiez plusieurs éléments `Condition` dans une instruction, ou plusieurs clés dans un seul élément `Condition`, AWS les évalue à l'aide d'une opération `AND` logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une `OR` opération logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez accorder à un utilisateur IAM l'autorisation d'accéder à une ressource uniquement si elle est balisée avec son nom d'utilisateur IAM. Pour plus d'informations, consultez Éléments d'une politique IAM : variables et identifications dans le Guide de l'utilisateur IAM.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques au service. Pour voir toutes les clés de condition AWS globales, voir les clés de contexte de condition AWS globales dans le guide de l'utilisateur IAM.

Pour consulter la liste des actions ARC relatives à la vérification de l'état de préparation d'Amazon Route 53, consultez la section Clés de condition pour Amazon Route 53 Recovery Readiness

Pour connaître les actions et les ressources que vous pouvez utiliser avec une clé de condition avec vérification de l'état de préparation, consultez Actions définies par Amazon Route 53 Recovery Readiness

Pour consulter des exemples de politiques basées sur l'identité de Route 53 ARC pour le contrôle de l'état de préparation, voir. Exemples de politiques basées sur l'identité pour le contrôle de l'état de préparation dans Amazon Route 53 Application Recovery Controller

Listes de contrôle d'accès (ACL) en cours de vérification de l'état de préparation

Prend en charge les listes ACL	Non

Les listes de contrôle d'accès (ACL) vérifient quels principaux (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Contrôle d'accès basé sur les attributs (ABAC) avec vérification de l'état de préparation

Prise en charge d'ABAC (identifications dans les politiques)	Partielle

Le contrôle d'accès basé sur les attributs (ABAC) est une politique d'autorisation qui définit des autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et à de nombreuses AWS ressources. L'étiquetage des entités et des ressources est la première étape d'ABAC. Vous concevez ensuite des politiques ABAC pour autoriser des opérations quand l'identification du principal correspond à celle de la ressource à laquelle il tente d'accéder.

L'ABAC est utile dans les environnements qui connaissent une croissance rapide et pour les cas où la gestion des politiques devient fastidieuse.

Pour contrôler l'accès basé sur des étiquettes, vous devez fournir les informations d'étiquette dans l'élément de condition d'une politique utilisant les clés de condition `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d'informations sur l'ABAC, consultez Qu'est-ce que le contrôle d'accès basé sur les attributs (ABAC) ? dans le Guide de l'utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration de l'ABAC, consultez Utilisation du contrôle d'accès par attributs (ABAC) dans le Guide de l'utilisateur IAM.

Recovery Readiness (vérification de l'état de préparation) prend en charge l'ABAC.

Utilisation d'informations d'identification temporaires avec vérification de l'état de préparation

Prend en charge les informations d’identif ication temporaires	Oui

Certains Services AWS ne fonctionnent pas lorsque vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, y compris celles qui Services AWS fonctionnent avec des informations d'identification temporaires, consultez Services AWS la section relative à l'utilisation d'IAM dans le guide de l'utilisateur d'IAM.

Vous utilisez des informations d'identification temporaires si vous vous connectez à l' AWS Management Console aide d'une méthode autre qu'un nom d'utilisateur et un mot de passe. Par exemple, lorsque vous accédez à AWS l'aide du lien d'authentification unique (SSO) de votre entreprise, ce processus crée automatiquement des informations d'identification temporaires. Vous créez également automatiquement des informations d’identification temporaires lorsque vous vous connectez à la console en tant qu’utilisateur, puis changez de rôle. Pour plus d’informations sur le changement de rôle, consultez Changement de rôle (console) dans le Guide de l’utilisateur IAM.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide de l' AWS API AWS CLI or. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour y accéder AWS. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d’informations, consultez Informations d’identification de sécurité temporaires dans IAM.

Autorisations principales interservices pour le contrôle de l'état de préparation

Prend en charge les sessions d'accès direct (FAS)	Oui

Lorsque vous utilisez une entité IAM (utilisateur ou rôle) pour effectuer des actions AWS, vous êtes considéré comme un mandant. Les politiques accordent des autorisations au principal. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui déclenche une autre action dans un autre service. Dans ce cas, vous devez disposer d’autorisations nécessaires pour effectuer les deux actions.

Pour savoir si une action dans le cadre du contrôle de préparation nécessite des actions dépendantes supplémentaires dans une politique, consultez Amazon Route 53 Recovery Readiness

Rôles de service pour le contrôle du niveau de préparation

Prend en charge les fonctions de service	Non

Une fonction du service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du 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.

Rôles liés aux services pour la vérification de l'état de préparation

Prend en charge les rôles liés à un service.	Oui

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.

Pour plus de détails sur la création ou la gestion des rôles liés au service Route 53 ARC, consultez. Utilisation d'un rôle lié au service pour vérifier l'état de préparation dans Route 53 ARC

Pour plus d'informations sur la création ou la gestion des rôles liés à un service, consultez Services AWS qui fonctionnent avec IAM. Recherchez un service dans le tableau qui inclut un `Yes` dans la colonne Rôle lié à un service. Choisissez le lien Oui pour consulter la documentation du rôle lié à ce service.

Exemples de politiques basées sur l'identité pour le contrôle de l'état de préparation dans Amazon Route 53 Application Recovery Controller

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier les ressources ARC de la Route 53. Ils ne peuvent pas non plus effectuer de tâches à l'aide de l'API AWS Management Console, AWS Command Line Interface (AWS CLI) ou de AWS l'API. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Pour apprendre à créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, consultez Création de politiques dans l'onglet JSON dans le Guide de l'utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par Route 53 ARC, y compris le format des ARN pour chacun des types de ressources, consultez la section Actions, ressources et clés de condition pour Amazon Route 53 Application Recovery Controller dans le Service Authorization Reference.

Rubriques

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer des ressources Route 53 ARC dans votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez politiques gérées par AWS ou politiques gérées par AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.
- Accorder les autorisations de moindre privilège : lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l'exécution d'une seule tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation de IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utiliser des conditions dans les politiques IAM pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes

doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que AWS CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

- Utilisez IAM Access Analyzer pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : IAM Access Analyzer valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez Validation de politique IAM Access Analyzer dans le Guide de l'utilisateur IAM.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue. Compte AWS Pour exiger le MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Configuration de l'accès aux API protégé par MFA dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

Exemple : accès à la console de vérification de l'état de préparation

Pour accéder à la console Amazon Route 53 Application Recovery Controller, vous devez disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et d'afficher les détails des ressources ARC de la Route 53 présentes dans votre Compte AWS. Si vous créez une stratégie basée sur l'identité qui est plus restrictive que l'ensemble minimum d'autorisations requis, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs ou rôles) tributaires de cette stratégie.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement l'API AWS CLI ou l' AWS API. Autorisez plutôt l'accès à uniquement aux actions qui correspondent à l'opération d'API qu'ils tentent d'effectuer.

Pour garantir que les utilisateurs et les rôles peuvent toujours utiliser la console de vérification du niveau de préparation lorsque vous n'autorisez l'accès qu'à des opérations d'API spécifiques, associez également une politique `ReadOnly` AWS gérée pour le contrôle de préparation aux entités. Pour plus d'informations, consultez la page Politiques gérées du contrôle de préparation ou l'ajout d'autorisations à un utilisateur dans le guide de l'utilisateur IAM.

Pour effectuer certaines tâches, les utilisateurs doivent être autorisés à créer le rôle lié au service associé au contrôle de préparation dans Route 53 ARC. Pour en savoir plus, veuillez consulter la section Utilisation d'un rôle lié au service pour vérifier l'état de préparation dans Route 53 ARC.

Pour donner aux utilisateurs un accès complet aux fonctionnalités de vérification du niveau de préparation via la console, associez une politique telle que la suivante à l'utilisateur :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                   "route53-recovery-readiness:CreateCell",
                   "route53-recovery-readiness:CreateCrossAccountAuthorization",
                   "route53-recovery-readiness:CreateReadinessCheck",
                   "route53-recovery-readiness:CreateRecoveryGroup",
                   "route53-recovery-readiness:CreateResourceSet",
                   "route53-recovery-readiness:DeleteCell",
                   "route53-recovery-readiness:DeleteCrossAccountAuthorization",
                   "route53-recovery-readiness:DeleteReadinessCheck",
                   "route53-recovery-readiness:DeleteRecoveryGroup",
                   "route53-recovery-readiness:DeleteResourceSet",
                   "route53-recovery-readiness:GetArchitectureRecommendations",
                   "route53-recovery-readiness:GetCell",
                   "route53-recovery-readiness:GetCellReadinessSummary",
                   "route53-recovery-readiness:GetReadinessCheck",
                   "route53-recovery-readiness:GetReadinessCheckResourceStatus",
                   "route53-recovery-readiness:GetReadinessCheckStatus",
                   "route53-recovery-readiness:GetRecoveryGroup",
                   "route53-recovery-readiness:GetRecoveryGroupReadinessSummary",
                   "route53-recovery-readiness:GetResourceSet",
                   "route53-recovery-readiness:ListCells",
                   "route53-recovery-readiness:ListCrossAccountAuthorizations",
                   "route53-recovery-readiness:ListReadinessChecks",
                   "route53-recovery-readiness:ListRecoveryGroups",
                   "route53-recovery-readiness:ListResourceSets",
                   "route53-recovery-readiness:ListRules",
                   "route53-recovery-readiness:UpdateCell",
                   "route53-recovery-readiness:UpdateReadinessCheck",
                   "route53-recovery-readiness:UpdateRecoveryGroup",
                   "route53-recovery-readiness:UpdateResourceSet"
            ],
```

```
            "Resource": "*"
        }
    ]
}
```

Exemples : actions de l'API de vérification de l'état de préparation pour le contrôle de préparation

Pour garantir qu'un utilisateur peut utiliser les actions de l'API Route 53 ARC pour travailler avec le plan de contrôle de disponibilité de Route 53 ARC, par exemple, pour créer des groupes de restauration, des ensembles de ressources et des contrôles de disponibilité, associez une politique correspondant aux opérations d'API avec lesquelles l'utilisateur doit travailler, comme décrit ci-dessous.

Pour effectuer certaines tâches, les utilisateurs doivent être autorisés à créer le rôle lié au service associé au contrôle de préparation dans Route 53 ARC. Pour en savoir plus, veuillez consulter la section Utilisation d'un rôle lié au service pour vérifier l'état de préparation dans Route 53 ARC.

Pour utiliser les opérations d'API à des fins de vérification de l'état de préparation, associez une politique telle que la suivante à l'utilisateur :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                   "route53-recovery-readiness:CreateCell",
                   "route53-recovery-readiness:CreateCrossAccountAuthorization",
                   "route53-recovery-readiness:CreateReadinessCheck",
                   "route53-recovery-readiness:CreateRecoveryGroup",
                   "route53-recovery-readiness:CreateResourceSet",
                   "route53-recovery-readiness:DeleteCell",
                   "route53-recovery-readiness:DeleteCrossAccountAuthorization",
                   "route53-recovery-readiness:DeleteReadinessCheck",
                   "route53-recovery-readiness:DeleteRecoveryGroup",
                   "route53-recovery-readiness:DeleteResourceSet",
                   "route53-recovery-readiness:GetArchitectureRecommendations",
                   "route53-recovery-readiness:GetCell",
                   "route53-recovery-readiness:GetCellReadinessSummary",
                   "route53-recovery-readiness:GetReadinessCheck",
                   "route53-recovery-readiness:GetReadinessCheckResourceStatus",
                   "route53-recovery-readiness:GetReadinessCheckStatus",
```

```
                "route53-recovery-readiness:GetRecoveryGroup",
                "route53-recovery-readiness:GetRecoveryGroupReadinessSummary",
                "route53-recovery-readiness:GetResourceSet",
                "route53-recovery-readiness:ListCells",
                "route53-recovery-readiness:ListCrossAccountAuthorizations",
                "route53-recovery-readiness:ListReadinessChecks",
                "route53-recovery-readiness:ListRecoveryGroups",
                "route53-recovery-readiness:ListResourceSets",
                "route53-recovery-readiness:ListRules",
                "route53-recovery-readiness:ListTagsForResources",
                "route53-recovery-readiness:UpdateCell",
                "route53-recovery-readiness:UpdateReadinessCheck",
                "route53-recovery-readiness:UpdateRecoveryGroup",
                "route53-recovery-readiness:UpdateResourceSet",
                "route53-recovery-readiness:TagResource",
                "route53-recovery-readiness:UntagResource"
            ],
            "Resource": "*"
        }
    ]
}
```

Utilisation d'un rôle lié au service pour vérifier l'état de préparation dans Route 53 ARC

Amazon Route 53 Application Recovery Controller utilise des rôles AWS Identity and Access Management liés à un service (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié à un service, dans ce cas, Route 53 ARC. Les rôles liés à un service sont prédéfinis par Route 53 ARC et incluent toutes les autorisations dont le service a besoin pour appeler d'autres AWS services en votre nom à des fins spécifiques.

Les rôles liés à un service facilitent la configuration de Route 53 ARC, car il n'est pas nécessaire d'ajouter manuellement les autorisations nécessaires. Route 53 ARC définit les autorisations de ses rôles liés aux services, et sauf indication contraire, seule la Route 53 ARC peut assumer 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 de ses ressources connexes. Cela protège vos ressources ARC de la Route 53, car vous ne pouvez pas supprimer par inadvertance l'autorisation d'accès aux ressources.

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés à un service, consultez la section AWS Services qui fonctionnent avec IAM et recherchez les services dont la

valeur est Oui dans la colonne Rôle lié au service. Choisissez un Yes (oui) ayant un lien permettant de consulter les détails du rôle pour ce service.

Route 53 ARC possède les rôles liés aux services suivants, décrits dans ce chapitre :

- Route 53 ARC utilise le rôle lié au service nommé Route53 RecoveryReadinessServiceRolePolicy pour accéder aux ressources et aux configurations afin de vérifier l'état de préparation.
- Route 53 ARC utilise le rôle lié au service nommé pour les essais d'autoshift, pour surveiller les CloudWatch alarmes Amazon et les AWS Health Dashboard événements clients fournis par les clients, et pour démarrer les essais.

Autorisations de rôle liées au service pour Route53 RecoveryReadinessServiceRolePolicy

Route 53 ARC utilise un rôle lié à un service nommé Route53 RecoveryReadinessServiceRolePolicy pour accéder aux ressources et aux configurations afin de vérifier l'état de préparation. Cette section décrit les autorisations pour le rôle lié au service, ainsi que des informations sur la création, la modification et la suppression du rôle.

Autorisations de rôle liées au service pour Route53 RecoveryReadinessServiceRolePolicy

Ce rôle lié à un service utilise la politique gérée.
`Route53RecoveryReadinessServiceRolePolicy`

Le rôle RecoveryReadinessServiceRolePolicy lié au service Route53 fait confiance au service suivant pour assumer le rôle :

- `route53-recovery-readiness.amazonaws.com`

Pour consulter les autorisations associées à cette politique, consultez Route53 RecoveryReadinessServiceRolePolicy dans le manuel AWS Managed Policy Reference.

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 Autorisations de rôles liés à un service dans le Guide de l'utilisateur IAM.

Création du rôle RecoveryReadinessServiceRolePolicy lié au service Route53 pour Route 53 ARC

Il n'est pas nécessaire de créer manuellement le rôle lié au RecoveryReadinessServiceRolePolicy service Route53. Lorsque vous créez le premier contrôle de préparation ou l'autorisation entre

comptes dans l' AWS Management Console AWS API AWS CLI, Route 53 ARC crée le rôle lié au service pour vous.

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 le premier contrôle de préparation ou l'autorisation entre comptes, Route 53 ARC crée à nouveau le rôle lié au service pour vous.

Modification du rôle RecoveryReadinessServiceRolePolicy lié au service Route53 pour Route 53 ARC

Route 53 ARC ne vous permet pas de modifier le rôle lié au RecoveryReadinessServiceRolePolicy service Route53. Après avoir créé le rôle lié à un service, vous ne pouvez pas modifier le nom du rôle car d'autres entités peuvent y faire référence. 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 du rôle RecoveryReadinessServiceRolePolicy lié au service Route53 pour Route 53 ARC

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.

Une fois que vous avez supprimé vos contrôles de préparation et vos autorisations entre comptes, vous pouvez supprimer le rôle lié au service Route53 RecoveryReadinessServiceRolePolicy. Pour plus d'informations sur les contrôles de préparation, consultezVérification de l'état de préparation dans Amazon Route 53 Application Recovery Controller. Pour plus d'informations sur les autorisations entre comptes, consultez. Création d'autorisations entre comptes dans Route 53 ARC

> **Note**
>
> Si le service Route 53 ARC utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression du rôle de service risque d'échouer. Dans ce cas, attendez quelques minutes et réessayez de supprimer le rôle.

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 service Route53RecoveryReadinessServiceRolePolicy. Pour plus d'informations, consultez Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Mises à jour du rôle lié au service Route 53 ARC pour la vérification de l'état de préparation

Pour les mises à jour des politiques AWS gérées pour les rôles liés au service Route 53 ARC, consultez le tableau des mises à jour des politiques AWS gérées pour Route 53 ARC. Vous pouvez également vous abonner aux alertes RSS automatiques sur la page d'historique des documents ARC de la Route 53.

AWS politiques gérées pour le contrôle de l'état de préparation dans Amazon Route 53 Application Recovery Controller

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 politique Service AWS est lancée ou lorsque de nouvelles opérations d'API sont disponibles pour les services existants.

Pour plus d'informations, consultez la section Politiques gérées par AWS dans le Guide de l'utilisateur IAM.

AWS politique gérée : Route53 RecoveryReadinessServiceRolePolicy

Vous ne pouvez pas joindre de `Route53RecoveryReadinessServiceRolePolicy` à vos entités IAM. Cette politique est associée à un rôle lié à un service qui permet à Amazon Route 53 Application Recovery Controller d'accéder aux AWS services et aux ressources utilisés ou gérés par Route 53

ARC. Pour plus d'informations, consultez Utilisation d'un rôle lié au service pour vérifier l'état de préparation dans Route 53 ARC.

AWS politique gérée : AmazonRoute 53 RecoveryReadinessFullAccess

Vous pouvez attacher `AmazonRoute53RecoveryReadinessFullAccess` à vos entités IAM. Cette politique donne un accès complet aux actions relatives à l'état de préparation au rétablissement (vérification de l'état de préparation) sur la Route 53 ARC. Associez-le aux utilisateurs IAM et aux autres principaux qui ont besoin d'un accès complet aux actions de préparation à la restauration.

Pour consulter les autorisations associées à cette politique, reportez-vous à la section AmazonRoute53 du RecoveryReadinessFullAccess manuel AWS Managed Policy Reference.

AWS politique gérée : AmazonRoute 53 RecoveryReadinessReadOnlyAccess

Vous pouvez attacher `AmazonRoute53RecoveryReadinessReadOnlyAccess` à vos entités IAM. Cette politique accorde un accès en lecture seule aux actions permettant de travailler sur la préparation à la reprise dans Route 53 ARC. C'est utile pour les utilisateurs qui ont besoin de consulter les états de préparation et les configurations des groupes de restauration. Ces utilisateurs ne peuvent pas créer, mettre à jour ou supprimer des ressources de préparation à la restauration.

Pour consulter les autorisations associées à cette politique, reportez-vous à la section AmazonRoute53 du RecoveryReadinessReadOnlyAccess manuel AWS Managed Policy Reference.

Mises à jour des politiques AWS gérées en matière de préparation

Pour plus de détails sur les mises à jour des politiques AWS gérées pour le contrôle de l'état de préparation dans Route 53 ARC depuis que ce service a commencé à suivre ces modifications, voirMises à jour des politiques AWS gérées pour Amazon Route 53 Application Recovery Controller. Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au fil RSS sur la page d'historique du document ARC Route 53.

Quotas pour le contrôle de préparation

Le contrôle du niveau de préparation dans Amazon Route 53 Application Recovery Controller est soumis aux quotas suivants (anciennement appelés limites).

Entité	Quota
Nombre de groupes de restauration par compte	5

Entité	Quota
Nombre de cellules par compte	15
Nombre de cellules imbriquées par cellule	3
Nombre de cellules par groupe de récupération	3
Nombre de ressources par cellule	10
Nombre de ressources par groupe de restauration	10
Nombre de ressources par ensemble de ressources	6
Nombre d'ensembles de ressources par compte	200
Nombre de contrôles de préparation par compte	200
Nombre d'autorisations entre comptes	100

Exemples de code pour Application Recovery Controller utilisant des AWS SDK

Les exemples de code suivants montrent comment utiliser Application Recovery Controller 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 et dans des exemples interservices.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation de ce service 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

- Actions pour Application Recovery Controller à l'aide de AWS kits de développement logiciel
  - Utilisation GetRoutingControlState avec un AWS SDK ou une CLI
  - Utilisation UpdateRoutingControlState avec un AWS SDK ou une CLI

Actions pour Application Recovery Controller à l'aide de AWS kits de développement logiciel

Les exemples de code suivants montrent comment effectuer des actions individuelles d'Application Recovery Controller avec des AWS SDK. Ces extraits appellent l'API Application Recovery Controller et sont des extraits de code de programmes plus volumineux qui doivent être exécutés en contexte. 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 une liste complète, consultez le manuel de référence de l'API Amazon Route 53 Application Recovery Controller.

Exemples

- Utilisation GetRoutingControlState avec un AWS SDK ou une CLI

- Utilisation UpdateRoutingControlState avec un AWS SDK ou une CLI

Utilisation **`GetRoutingControlState`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`GetRoutingControlState`.

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 GetRoutingControlStateResponse
 getRoutingControlState(List<ClusterEndpoint> clusterEndpoints,
            String routingControlArn) {
        // As a best practice, we recommend choosing a random cluster endpoint to
 get or
        // set routing control states.
        // For more information, see
        // https://docs.aws.amazon.com/r53recovery/latest/dg/route53-arc-best-
practices.html#route53-arc-best-practices.regional
        Collections.shuffle(clusterEndpoints);
        for (ClusterEndpoint clusterEndpoint : clusterEndpoints) {
            try {
                System.out.println(clusterEndpoint);
                Route53RecoveryClusterClient client =
 Route53RecoveryClusterClient.builder()
                        .endpointOverride(URI.create(clusterEndpoint.endpoint()))
                        .region(Region.of(clusterEndpoint.region())).build();
                return client.getRoutingControlState(
                        GetRoutingControlStateRequest.builder()
                                .routingControlArn(routingControlArn).build());
            } catch (Exception exception) {
                System.out.println(exception);
            }
        }
        return null;
```

```
    }
```

- Pour plus de détails sur l'API, reportez-vous GetRoutingControlStateà la section Référence des AWS SDK for Java 2.x API.

Python

SDK pour Python (Boto3)

> **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 boto3


def create_recovery_client(cluster_endpoint):
    """
    Creates a Boto3 Route 53 Application Recovery Controller client for the
 specified
    cluster endpoint URL and AWS Region.

    :param cluster_endpoint: The cluster endpoint URL and Region.
    :return: The Boto3 client.
    """
    return boto3.client(
        "route53-recovery-cluster",
        endpoint_url=cluster_endpoint["Endpoint"],
        region_name=cluster_endpoint["Region"],
    )



def get_routing_control_state(routing_control_arn, cluster_endpoints):
    """
    Gets the state of a routing control. Cluster endpoints are tried in
    sequence until the first successful response is received.
```

```
    :param routing_control_arn: The ARN of the routing control to look up.
    :param cluster_endpoints: The list of cluster endpoints to query.
    :return: The routing control state response.
    """

    # As a best practice, we recommend choosing a random cluster endpoint to get
 or set routing control states.
    # For more information, see https://docs.aws.amazon.com/r53recovery/latest/
dg/route53-arc-best-practices.html#route53-arc-best-practices.regional
    random.shuffle(cluster_endpoints)
    for cluster_endpoint in cluster_endpoints:
        try:
            recovery_client = create_recovery_client(cluster_endpoint)
            response = recovery_client.get_routing_control_state(
                RoutingControlArn=routing_control_arn
            )
            return response
        except Exception as error:
            print(error)
            raise error
```

- Pour plus de détails sur l'API, consultez GetRoutingControlStatele AWS manuel de référence de l'API SDK for Python (Boto3).

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation de ce service avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`UpdateRoutingControlState`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`UpdateRoutingControlState`.

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 UpdateRoutingControlStateResponse
 updateRoutingControlState(List<ClusterEndpoint> clusterEndpoints,
            String routingControlArn,
            String routingControlState) {
        // As a best practice, we recommend choosing a random cluster endpoint to
 get or
        // set routing control states.
        // For more information, see
        // https://docs.aws.amazon.com/r53recovery/latest/dg/route53-arc-best-
practices.html#route53-arc-best-practices.regional
        Collections.shuffle(clusterEndpoints);
        for (ClusterEndpoint clusterEndpoint : clusterEndpoints) {
            try {
                System.out.println(clusterEndpoint);
                Route53RecoveryClusterClient client =
 Route53RecoveryClusterClient.builder()
                        .endpointOverride(URI.create(clusterEndpoint.endpoint()))
                        .region(Region.of(clusterEndpoint.region()))
                        .build();
                return client.updateRoutingControlState(
                        UpdateRoutingControlStateRequest.builder()

 .routingControlArn(routingControlArn).routingControlState(routingControlState).build());
            } catch (Exception exception) {
                System.out.println(exception);
            }
        }
        return null;
    }
```

- Pour plus de détails sur l'API, reportez-vous UpdateRoutingControlStateà la section Référence des AWS SDK for Java 2.x API.

Python

SDK pour Python (Boto3)

> **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 boto3


def create_recovery_client(cluster_endpoint):
    """
    Creates a Boto3 Route 53 Application Recovery Controller client for the
 specified
    cluster endpoint URL and AWS Region.

    :param cluster_endpoint: The cluster endpoint URL and Region.
    :return: The Boto3 client.
    """
    return boto3.client(
        "route53-recovery-cluster",
        endpoint_url=cluster_endpoint["Endpoint"],
        region_name=cluster_endpoint["Region"],
    )



def update_routing_control_state(
    routing_control_arn, cluster_endpoints, routing_control_state
):
    """
    Updates the state of a routing control. Cluster endpoints are tried in
    sequence until the first successful response is received.
```

```
    :param routing_control_arn: The ARN of the routing control to update the
 state for.
    :param cluster_endpoints: The list of cluster endpoints to try.
    :param routing_control_state: The new routing control state.
    :return: The routing control update response.
    """

    # As a best practice, we recommend choosing a random cluster endpoint to get
 or set routing control states.
    # For more information, see https://docs.aws.amazon.com/r53recovery/latest/
dg/route53-arc-best-practices.html#route53-arc-best-practices.regional
    random.shuffle(cluster_endpoints)
    for cluster_endpoint in cluster_endpoints:
        try:
            recovery_client = create_recovery_client(cluster_endpoint)
            response = recovery_client.update_routing_control_state(
                RoutingControlArn=routing_control_arn,
                RoutingControlState=routing_control_state,
            )
            return response
        except Exception as error:
            print(error)
```

- Pour plus de détails sur l'API, consultez UpdateRoutingControlStatele AWS manuel de référence de l'API SDK for Python (Boto3).

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation de ce service avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Sécurité dans le contrôleur de restauration d'applications Amazon Route 53

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez de centres de données et d'architectures 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 cela comme la sécurité du cloud et la 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 AWS conformité Programmes de de conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent à Amazon Route 53 Application Recovery Controller, consultez la section AWS Services concernés par programme de conformitéAWS .
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation de Route 53 ARC. Les rubriques suivantes expliquent comment configurer Route 53 ARC 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 ARC de la Route 53.

Rubriques

Protection des données dans Amazon Route 53 Application Recovery Controller

Le modèle de responsabilité AWS partagée s'applique à la protection des données dans Amazon Route 53 Application Recovery Controller. 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.
- Utilisez le protocole SSL/TLS pour communiquer avec les ressources. AWS Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail.
- 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 140-2 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 (Federal Information Processing Standard) disponibles, consultez Federal Information Processing Standard (FIPS) 140-2 (Normes de traitement de l'information fédérale).

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 Name (Nom). Cela inclut lorsque vous travaillez avec Route 53 ARC ou autre à Services AWS l'aide de la console, de l'API ou AWS des SDK. 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.

Chiffrement au repos

Les informations de configuration du client sont stockées dans des tables globales Amazon DynamoDB appartenant au service et sont chiffrées au repos.

Les ensembles de données contenant l'état des cellules d'un cluster Route 53 ARC sont écrits sur un volume Amazon EBS pour être sauvegardés. Route 53 ARC utilise le chiffrement Amazon EBS par défaut lorsque les données sont au repos.

Chiffrement en transit

Les demandes et réponses des clients (relatives à la configuration de la Route 53 ARC, aux requêtes relatives à l'état de préparation, aux mises à jour de l'état des cellules, etc.) sont chiffrées pendant le transport dans l'ensemble du service à l'aide du protocole TLS.

Identity and Access Management pour le contrôleur de restauration d'applications Amazon Route 53

AWS Identity and Access Management (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les ressources ARC de la Route 53. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez dans Route 53 ARC.

Utilisateur du service : si vous utilisez le service Route 53 ARC pour effectuer votre travail, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez

besoin. Au fur et à mesure que vous utilisez de plus en plus de fonctionnalités ARC de Route 53 pour effectuer votre travail, vous aurez peut-être besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne pouvez pas accéder à une fonctionnalité dans Route 53 ARC, consultezRésolution des problèmes d'identité et d'accès à Amazon Route 53 Application Recovery Controller.

Administrateur du service — Si vous êtes responsable des ressources de la Route 53 ARC au sein de votre entreprise, vous avez probablement un accès complet à la Route 53 ARC. C'est à vous de déterminer les fonctionnalités et les ressources de la Route 53 ARC auxquelles les utilisateurs du service doivent accéder. Vous devez ensuite soumettre les demandes à votre administrateur IAM pour modifier les autorisations des utilisateurs de votre service. Consultez les informations sur cette page pour comprendre les concepts de base d'IAM. Pour en savoir plus sur la manière dont votre entreprise peut utiliser IAM avec Route 53 ARC, consultezComment les fonctionnalités d'Amazon Route 53 Application Recovery Controller fonctionnent avec IAM.

Administrateur IAM : si vous êtes administrateur IAM, vous souhaiterez peut-être en savoir plus sur la manière dont vous pouvez rédiger des politiques pour gérer l'accès à Route 53 ARC. Pour consulter des exemples de politiques basées sur l'identité ARC de la Route 53 que vous pouvez utiliser dans IAM, consultez. Exemples de politiques basées sur l'identité dans Amazon Route 53 Application Recovery Controller

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 vous-même les demandes, consultez la section Signature des demandes AWS 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 en savoir plus, consultez Authentification multifactorielle dans le Guide de l'utilisateur AWS IAM Identity Center et Utilisation de l'authentification multifactorielle (MFA) dans l'interface AWS 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 root, consultez Tâches nécessitant des informations d'identification d'utilisateur root 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 une seule 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 tels que les 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 de faire pivoter les 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 avoir un groupe nommé IAMAdmins et accorder à ce groupe les autorisations d'administrer des 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 en savoir plus, consultez Quand créer un utilisateur IAM (au lieu d'un rôle) 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. Vous pouvez assumer temporairement un rôle IAM dans le en AWS Management Console changeant de rôle. 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 Utilisation de rôles IAM 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 la rubrique 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 Différence entre les rôles IAM et les politiques basées sur les ressources 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 la politique relative à la transmission de demandes FAS, consultez Sessions de transmission 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 une fonction du 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 instance EC2 et qui envoient des demandes d'API. AWS CLI AWS Cette solution est préférable au stockage des clés d’accès au sein de l’instance EC2. Pour attribuer un AWS rôle à une instance EC2 et le mettre à la disposition de 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 qui s’exécutent sur l’instance EC2 d’obtenir des informations d’identification temporaires. Pour plus d’informations, consultez Utilisation d’un rôle IAM pour accorder des autorisations à des applications s’exécutant sur des instances Amazon EC2 dans le Guide de l’utilisateur IAM.

Pour savoir dans quel cas utiliser des rôles ou des utilisateurs IAM, consultez Quand créer un rôle IAM (au lieu d’un utilisateur) dans le Guide de l’utilisateur IAM.

Gestion des accès à l’aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique est un objet AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal (utilisateur, utilisateur root ou session de rôle) fait une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d’informations sur la structure et le contenu des documents de politique JSON, consultez Vue d’ensemble des politiques JSON dans le Guide de l’utilisateur IAM.

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Les politiques IAM définissent les autorisations d'une action, quelle que soit la méthode que vous utilisez pour exécuter l'opération. Par exemple, supposons que vous disposiez d'une politique qui autorise l'action `iam:GetRole`. Un utilisateur appliquant cette politique peut obtenir des informations sur le rôle à partir de AWS Management Console AWS CLI, de ou de l' AWS API.

Politiques basées sur l'identité

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Création de politiques IAM dans le Guide de l'utilisateur IAM.

Les politiques basées sur l'identité peuvent être classées comme des politiques en ligne ou des politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les politiques gérées sont des politiques autonomes que vous pouvez associer à plusieurs utilisateurs, groupes et rôles au sein de votre Compte AWS. Les politiques gérées incluent les politiques AWS gérées et les politiques gérées par le client. Pour découvrir comment choisir entre une politique gérée et une politique en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les

ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les politiques AWS gérées par IAM dans une stratégie basée sur les ressources.

Listes de contrôle d'accès (ACL)

Les listes de contrôle d'accès (ACL) vérifie quels principals (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Amazon S3 et Amazon VPC sont des exemples de services qui prennent en charge les ACL. AWS WAF Pour en savoir plus sur les listes de contrôle d'accès, consultez Vue d'ensemble des listes de contrôle d'accès (ACL) dans le Guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de politiques moins courants. Ces types de politiques peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants.

- Limite d'autorisations : une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le nombre maximal d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM (utilisateur ou rôle IAM). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations en résultant représentent la combinaison des politiques basées sur l'identité d'une entité et de ses limites d'autorisation. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques remplace l'autorisation. Pour plus d'informations sur les limites d'autorisations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.
- Politiques de contrôle des services (SCP) — Les SCP sont des politiques JSON qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans. AWS Organizations AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée Comptes AWS les multiples propriétés de votre entreprise. Si vous activez toutes les fonctionnalités d'une organisation, vous pouvez appliquer les politiques de contrôle des services (SCP) à l'un ou à l'ensemble de vos comptes. Le SCP limite les autorisations pour les entités

figurant dans les comptes des membres, y compris chacune Utilisateur racine d'un compte AWS d'entre elles. Pour plus d'informations sur les organisations et les SCP, consultez Fonctionnement des SCP dans le Guide de l'utilisateur AWS Organizations .

- Politiques de séance : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de séance en résultant sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations, consultez politiques de séance dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de l'utilisateur IAM.

Comment les fonctionnalités d'Amazon Route 53 Application Recovery Controller fonctionnent avec IAM

Pour plus d'informations sur le fonctionnement de chaque fonctionnalité d'Amazon Route 53 Application Recovery Controller avec IAM, consultez les rubriques suivantes :

- IAM pour le changement de zone
- IAM pour l'autoshift zonal
- IAM pour le contrôle du routage
- IAM pour la vérification de l'état de préparation

Exemples de politiques basées sur l'identité dans Amazon Route 53 Application Recovery Controller

Pour consulter des exemples de politiques basées sur l'identité pour chaque fonctionnalité d'Amazon Route 53 Application Recovery Controller, consultez les rubriques suivantes dans les AWS Identity and Access Management chapitres consacrés à chaque fonctionnalité :

- Exemples de politiques basées sur l'identité pour le changement automatique zonal
- Exemples de politiques basées sur l'identité pour le changement de zone dans Amazon Route 53 Application Recovery Controller
- Exemples de politiques basées sur l'identité pour le contrôle du routage dans Amazon Route 53 Application Recovery Controller
- Exemples de politiques basées sur l'identité pour le contrôle de l'état de préparation dans Amazon Route 53 Application Recovery Controller

AWS politiques gérées pour Amazon Route 53 Application Recovery Controller

Pour plus d'informations sur les politiques AWS gérées pour les fonctionnalités d'Amazon Route 53 Application Recovery Controller avec des politiques gérées, y compris une politique gérée pour un rôle lié à un service, consultez les rubriques suivantes :

- Politiques gérées pour l'autoshift zonal
- Politiques gérées pour le contrôle du routage
- Politiques gérées pour le contrôle de l'état de préparation

Mises à jour des politiques AWS gérées pour Amazon Route 53 Application Recovery Controller

Consultez les détails des mises à jour des politiques AWS gérées relatives aux fonctionnalités de Route 53 ARC depuis que ce service a commencé à suivre ces modifications. Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au fil RSS sur la page d'historique du document ARC Route 53.

Modification	Description	Date
AWSServiceRoleForPercPracticePolicy— Nouvelle politique	Route 53 ARC a ajouté un nouveau rôle lié au service pour le passage automatique et les courses d'entraînement. Route 53 ARC utilise les autorisations activées	30 novembre 2023

Modification	Description	Date
	par le rôle lié au service pour surveiller les alarmes CloudWatch Amazon fournies par le AWS Health Dashboard client et les événements clients pour les essais, et pour démarrer les essais. Pour en savoir plus sur le nouveau rôle lié à un service, consultez. Autorisations de rôle liées à un service pour AWSServiceRoleForZonalAutoshiftPracticeRun	
AmazonRoute53 RecoveryControl ConfigRead OnlyAccess — Politique mise à jour	Ajoute des autorisations pour`GetResourcePolicy` , afin de permettre le renvoi de détails sur les politiques de AWS Resource Access Manager ressources pour les ressources partagées.	18 octobre 2023

Modification	Description	Date

Politique Route53 — RecoveryReadiness ServiceRole Politique mise à jour	Route 53 ARC a ajouté de nouvelles autorisations pour demander des informations sur les instances Amazon EC2.
	
	Route 53 ARC utilise les autorisations suivantes pour permettre d'interroger les instances Amazon EC2, d'exécuter des contrôles de préparation et de détermine r l'état de préparation des instances.
	
	`ec2:DescribeVpnGat eways`
	
	`ec2:DescribeCustom erGateways`
		17 février 2023

Modification	Description	Date
Politique Route53 — RecoveryReadiness ServiceRole Politique mise à jour	Route 53 ARC a ajouté une nouvelle autorisation pour demander des informations sur les fonctions Lambda. Route 53 ARC utilise l'autorisation suivante pour demander des informations sur les fonctions Lambda afin d'exécuter des contrôles de disponibilité et de déterminer l'état de préparation des fonctions. `lambda:ListProvisionedConcurrencyConfigs`	31 août 2022
AmazonRoute5.3 RecoveryControl ConfigFull Accès — Politique mise à jour	Suppression des autorisations Amazon Route 53 de la politique et ajout d'une note répertoriant les autorisations facultatives.	26 mai 2022
AmazonRoute5.3 RecoveryControl ConfigFull Accès — Politique mise à jour	Les autorisations Amazon Route 53 manquantes ont été ajoutées à la politique.	15 avril 2022
AmazonRoute5.3 RecoveryCluster ReadOnly Accès — Politique mise à jour	Route 53 ARC a ajouté une nouvelle autorisation`route53-recovery-cluster:ListRoutingControls` , pour permettre de répertorier les ARN de contrôle de routage à haute disponibilité.	15 mars 2022

Modification	Description	Date
AmazonRoute53 RecoveryControl ConfigRead OnlyAccess — Politique mise à jour	Route 53 ARC a ajouté une nouvelle autorisation `route53-recovery-control-config:ListTagsForResources`, permettant de répertorier les balises d'une ressource.	20 décembre 2021
Politique Route53 — RecoveryReadiness ServiceRole Politique mise à jour	Route 53 ARC a ajouté une nouvelle autorisation pour demander des informations sur Amazon API Gateway. Route 53 ARC utilise l'autorisation `apigateway:GET`, pour demander des informations sur API Gateway afin d'exécuter des contrôles de préparation et de déterminer l'état de préparation.	28 octobre 2021

Modification	Description	Date
AmazonRoute5.3 RecoveryReadiness ReadOnly Accès — Ajout de nouvelles autorisations	Route 53 ARC a ajouté deux nouvelles autorisations à AmazonRoute53 RecoveryReadiness ReadOnly Access : Route 53 ARC utilise `route53-recovery-readiness:GetArchitectureRecommendations` et `route53-recovery-readiness:GetCellReadinessSummary` pour autoriser un accès en lecture seule à ces actions pour travailler sur la préparation à la restauration.	15 octobre 2021

Modification	Description	Date

Politique Route53 — RecoveryReadiness ServiceRole Politique mise à jour	Route 53 ARC a ajouté de nouvelles autorisations pour demander des informations sur les fonctions Lambda.
	
	Route 53 ARC utilise les autorisations suivantes pour demander des informations sur les fonctions Lambda afin d'exécuter des contrôles de disponibilité et de déterminer l'état de préparation de ces fonctions.
	
	`lambda:GetFunctionConcurrency`
	
	`lambda:GetFunctionConfiguration`
	
	`lambda:GetProvisionedConcurrencyConfig`
	
	`lambda:ListAliases`
	
	`lambda:ListVersionsByFunction`
	
	`lambda:ListEventSourceMappings`
	
	`lambda:ListFunctions`
		8 octobre 2021

Modification	Description	Date
Politique Route53 — Ajout de nouvelles RecoveryReadiness ServiceRole politiques gérées	Route 53 ARC a ajouté les nouvelles politiques gérées suivantes : AmazonRoute53 RecoveryReadiness FullAccess AmazonRoute5.3 RecoveryReadiness ReadOnly Accès AmazonRoute53 RecoveryCluster FullAccess AmazonRoute5.3 RecoveryCluster ReadOnly Accès AmazonRoute5.3 RecoveryControl ConfigFull Accès AmazonRoute53 RecoveryControl ConfigRead OnlyAccess	18 août 2021
Route 53 ARC a commencé à suivre les modifications	Route 53 ARC a commencé à suivre les modifications apportées AWS à ses politiques gérées.	27 Juillet 2021

Résolution des problèmes d'identité et d'accès à Amazon Route 53 Application Recovery Controller

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec Amazon Route 53 Application Recovery Controller et IAM.

Rubriques

- Je ne suis pas autorisé à effectuer une action dans Route 53 ARC

- Je ne suis pas autorisé à effectuer iam : PassRole
- Je souhaite permettre à des personnes extérieures Compte AWS à moi d'accéder à mes ressources ARC de la Route 53

Je ne suis pas autorisé à effectuer une action dans Route 53 ARC

S'il vous AWS Management Console indique que vous n'êtes pas autorisé à effectuer une action, vous devez contacter votre administrateur pour obtenir de l'aide. Votre administrateur est la personne qui vous a fourni vos informations d'identification.

L'exemple d'erreur suivant se produit quand l'utilisateur IAM `mateojackson` tente d'utiliser la console pour afficher des informations détaillées sur une ressource *`my-example-widget`* fictive, mais ne dispose pas des autorisations `route53-recovery-readiness:`*`GetWidget`* fictives.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 route53-recovery-readiness:GetWidget on resource: my-example-widget
```

Dans ce cas, Mateo demande à son administrateur de mettre à jour ses politiques pour lui permettre d'accéder à la ressource *`my-example-widget`* à l'aide de l'action `route53-recovery-readiness:`*`GetWidget`*.

Je ne suis pas autorisé à effectuer iam : PassRole

Si vous recevez un message d'erreur indiquant que vous n'êtes pas autorisé à effectuer l'`iam:PassRole`action, vos politiques doivent être mises à jour pour vous permettre de transmettre un rôle à Route 53 ARC.

Certains vous Services AWS permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, un utilisateur doit disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un utilisateur IAM nommé `marymajor` essaie d'utiliser la console pour effectuer une action dans Route 53 ARC. Toutefois, l'action nécessite que le service ait des autorisations accordées par un rôle de service. Mary ne dispose pas des autorisations nécessaires pour transférer le rôle au service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je souhaite permettre à des personnes extérieures Compte AWS à moi d'accéder à mes ressources ARC de la Route 53

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACL), vous pouvez utiliser ces politiques pour donner l'accès à vos ressources.

Pour en savoir plus, consultez les éléments suivants :

- Pour savoir si Route 53 ARC prend en charge ces fonctionnalités, consultezComment les fonctionnalités d'Amazon Route 53 Application Recovery Controller fonctionnent avec IAM.
- Pour savoir comment fournir l'accès à vos ressources sur celles Comptes AWS que vous possédez, consultez la section Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.
- Pour découvrir quelle est la différence entre l'utilisation des rôles et l'utilisation des politiques basées sur les ressources pour l'accès entre comptes, consultez Différence entre les rôles IAM et les politiques basées sur les ressources dans le Guide de l'utilisateur IAM.

Journalisation et surveillance dans Amazon Route 53 Application Recovery Controller

La surveillance joue un rôle important dans le maintien de la disponibilité et des performances d'Amazon Route 53 Application Recovery Controller et 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. AWS fournit plusieurs outils pour surveiller les ressources et l'activité de votre Route 53 ARC, et pour répondre aux incidents potentiels, par exemple, AWS CloudTrail et Amazon CloudWatch.

Pour plus d'informations sur la surveillance de chaque fonctionnalité de Route 53 ARC, consultez les rubriques suivantes :

- Enregistrement et surveillance pour le changement de zone
- Enregistrement et surveillance pour le changement automatique zonal
- Journalisation et surveillance pour le contrôle du routage
- Enregistrement et surveillance pour vérifier l'état de préparation

Validation de conformité pour Amazon Route 53 Application Recovery Controller

Des auditeurs tiers évaluent la sécurité et la conformité d'Amazon Route 53 Application Recovery Controller dans le cadre de plusieurs programmes de AWS conformité. Il s'agit notamment des certifications SOC, PCI, HIPAA.

Pour savoir si un programme Services AWS de conformité Service AWS s'inscrit dans le champ d'application de programmes de conformité spécifiques, consultez Services AWS la section de conformité et sélectionnez le programme de conformité qui vous intéresse. Pour des informations générales, voir Programmes de AWS conformité Programmes AWS de .

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, voir Téléchargement de rapports dans AWS Artifact .

Votre responsabilité en matière de conformité lors de l'utilisation Services AWS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise et les lois et réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- 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 AWS la sécurité et la conformité.

- Architecture axée sur la sécurité et la conformité HIPAA sur Amazon Web Services : ce livre blanc décrit comment les entreprises peuvent créer des applications AWS conformes à la loi HIPAA.

> **Note**
>
> Tous ne Services AWS sont pas éligibles à la loi HIPAA. Pour plus d'informations, consultez le HIPAA Eligible Services Reference.

- AWS Ressources de https://aws.amazon.com/compliance/resources/ de conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- AWS Guides de conformité destinés aux clients — Comprenez le modèle de responsabilité partagée sous l'angle de la conformité. Les guides résument les meilleures pratiques en matière de sécurisation Services AWS et décrivent les directives relatives aux contrôles de sécurité dans de nombreux cadres (notamment le National Institute of Standards and Technology (NIST), le Payment Card Industry Security Standards Council (PCI) et l'Organisation internationale de normalisation (ISO)).
- Évaluation des ressources à l'aide des règles du guide du AWS Config développeur : le AWS Config 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— Cela Service AWS fournit une vue complète de votre état de sécurité interne AWS. Security Hub utilise des contrôles de sécurité pour évaluer vos ressources AWS et vérifier votre conformité par rapport aux normes et aux bonnes pratiques du secteur de la sécurité. Pour obtenir la liste des services et des contrôles pris en charge, consultez Référence des contrôles Security Hub.
- Amazon GuardDuty — Cela Service AWS détecte les menaces potentielles qui pèsent sur vos charges de travail Comptes AWS, vos conteneurs et vos données en surveillant votre environnement pour détecter toute activité suspecte et malveillante. GuardDuty peut vous aider à répondre à diverses exigences de conformité, telles que la norme PCI DSS, en répondant aux exigences de détection des intrusions imposées par certains cadres de conformité.
- AWS Audit Manager— Cela vous Service AWS permet d'auditer en permanence votre AWS utilisation afin de simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

Résilience dans le contrôleur de restauration d'applications Amazon Route 53

L'infrastructure AWS mondiale est construite autour Régions AWS de zones de disponibilité. Régions AWS 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 à l'autre sans interruption. Les zones de disponibilité sont davantage disponibles, tolérantes aux pannes et ont une plus grande capacité de mise à l'échelle que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur les zones de disponibilité Régions AWS et les zones de disponibilité, consultez la section Infrastructure AWS globale.

Outre l'infrastructure AWS mondiale, Route 53 ARC propose plusieurs fonctionnalités pour répondre à vos besoins en matière de résilience et de sauvegarde des données.

Sécurité de l'infrastructure dans Amazon Route 53 Application Recovery Controller

En tant que service géré, Amazon Route 53 Application Recovery Controller 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 la Route 53 ARC 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.

Historique du document relatif au guide du développeur Amazon Route 53 Application Recovery Controller

Les entrées suivantes décrivent les modifications importantes apportées à la documentation d'Amazon Route 53 Application Recovery Controller.

- Version : dernière
- Dernière mise à jour de la documentation : 30 avril 2024

Modification	Description	Date
Réorganisation des documents en fonction de chaque fonctionnalité	Réorganise le contenu du guide du développeur pour le cloisonner dans des guides de sous-développement . En d'autres termes, des sections distinctes contiennent désormais des informations complètes pour chaque fonctionnalité de Route 53 ARC : changement de zone et décalage automatique de zone pour la restauration multi-AZ, et contrôle du routage et vérification de l'état de préparation pour la restauration multirégionale. Pour plus d'informations, consultez Qu'est-ce qu'Amazon Route 53 Application Recovery Controller ?	30 avril 2024

Modification	Description	Date
Ajoute une capacité de changement automatique zonal	Ajoute une nouvelle fonctionn alité dans Route 53 ARC dans laquelle vous autorisez AWS le transfert du trafic des ressources d'une application depuis une zone de disponibi lité, en votre nom, afin de réduire le temps de restaurat ion en cas d'événements. Pour plus d'informations, consultez la section Zonal Autoshift dans Amazon Route 53 Application Recovery Controller.	30 novembre 2023
Ajoute un nouveau rôle lié à un service	Ajoute un nouveau rôle lié au service AWSServiceRoleForZ onalAutoshiftPracticeRun, pour les essais pratiques de changement automatique zonaux. Pour plus d'informations, consultez la section Autorisat ions de rôle liées à un service pour. AWSServiceRoleForZ onalAutoshiftPracticeRun	30 novembre 2023

Modification	Description	Date
Ajoute le support multi-comptes pour les clusters	Ajoute la prise en charge multicompte pour les clusters de Route 53 ARC with AWS Resource Access Manager, afin que vous puissiez utiliser facilement et en toute sécurité un cluster pour héberger des panneaux de contrôle et des contrôles de routage appartenant à plusieurs AWS comptes différents. Pour plus d'informations, consultez la section Support des comptes croisés pour les clusters dans Route 53 ARC.	18 octobre 2023
Met à jour une politique gérée	Met à jour la politique `AmazonRoute53RecoveryControlConfigReadOnly` gérée pour ajouter des autorisations`GetResourcePolicy`, afin de permettre le renvoi de détails sur les politiques de AWS Resource Access Manager ressources pour les ressources partagées . Pour plus d'informations, consultez la section Politiques AWS gérées.	19 septembre 2023

Modification	Description	Date
Rôle lié à un service mis à jour	De nouvelles autorisations ont été ajoutées `ec2:DescribeVpnGateways` et `ec2:DescribeCustomerGateways` , au rôle lié au service pour Route 53 ARC, la prise en charge de l'interrogation des instances Amazon EC2. Pour plus d'informations, consultez la section Utilisation de rôles liés à un service pour Route 53 ARC.	17 février 2023
Déclenchement GA pour changement de zone	Prend en charge la version GA du décalage de zone pour Route 53 ARC, qui inclut le contrôle d'accès basé sur les attributs (ABAC) pour les ressources gérées enregistrées dans Route 53 ARC pour le décalage zonal. Pour plus d'informations, consultez la section Contrôle d'accès basé sur les attributs (ABAC) avec Route 53 ARC.	10 janvier 2023

Modification	Description	Date
Ajout d'un nouveau changement de zone multi-AZ	Ajout de contenu décrivant un nouveau service dans Route 53 ARC, le changement de zone, pour les applications multi-AZ. Vous pouvez commencer un changement de zone pour déplacer temporairement le trafic d'une ressource d'équilibrage de charge hors d'une zone de disponibilité. Pour plus d'informations, voir Déplacement de zone dans Route 53 ARC.	28 novembre 2022
Rôle lié à un service mis à jour	Ajout d'une nouvelle autorisation au rôle lié au service permettant à Route 53 ARC de demander des informations sur les fonctions Lambda. `lambda:ListProvisionedConcurrencyConfigs` Pour plus d'informations, consultez la section Utilisation de rôles liés à un service pour Route 53 ARC.	31 août 2022

Modification	Description	Date
Politique gérée mise à jour	Mise à jour de la politique `AmazonRoute53RecoveryControlConfigFullAccess` gérée pour supprimer les autorisations Amazon Route 53 et les répertorier comme facultatives. Pour plus d'informations, consultez les politiques AWS gérées pour Amazon Route 53 Application Recovery Controller.	26 mai 2022
Politique gérée mise à jour	Mise à jour de la politique `AmazonRoute53RecoveryControlConfigFullAccess` gérée pour inclure les autorisations Amazon Route 53 requises. Pour plus d'informations, consultez les politiques AWS gérées pour Amazon Route 53 Application Recovery Controller.	15 avril 2022

Modification	Description	Date
Exemple de CLI ajouté pour la nouvelle API de contrôles de routage de liste	Ajout d'un exemple de commande CLI et de recommandations de bonnes pratiques pour le nouveau fonctionnement de l'API de contrôle de routage de liste inclus dans l'API extrêmement fiable du plan de données Route 53 ARC. Pour plus d'informations, voir Répertorier et mettre à jour les contrôles et les états de routage.	31 mars 2022
Support supplémentaire pour contourner les règles de sécurité	Ajout de la prise en charge du contournement des règles de sécurité, ce qui vous permet de contourner les mesures de contrôle de routage appliquées par les règles de sécurité que vous avez configurées. Des dérogations aux règles de sécurité peuvent être nécessaires, par exemple, dans un scénario de « rupture de vitre » lors d'un basculement en cas de reprise après sinistre. Pour plus d'informations, consultez la section Remplacer les règles de sécurité pour rediriger le trafic.	2 mars 2022

Modification	Description	Date
Ajout d'un support de balisage supplémentaire	Ajout de la prise en charge du balisage de ressource s supplémentaires dans Route 53 ARC, notamment les clusters, les panneaux de commande, les contrôles de routage et les règles de sécurité. Pour plus d'informations, consultez la section Balisage dans Amazon Route 53 Application Recovery Controller.	20 décembre 2021
Politique gérée mise à jour	Mise à jour de la politique `AmazonRoute53RecoveryControlConfigReadOnly` gérée pour ajouter l'autorisation de répertorier les balises d'une ressource. Pour plus d'informations, consultez les politiques AWS gérées pour Amazon Route 53 Application Recovery Controller	20 décembre 2021

Modification	Description	Date
Ajout de la prise en charge des alertes en temps réel avec EventBridge	Ajout de la prise en charge EventBridge, ce qui signifie que vous pouvez désormais ajouter des règles pour recevoir des alertes et agir en cas de modification de l'état de préparation de la Route 53 ARC, par exemple lorsqu'un statut passe de PRÊT à PAS PRÊT. Pour plus d'informations, consultez la section Utilisation de Route 53 ARC avec Amazon EventBridge.	20 décembre 2021
Exemples de code d'état de contrôle de routage ajoutés	Des exemples de code ont été ajoutés pour illustrer l'essai séquentiel des points de terminaison du cluster lorsque vous utilisez des opérations d'API pour obtenir ou mettre à jour des états de contrôle de routage. Pour plus d'informations, consultez les exemples d'API pour Amazon Route 53 Application Recovery Controller.	16 novembre 2021

Modification	Description	Date
Ajout de nouvelles autorisations à une politique de lecture seule	Deux nouvelles autorisations ont été ajoutées à la politique `AmazonRoute53RecoveryReadinessReadOnlyAccess` : `route53-recovery-readiness:GetArchitectureRecommendations` et `route53-recovery-readiness:GetCellReadinessSummary`. Pour plus d'informations, consultez les politiques AWS gérées pour Amazon Route 53 Application Recovery Controller.	9 novembre 2021
Ajout de la prise en charge du type de ressource Amazon API Gateway	Ajout d'un nouveau type de ressource, Amazon API Gateway, et mise à jour des autorisations de rôle liées au service Route 53 ARC afin que Route 53 ARC puisse auditer API Gateway à l'aide de contrôles de préparation. Pour plus d'informations, consultez les sections Règles de préparation et types de ressources pris en charge et Utilisation de rôles liés à un service pour Route 53 ARC.	28 octobre 2021

Modification	Description	Date
Ajout du support pour le type de ressource des fonctions Lambda	Ajout d'un nouveau type de ressource, les fonctions Lambda, et mise à jour des autorisations de rôle liées au service Route 53 ARC afin que Route 53 ARC puisse auditer les fonctions Lambda en vérifiant leur disponibilité. Pour plus d'informations, consultez les sections Règles de préparation et types de ressources pris en charge et Utilisation de rôles liés à un service pour Route 53 ARC.	8 octobre 2021
Liens CloudFormation et modèles Terraform ajoutés	Ajout de liens vers des modèles téléchargeables AWS CloudFormation et des modèles Hashicorp Terraform pour vous aider à démarrer rapidement avec Route 53 Arc. Pour plus d'informations, voir Préparation à la restauration avec une nouvelle application.	13 septembre 2021

Modification	Description	Date
Ajout de nouvelles politiques gérées	Les politiques AWS gérées suivantes ont été ajoutées pour Route 53 ARC : `AmazonRoute53RecoveryReadinessFullAccess` `AmazonRoute53RecoveryReadinessReadOnlyAccess` ,`AmazonRoute53RecoveryClusterFullAccess` ,`AmazonRoute53RecoveryClusterReadOnlyAccess` ,`AmazonRoute53RecoveryControlConfigFullAccess` , et`AmazonRoute53RecoveryControlConfigReadOnlyAccess` . Pour plus d'informations, consultez les politiques AWS gérées pour Amazon Route 53 Application Recovery Controller.	18 août 2021

Modification	Description	Date
J'ai commencé AWS à suivre les politiques gérées pour Amazon Route 53 Application Recovery Controller	Les mises à jour des politiques gérées seront suivies à partir de la date de publication initiale. Pour plus d'informations, consultez les politiques AWS gérées pour Amazon Route 53 Application Recovery Controller.	27 Juillet 2021
Version initiale d'Amazon Route 53 Application Recovery Controller	Route 53 ARC améliore la disponibilité des applications en coordonnant de manière centralisée les basculements au sein d'une AWS région ou entre plusieurs régions. Route 53 ARC fournit des contrôles de préparation pour garantir que vos applications sont dimensionnées pour gérer le trafic de basculement et configurées pour contourner les défaillances. Il fournit également un contrôle de routage extrêmement fiable qui vous permet de récupérer les applications en réacheminant le trafic, par exemple entre les zones de disponibilité ou les régions. Pour plus d'informations, consultez Qu'est-ce que la Route 53 ARC ? .	27 Juillet 2021

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.