aws

Guide du développeur

Contrôleur Amazon Application Recovery (ARC)

Contrôleur Amazon Application Recovery (ARC): Guide du développeur

Table of Contents

Qu'est-ce que l'ARC ?

Amazon Application Recovery Controller (ARC) vous aide à préparer et à effectuer une restauration plus rapide pour les applications exécutées sur l'infrastructure cloud AWS mondiale.

ARC fournit les fonctionnalités suivantes :

- Restauration dans une zone de disponibilité multiple (AZ), y compris le changement de zone et le changement automatique de zone, qui vous permettent de récupérer en cas de défaillance d'une seule zone en transférant temporairement le trafic d'une zone Z altérée vers une zone saine.
- Restauration multirégionale, qui inclut le contrôle du routage et le changement de région pour la restauration des applications régionales, ainsi que le contrôle de l'état de préparation pour la surveillance des applications.

Restauration dans une zone de multidisponibilité

Déplacement zonal

Vous pouvez utiliser le décalage de zone ARC pour isoler et rétablir rapidement les défaillances d'une seule zone de disponibilité (AZ). Le changement de zone déplace temporairement le trafic d'une ressource prise en charge d'une AZ altérée vers un trafic sain AZs dans la même AWS région. 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 dans AWS une seule zone de disponibilité. Le fait de déplacer le trafic en dehors de la zone de zone affectée réduit l'impact pour les clients qui utilisent votre application dans la zone de zone affectée.

Vous pouvez commencer un changement de zone pour n'importe quelle ressource prise en charge sur votre compte dans une AWS région. Les changements de zone sont manuels et temporaires. Lorsque vous commencez un changement de zone, vous devez spécifier un délai d'expiration (extensible) pouvant aller jusqu'à trois jours. Pour activer le changement de zone pour les ressources prises en charge, reportez-vous àRessources prises en charge.

Autoshift zonal

L'autoshift zonal ARC autorise le transfert du trafic AWS d'une AZ altérée pour les ressources prises en charge, en votre nom, vers un trafic sain AZs dans la même région. AWS AWS lance un changement automatique de zone lorsque la télémétrie interne indique qu'il existe une anomalie dans

une AZ d'une AWS 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 décalages automatiques zonaux sont temporaires. AWS met fin à un changement automatique de zone lorsque les indicateurs de télémétrie internes indiquent qu'il n'y a plus de problème réel ou potentiel.

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

- Changement de zone dans ARC
- Changement de zone automatique dans ARC

Restauration multirégionale

Changement de région

Le changement de région dans ARC fournit une solution centralisée, automatisée et observable pour la restauration d'applications multirégionales. Le changement de région vous aide à planifier et à coordonner la restauration de vos applications dans l'ensemble Régions AWS, afin de garantir la continuité des activités et de réduire les frais d'exploitation.

Vous pouvez utiliser le changement de région pour orchestrer des tâches de restauration complexes et à grande échelle pour les ressources de votre application, sur plusieurs AWS comptes. En cas Région AWS de panne, les plans que vous créez à l'aide du changement de région peuvent basculer ou transférer vos ressources vers une autre région, afin que votre application puisse continuer à fonctionner en toute sécurité Région AWS.

Contrôle du routage

Les contrôles de routage extrêmement fiables d'ARC permettent une restauration multirégionale afin que vos applications puissent basculer le trafic DNS du système de noms de domaine entre les régions AWS .

Si votre application est conçue pour fonctionner à partir de plusieurs AWS régions, vous pouvez utiliser le contrôle de routage ARC pour basculer entre les régions. Le contrôle du routage vous permet de transférer le trafic d'une AWS région affectée vers une AWS région saine, 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 imprévus en imposant des garde-corps que vous définissez vous-

même. Par exemple, vous pouvez imposer une règle de sécurité selon laquelle une seule des répliques de vos applications, active ou en veille, est activée et utilisée.

Contrôle de préparation

Le contrôle de préparation à l'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 application répliquée et à vous remettre en état après une détérioration de la région. Des contrôles de disponibilité continus garantissent que vous pouvez maintenir vos applications multirégionales dans un état adapté et configuré pour gérer le trafic de basculement. Le contrôle de préparation est utile lorsque vous configurez 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 :

- Changement de région dans ARC
- Contrôle du routage dans ARC
- Vérification de l'état de préparation dans ARC

Modification de la disponibilité du test de disponibilité d'Amazon Application Recovery Controller (ARC)

> **Note**
>
> La fonctionnalité de vérification du niveau de préparation d'Amazon Application Recovery Controller (ARC) ne sera plus ouverte aux nouveaux clients à compter du 30 avril 2026. Les clients existants peuvent continuer à utiliser le service normalement.

Après mûre réflexion, nous avons décidé de fermer la fonctionnalité de vérification du niveau de préparation d'Amazon Application Recovery Controller (ARC) aux nouveaux clients à compter du 30 avril 2026. Les clients existants peuvent continuer à utiliser le service normalement.

La vérification de l'état de préparation de l'ARC est une fonctionnalité qui vous permet de contrôler l'état de préparation de vos ressources en cas de reprise après sinistre. ARC est toujours disponible, mais la fonction de vérification de l'état de préparation ne sera plus ouverte aux nouveaux clients à compter du 30 avril 2026.

> **Note**
>
> L'ARC et le changement de région ARC continuent d'être entièrement pris en charge. Seule la fonction de vérification de l'état de préparation est affectée par cette modification. Aucune modification n'est apportée au changement de région, aux commandes de routage, au décalage de zone et au décalage automatique de zone.

Options de migration

Pour des fonctionnalités similaires à la vérification de l'état de préparation, nous vous recommandons d'intégrer votre application multirégionale au changement de région ARC.

Le commutateur de région ARC est un service entièrement géré qui fournit une orchestration complète de la restauration multirégionale. Il inclut une fonctionnalité appelée évaluation du plan, qui surveille régulièrement l'état de votre plan de changement de région afin de garantir qu'il est prêt à être exécuté.

Pour commencer à utiliser le changement de région ARC, voirChangement de région dans ARC.

Comparez les fonctionnalités de restauration multi-AZ et multirégionales dans ARC

Le changement de zone, le décalage automatique de zone, le contrôle du routage et le changement de région dans Amazon Application Recovery Controller (ARC) peuvent tous permettre une restauration rapide et vous aider à garantir la résilience de vos applications. AWS Ces fonctionnalités sont hautement disponibles et aident à prendre en charge la restauration dans les scénarios où votre application connaît une latence accrue ou une disponibilité réduite. Ces fonctionnalités permettent également 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 et le changement de région se concentrent sur AWS les applications multirégionales, tandis que le décalage de zone et le décalage automatique de zone ne prennent en charge que le transfert de trafic pour les ressources prises en charge par les applications multi-AZ. Régions AWS

Les informations du tableau suivant incluent certaines des principales fonctionnalités des capacités de résilience de l'ARC. Ces descriptions peuvent vous aider à mieux comprendre comment une option spécifique peut être la meilleure solution pour les besoins de votre application.

Contrôle du routage	Changement de région	Changement de zone	Autoshift zonal
Régional Réachemine le trafic d'une AWS région à une autre (principa lement)	Régional Réachemine le trafic d'une AWS région à une autre (principa lement)	Zonal 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	Zonal 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	Nécessite une configuration	Peut nécessiter une configuration	Nécessite une configuration

Contrôle du routage	Changement de région	Changement de zone	Autoshift zonal
Nécessite une configuration et un paramétrage	Nécessite une configuration et un paramétrage	Nécessite l'inscription à certaines ressources prises en charge Pour plus d'informations, reportez-vous à Ressources prises en charge	Doit être activé pour une ressource prise en charge Pour plus d'informations, reportez-vous à Ressources prises en charge
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 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	Basé sur des frais Nécessite des frais distincts pour les forfaits de changement de région	Inclus avec les services (sans frais supplémentaires) La création de décalages zonaux pour éloigner le trafic AZs est incluse pour les ressources prises en charge	Inclus avec les services (sans frais supplémentaires) Le démarrage des transferts automatiques pour déplacer le trafic en votre AZs nom est inclus dans les ressources prises en charge
N'expire pas Le trafic peut être redirigé indéfiniment vers une réplique	N'expire pas L'application peut être déplacée 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 ARC
- Changement de zone automatique dans ARC
- Contrôle du routage dans ARC
- Changement de région dans ARC

Utilisez le décalage de zone et le décalage automatique de zone pour récupérer des applications dans ARC

Cette section explique comment utiliser les fonctionnalités d'Amazon Application Recovery Controller (ARC) pour récupérer de manière fiable vos AWS ressources en cas de problème dans une zone de disponibilité (AZ) altérée. Le changement de zone et le décalage automatique de zone déplacent temporairement le trafic d'une ressource prise en charge vers une zone de zone endommagée, ce qui réduit 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 prise en charge vers ou Région AWS hors d'une zone de disponibilité.
- Avec l'autoshift zonal, le trafic d'une ressource prise en charge est automatiquement transféré hors d'une AZ altérée et redirigé vers un trafic sain AZs dans la même région. AWS

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 ARC

Le changement de zone d'Amazon Application Recovery Controller (ARC) vous permet de transférer le trafic d'une ressource prise en charge d'une zone de disponibilité altérée (AZ) Région AWS vers une zone saine AZs dans la même région. Le fait de déplacer le trafic de vos ressources en dehors d'une zone de zone endommagée réduit 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, et contribue à atténuer les problèmes et à restaurer rapidement votre application. Vous pouvez choisir de déplacer le trafic, par exemple, parce qu'un mauvais déploiement entraîne des problèmes de latence ou parce que la zone de disponibilité est défaillante.

Vous devez activer les ressources pour utiliser le changement de zone. Pour plus d'informations, consultez Ressources prises en charge.

Avant de commencer un changement de zone, vous devez réaliser une mise à l'échelle de votre application et vous assurer que vous disposez d'une capacité suffisante pour déplacer le trafic hors d'une zone de disponibilité. Après le prédimensionnement, vous pouvez choisir la zone de disponibilité à partir de laquelle vous souhaitez vous éloigner et la ressource vers laquelle vous souhaitez déplacer le trafic, puis commencer le changement de zone. Vous pouvez annuler le changement à tout moment pour que le trafic commence à revenir à la zone de disponibilité d'origine. Pour de plus amples informations, consultez Bonnes pratiques pour le changement de zone dans ARC.

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, comprise entre une minute et trois jours (72 heures), que vous pouvez prolonger si vous devez poursuivre le transfert de trafic.

Dans certains scénarios, le changement de zone n'éloigne pas le trafic de l'AZ. Pour de plus amples informations, veuillez consulter Ressources prises en charge.

Comment fonctionne un changement de zone

Lorsque vous commencez un changement de zone pour une ressource prise en charge, le trafic de cette ressource est déplacé hors de la zone de disponibilité (AZ) que vous avez spécifiée. Les ressources prises en charge par l'ARC fournissent des intégrations qui signalent l'AZ spécifié comme étant en mauvais état, ce qui entraîne un déplacement du trafic vers l'AZ altéré.

Le trafic commence à changer - Lorsque vous commencez un changement de zone dans ARC, 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 prendre un certain temps, en fonction du comportement du client et de la réutilisation des connexions. Les paramètres DNS et d'autres facteurs, y compris les connexions existantes, peuvent être terminés en quelques minutes, mais ils peuvent prendre plus de temps. Pour plus d'informations, consultez la section Veiller à ce que les changements de trafic se terminent rapidement.

Fin du transfert de trafic - Lorsqu'un changement de zone expire ou que vous l'annulez, l'ARC prend des mesures pour arrêter le transfert de trafic et inverse le processus de démarrage d'un changement de trafic. Désormais, l'AZ récupéré est reconnu comme étant disponible pour la ressource et le trafic reprend 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.

Lorsque le trafic ne s'éloigne pas : dans certains scénarios, un changement de zone ne déplace pas le trafic depuis la zone de disponibilité. Supposons, par exemple, que vous commenciez un changement de zone pour un équilibreur de charge lorsque les groupes cibles de l'équilibreur de charge AZs n'ont aucune instance ou si toutes les instances ne fonctionnent pas correctement. Dans ce scénario, l'équilibreur de charge est en état d'ouverture automatique et le lancement d'un changement de zone n'entraîne pas de perte de trafic.

Avant de commencer un changement de zone pour une ressource, assurez-vous que toutes les conditions d'un changement de zone réussi sont réunies. AWS les ressources gèrent différemment les changements de zone. Pour plus d'informations sur la prise en charge du décalage zonal, consultezRessources prises en charge.

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 Application Recovery Controller (ARC), consultez la section Points de terminaison et quotas Amazon Application Recovery Controller (ARC) dans le manuel Amazon Web Services General Reference.

Le changement de zone et le changement automatique de zone sont actuellement disponibles dans la Régions AWS liste ci-dessous. Le changement de zone et le changement automatique de zone sont également disponibles dans les régions de Chine, à savoir les régions de Chine (Pékin) et de Chine (Ningxia). Les ressources qui utilisent Amazon Application Recovery Controller (ARC) peuvent présenter des considérations supplémentaires. Pour plus d’informations, consultez Ressources prises en charge.

Nom de la région	Région	Point de terminaison	Protocole	
US East (Ohio)	us-east-2	arc-zonal-shift.us-east-2.amazonaws.com	HTTPS	
		arc-zonal-shift-fips.us-east-2.api.aws	HTTPS	

Nom de la région	Région	Point de terminaison	Protocole
		arc-zonal-shift.us-east-2.api.aws	HTTPS
USA Est (Virginie du Nord)	us-east-1	arc-zonal-shift.us-east-1.amazonaws.com	HTTPS
		arc-zonal-shift-fips.us-east-1.api.aws	HTTPS
		arc-zonal-shift.us-east-1.api.aws	HTTPS
USA Ouest (Californie du Nord)	us-west-1	arc-zonal-shift.us-west-1.amazonaws.com	HTTPS
		arc-zonal-shift-fips.us-west-1.api.aws	HTTPS
		arc-zonal-shift.us-west-1.api.aws	HTTPS
US West (Oregon)	us-west-2	arc-zonal-shift.us-west-2.amazonaws.com	HTTPS
		arc-zonal-shift-fips.us-west-2.api.aws	HTTPS
		arc-zonal-shift.us-west-2.api.aws	HTTPS
Afrique (Le Cap)	af-south-1	arc-zonal-shift.af-south-1.amazonaws.com	HTTPS
		arc-zonal-shift.af-south-1.api.aws	HTTPS
Asie-Pacifique (Hong Kong)	ap-east-1	arc-zonal-shift.ap-east-1.amazonaws.com	HTTPS
		arc-zonal-shift.ap-east-1.api.aws	HTTPS
Asie-Pacifique (Hyderabad)	ap-south-2	arc-zonal-shift.ap-south-2.amazonaws.com	HTTPS
		arc-zonal-shift.ap-south-2.api.aws	HTTPS
Asie-Pacifique (Jakarta)	ap-southeast-3	arc-zonal-shift.ap-southeast-3.amazonaws.com	HTTPS
		arc-zonal-shift.ap-southeast-3.api.aws	HTTPS

Nom de la région	Région	Point de terminaison	Protocole
Asie-Pacifique (Malaisie)	ap-southeast-5	arc-zonal-shift.ap-southeast-5.amazonaws.com arc-zonal-shift.ap-southeast-5.api.aws	HTTPS HTTPS
Asie-Pacifique (Melbourne)	ap-southeast-4	arc-zonal-shift.ap-southeast-4.amazonaws.com arc-zonal-shift.ap-southeast-4.api.aws	HTTPS HTTPS
Asia Pacific (Mumbai)	ap-south-1	arc-zonal-shift.ap-south-1.amazonaws.com arc-zonal-shift.ap-south-1.api.aws	HTTPS HTTPS
Asie-Pacifique (Nouvelle Zélande)	ap-southeast-6	arc-zonal-shift.ap-southeast-6.amazonaws.com arc-zonal-shift.ap-southeast-6.api.aws	HTTPS HTTPS
Asie-Pacifique (Osaka)	ap-northeast-3	arc-zonal-shift.ap-northeast-3.amazonaws.com arc-zonal-shift.ap-northeast-3.api.aws	HTTPS HTTPS
Asia Pacific (Seoul)	ap-northeast-2	arc-zonal-shift.ap-northeast-2.amazonaws.com arc-zonal-shift.ap-northeast-2.api.aws	HTTPS HTTPS
Asie-Pacifique (Singapour)	ap-southeast-1	arc-zonal-shift.ap-southeast-1.amazonaws.com arc-zonal-shift.ap-southeast-1.api.aws	HTTPS HTTPS
Asia Pacific (Sydney)	ap-southeast-2	arc-zonal-shift.ap-southeast-2.amazonaws.com arc-zonal-shift.ap-southeast-2.api.aws	HTTPS HTTPS

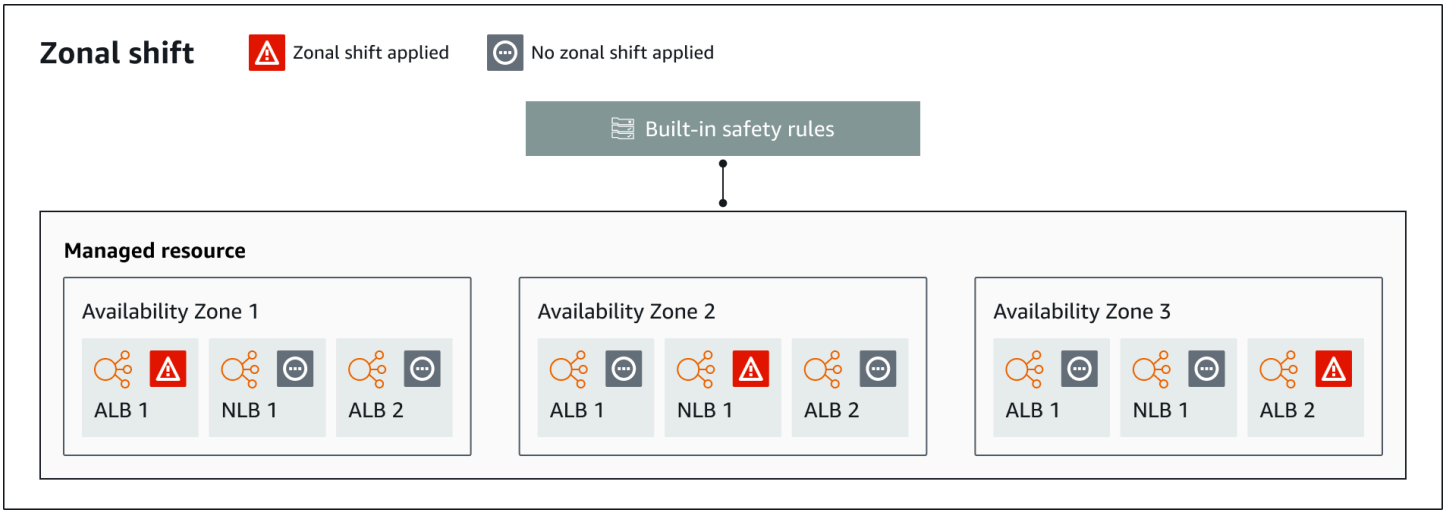
Nom de la région	Région	Point de terminaison	Protocole
Asie-Pacifique (Taipei)	ap-east-2	arc-zonal-shift.ap-east-2.amazonaws.com	HTTPS
		arc-zonal-shift.ap-east-2.api.aws	HTTPS
Asie-Pacifique (Thaïlande)	ap-southeast-7	arc-zonal-shift.ap-southeast-7.amazonaws.com	HTTPS
		arc-zonal-shift.ap-southeast-7.api.aws	HTTPS
Asie-Pacifique (Tokyo)	ap-northeast-1	arc-zonal-shift.ap-northeast-1.amazonaws.com	HTTPS
		arc-zonal-shift.ap-northeast-1.api.aws	HTTPS
Canada (Centre)	ca-central-1	arc-zonal-shift.ca-central-1.amazonaws.com	HTTPS
		arc-zonal-shift-fips.ca-central-1.api.aws	HTTPS
		arc-zonal-shift.ca-central-1.api.aws	HTTPS
Canada-Ouest (Calgary)	ca-west-1	arc-zonal-shift.ca-west-1.amazonaws.com	HTTPS
		arc-zonal-shift-fips.ca-west-1.api.aws	HTTPS
		arc-zonal-shift.ca-west-1.api.aws	HTTPS
Europe (Francfort)	eu-central-1	arc-zonal-shift.eu-central-1.amazonaws.com	HTTPS
		arc-zonal-shift.eu-central-1.api.aws	HTTPS
Europe (Irlande)	eu-west-1	arc-zonal-shift.eu-west-1.amazonaws.com	HTTPS
		arc-zonal-shift.eu-west-1.api.aws	HTTPS
Europe (Londres)	eu-west-2	arc-zonal-shift.eu-west-2.amazonaws.com	HTTPS
		arc-zonal-shift.eu-west-2.api.aws	HTTPS

Nom de la région	Région	Point de terminaison	Protocole
Europe (Milan)	eu-south-1	arc-zonal-shift.eu-south-1.amazonaws.com	HTTPS
		arc-zonal-shift.eu-south-1.api.aws	HTTPS
Europe (Paris)	eu-west-3	arc-zonal-shift.eu-west-3.amazonaws.com	HTTPS
		arc-zonal-shift.eu-west-3.api.aws	HTTPS
Europe (Espagne)	eu-south-2	arc-zonal-shift.eu-south-2.amazonaws.com	HTTPS
		arc-zonal-shift.eu-south-2.api.aws	HTTPS
Europe (Stockholm)	eu-north-1	arc-zonal-shift.eu-north-1.amazonaws.com	HTTPS
		arc-zonal-shift.eu-north-1.api.aws	HTTPS
Europe (Zurich)	eu-central-2	arc-zonal-shift.eu-central-2.amazonaws.com	HTTPS
		arc-zonal-shift.eu-central-2.api.aws	HTTPS
Israël (Tel Aviv)	il-central-1	arc-zonal-shift.il-central-1.amazonaws.com	HTTPS
		arc-zonal-shift.il-central-1.api.aws	HTTPS
Mexique (Centre)	mx-central-1	arc-zonal-shift.mx-central-1.amazonaws.com	HTTPS
		arc-zonal-shift.mx-central-1.api.aws	HTTPS
Moyen-Orient (Bahreïn)	me-south-1	arc-zonal-shift.me-south-1.amazonaws.com	HTTPS
		arc-zonal-shift.me-south-1.api.aws	HTTPS
Moyen-Orient (EAU)	me-central-1	arc-zonal-shift.me-central-1.amazonaws.com	HTTPS
		arc-zonal-shift.me-central-1.api.aws	HTTPS

Nom de la région	Région	Point de terminaison	Protocole
Amérique du Sud (São Paulo)	sa-east-1	arc-zonal-shift.sa-east-1.amazonaws.com arc-zonal-shift.sa-east-1.api.aws	HTTPS HTTPS
AWS GovCloud (USA Est)	us-gov-east-1	arc-zonal-shift.us-gov-east-1.amazonaws.com arc-zonal-shift-fips.us-gov-east-1.api.aws arc-zonal-shift.us-gov-east-1.api.aws	HTTPS HTTPS HTTPS
AWS GovCloud (US-Ouest)	us-gov-west-1	arc-zonal-shift.us-gov-west-1.amazonaws.com arc-zonal-shift-fips.us-gov-west-1.api.aws arc-zonal-shift.us-gov-west-1.api.aws	HTTPS HTTPS HTTPS

Composants de changement de zone

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 dans 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 située dans une zone de disponibilité vers une Région AWS zone saine AZs dans la région, afin de remédier rapidement à un problème dans une zone de disponibilité. Pour plus d'informations sur les ressources prises en charge pour le changement de zone, reportez-vous àRessources prises en charge.

Contrôles de sécurité intégrés

Les contrôles intégrés à l'ARC empêchent que plusieurs transferts de trafic pour une ressource soient effectués à la fois. En d'autres termes, un seul changement de zone, un entraînement ou un transfert automatique initié par le client 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 Changement de zone automatique dans ARC 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.

Dans le cas d'un changement de zone, vous ne pouvez sélectionner les ressources de votre compte que pour un AWS service pris en charge par l'ARC. Pour plus d'informations sur les ressources prises en charge pour le changement de zone, reportez-vous àRessources prises en charge.

Ressource gérée

Certaines AWS ressources doivent accepter manuellement le changement de zone, tandis que d'autres sont automatiquement activées. Pour plus d'informations sur les ressources prises en charge pour le changement de zone, reportez-vous àRessources prises en charge.

Nom de la ressource

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

État (statut de changement de zone)

Un statut pour un changement de zone. `Status`Pour un décalage de zone, vous pouvez 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.

Type de quart de travail

Définit le type de décalage zonal. Les valeurs `shiftType` peuvent être les suivantes :

- ZONAL_SHIFT
- ZONAL_AUTOSHIFT
- PRACTICE_RUN
- FIS_EXPERIMENT

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, vous pouvez initialement définir un décalage 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 l'ARC convertit en date d'expiration (heure d'expiration). Vous pouvez annuler un changement de zone, 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 les essais d'entraînement relatifs au changement de zone qui font partie du 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 l'ARC

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 n'entraîne aucun frais supplémentaire.

Pour obtenir des informations détaillées sur la tarification de l'ARC et des exemples de tarification, consultez la section Tarification de l'ARC.

Bonnes pratiques pour le changement de zone dans ARC

Nous recommandons les meilleures pratiques suivantes pour utiliser les décalages de zone pour la restauration multi-AZ dans ARC.

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 de manière temporaire

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 entamez un changement de zone pour une ressource prise en charge et que le trafic est transféré hors d'une zone AZ, la capacité utilisée par votre application pour traiter les demandes est supprimée. Vous devez vous assurer que vous avez prévu un transfert de trafic en dehors d'un AZ et que vous pouvez continuer à traiter les demandes pendant le reste AZs.

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

Lorsqu'Amazon Application Recovery Controller (ARC) 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 ARC pour déplacer le trafic de votre application est une mise à jour du 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.

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 initiaux, 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 ressources de 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.

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 de manière temporaire

Un changement de zone déplace le trafic hors d'une zone de disponibilité de façon temporaire, afin d'atténuer les perturbations. 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 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 comprend 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 ARC	Utilisation de l'API ARC
Lancement d'un changement de zone	Consultez Lancement d'un changement de zone	Consultez StartZonalShift
Mise à jour d'un changement de zone	Consultez Mise à jour ou annulation d'un changement de zone	Consultez UpdateZonalShift
Répertorier les décalages de zone	Consultez Changement de zone dans ARC	Consultez ListZonalShifts
Répertorier les ressources gérées	Consultez Ressources prises en charge	Consultez ListManagedResources
Obtenez une ressource gérée	Consultez Ressources prises en charge	Consultez GetManagedResource
Annulation d'un changement de zone	Consultez Mise à jour ou annulation d'un changement de zone	Consultez CancelZonalShift

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

Cette section fournit des exemples d'applications utilisant le décalage de zone, en utilisant la fonctionnalité AWS Command Line Interface de décalage de zone d'Amazon Application Recovery Controller (ARC) 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 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

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:elasticloadbalancing:us-
east-1:111122223333:loadbalancer/app/Testing/5a19403ecd42dc05 \
       --away-from use1-az1 \
       --expires-in 10m \
       --comment "Shifting traffic away from use1-az1"
```

```
{
    "awayFrom": "use1-az1",
    "comment": "Shifting traffic away from use1-az1",
    "expiryTime": "2024-12-17T21:37:26-08:00",
    "resourceIdentifier": "arn:aws:elasticloadbalancing:us-
east-1:111122223333:loadbalancer/app/Testing/5a19403ecd42dc05",
    "startTime": "2024-12-17T21:27:26-08:00",
    "status": "ACTIVE",
    "zonalShiftId": "9ac9ec1e-1df1-0755-3dc5-8cf573cd9c38"
}
```

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:elasticloadbalancing:us-
east-1:111122223333:loadbalancer/app/Testing/5a19403ecd42dc05
```

```
{
    "appliedWeights": {
        "use1-az1": 0.0,
        "use1-az2": 1.0,
```

```
        "use1-az6": 1.0
    },
    "arn": "arn:aws:elasticloadbalancing:us-east-1:111122223333:loadbalancer/app/
Testing/5a19403ecd42dc05",
    "autoshifts": [],
    "name": "Testing",
    "zonalAutoshiftStatus": "DISABLED",
    "zonalShifts": [
        {
            "appliedStatus": "APPLIED",
            "awayFrom": "use1-az1",
            "comment": "Shifting traffic away from use1-az1",
            "expiryTime": "2024-12-17T21:37:26-08:00",
            "resourceIdentifier": "arn:aws:elasticloadbalancing:us-
east-1:111122223333:loadbalancer/app/Testing/5a19403ecd42dc05",
            "startTime": "2024-12-17T21:27:26-08:00",
            "zonalShiftId": "9ac9ec1e-1df1-0755-3dc5-8cf573cd9c38"
            "shiftType": "MANUAL"
        }
    ]
}
```

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": [
        {
            "appliedWeights": {
                "use1-az1": 0.0,
                "use1-az2": 1.0,
                "use1-az6": 1.0
            },
            "arn": "arn:aws:elasticloadbalancing:us-east-1:111122223333:loadbalancer/
app/Testing/5a19403ecd42dc05",
            "autoshifts": [],
            "availabilityZones": [
                "use1-az1",
```

```
                "use1-az2",
                "use1-az6"
            ],
            "name": "Testing",
            "practiceRunStatus": "DISABLED",
            "zonalAutoshiftStatus": "DISABLED",
            "zonalShifts": [
                {
                    "appliedStatus": "APPLIED",
                    "awayFrom": "use1-az1",
                    "comment": "Shifting traffic away from use1-az1",
                    "expiryTime": "2024-12-17T21:37:26-08:00",
                    "resourceIdentifier": "arn:aws:elasticloadbalancing:us-
east-1:111122223333:loadbalancer/app/Testing/5a19403ecd42dc05",
                    "startTime": "2024-12-17T21:27:26-08:00",
                    "zonalShiftId": "9ac9ec1e-1df1-0755-3dc5-8cf573cd9c38"
                }
            ]
        }
    ]
}
```

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": [
        {
            "awayFrom": "use1-az1",
            "comment": "Shifting traffic away from use1-az1",
            "expiryTime": "2024-12-17T21:37:26-08:00",
            "resourceIdentifier": "arn:aws:elasticloadbalancing:us-
east-1:111122223333:loadbalancer/app/Testing/5a19403ecd42dc05",
            "startTime": "2024-12-17T21:27:26-08:00",
            "status": "ACTIVE",
            "zonalShiftId": "9ac9ec1e-1df1-0755-3dc5-8cf573cd9c38"
        }
    ]
```

```
}
```

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 9ac9ec1e-1df1-0755-3dc5-8cf573cd9c38 \
       --expires-in 1h \
       --comment "Still shifting traffic away from use1-az1"
```

```
{
    "awayFrom": "use1-az1",
    "comment": "Still shifting traffic away from use1-az1",
    "expiryTime": "2024-12-17T22:29:38-08:00",
    "resourceIdentifier": "arn:aws:elasticloadbalancing:us-
east-1:111122223333:loadbalancer/app/Testing/5a19403ecd42dc05",
    "startTime": "2024-12-17T21:27:26-08:00",
    "status": "ACTIVE",
    "zonalShiftId": "9ac9ec1e-1df1-0755-3dc5-8cf573cd9c38"
}
```

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 9ac9ec1e-1df1-0755-3dc5-8cf573cd9c38
```

```
{
    "awayFrom": "use1-az1",
    "comment": "Still shifting traffic away from use1-az1",
    "expiryTime": "2024-12-17T22:29:38-08:00",
    "resourceIdentifier": "arn:aws:elasticloadbalancing:us-
east-1:111122223333:loadbalancer/app/Testing/5a19403ecd42dc05",
    "startTime": "2024-12-17T21:27:26-08:00",
    "status": "CANCELED",
    "zonalShiftId": "9ac9ec1e-1df1-0755-3dc5-8cf573cd9c38"
```

```
}
```

Ressources prises en charge

Amazon Application Recovery Controller (ARC) prend actuellement en charge l'activation des ressources suivantes pour le changement de zone et le décalage automatique de zone :

- Groupes Amazon EC2 Auto Scaling
- Amazon Elastic Kubernetes Service
- Application Load Balancersavec équilibrage de charge entre zones activé ou désactivé
- Network Load Balancersavec équilibrage de charge entre zones activé ou désactivé

Pour connaître les exigences spécifiques relatives aux équilibreurs de charge réseau et aux équilibreurs de charge d'application, consultez les rubriques supplémentaires de cette section.

Passez en revue les conditions suivantes pour utiliser les décalages de zone, le décalage automatique de zone et les ressources dans ARC :

- 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 ARC. Par exemple, consultez la liste des ressources gérées dans le AWS Management Console ou utilisez l'`get-managed-resource`opération avec l'identifiant de la ressource.
- 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 de l'AZ que vous souhaitez quitter, 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 de plus amples informations, veuillez consulter IAM et autorisations pour le changement de zone.
- Lorsqu'un Network Load Balancer ou un Application Load Balancer est en état d'ouverture défaillante, un changement de zone n'a aucun effet. Ce comportement est normal, car le changement de zone ne peut pas forcer un AZ à ne pas fonctionner correctement, puis déplacer le trafic vers l'autre AZs dans une région lorsqu'un équilibreur de charge ne s'ouvre pas. Pour plus d'informations, consultez les sections Utilisation du basculement DNS Route 53 pour votre

équilibreur de charge dans le Guide de l'utilisateur des équilibreurs de charge réseau et Utilisation du basculement DNS Route 53 pour votre équilibreur de charge dans le Guide de l'utilisateur des équilibreurs de charge d'application.

- Si plusieurs équilibreurs de charge transfèrent le trafic vers les mêmes cibles, un décalage de zone sur un équilibreur de charge compatible entre zones réduit la capacité cible de tous les équilibreurs de charge, même si leur trafic n'est pas décalé par un décalage de zone.

Groupes Amazon EC2 Auto Scaling

Un groupe Amazon EC2 Auto Scaling contient un ensemble d'instances Amazon EC2 traitées comme un regroupement logique à des fins de dimensionnement et de gestion automatiques. Ils vous permettent également d'utiliser des fonctionnalités Amazon EC2 Auto Scaling telles que les remplacements des surveillances de l'état et des politiques de mise à l'échelle. La mise à l'échelle et le maintien automatiques du nombre d'instances dans un groupe Auto-Scaling constitue la fonctionnalité de base du service Amazon EC2 Auto Scaling.

Utilisation du décalage de zone pour les groupes Auto Scaling

Pour activer le décalage zonal, appliquez l'une des méthodes suivantes.

Console

Pour activer le changement de zone sur un nouveau groupe (console)

1. Suivez les instructions de la section Create an Auto Scaling group using a launch template (Créer un groupe Auto Scaling à l'aide d'un modèle de lancement) et effectuez chaque étape de la procédure, jusqu'à l'étape 10.
2. Sur la page Intégrer à d'autres services, pour le décalage de zone ARC, cochez la case pour activer le décalage de zone.
3. Pour le comportement du bilan de santé, choisissez Ignorer un comportement malsain ou Remplacer un comportement malsain. Si ce paramètre est défini sur`replace-unhealthy`, les instances défectueuses seront remplacées dans la zone de disponibilité par le décalage de zone actif. Si ce paramètre est défini sur`ignore-unhealthy`, les instances défectueuses ne seront pas remplacées dans la zone de disponibilité par le décalage de zone actif.
4. Suivez les étapes décrites dans Create an Auto Scaling group using a launch template.

AWS CLI

Pour activer le décalage de zone sur un nouveau groupe ()AWS CLI

Ajoutez le paramètre `--availability-zone-impairment-policy` à la commande create-auto-scaling-group.

Le `--availability-zone-impairment-policy` paramètre comporte deux options :

- ZonalShiftEnabled— Si ce paramètre est défini sur`true`, Auto Scaling enregistre le groupe Auto Scaling avec le décalage de zone ARC et vous pouvez démarrer, mettre à jour ou annuler un décalage de zone sur la console ARC. S'il est défini sur`false`, Auto Scaling annule l'enregistrement du groupe Auto Scaling du décalage de zone ARC. Le décalage de zone doit déjà être activé pour être réglé sur. `false`
- ImpairedZoneHealthCheckBehavior— Si ce paramètre est défini sur`replace-unhealthy`, les instances défectueuses seront remplacées dans la zone de disponibilité par le décalage de zone actif. Si ce paramètre est défini sur`ignore-unhealthy`, les instances défectueuses ne seront pas remplacées dans la zone de disponibilité par le décalage de zone actif.

L'exemple suivant active le décalage de zone sur un nouveau groupe Auto Scaling nommé*my-asg*.

```
aws autoscaling create-auto-scaling-group \
  --launch-template LaunchTemplateName=my-launch-template,Version='1' \
  --auto-scaling-group-name my-asg \
  --min-size 1 \
  --max-size 10 \
  --desired-capacity 5 \
  --availability-zones us-east-1a us-east-1b us-east-1c \
  --availability-zone-impairment-policy '{
      "ZonalShiftEnabled": true,
      "ImpairedZoneHealthCheckBehavior": IgnoreUnhealthy
    }'
```

Console

Pour activer le changement de zone sur un groupe existant (console)

1. Ouvrez la console Amazon EC2 à l'adresse https://console.aws.amazon.com/ec2/, puis sélectionnez Auto Scaling Groups dans le volet de navigation.
2. Dans la barre de navigation en haut de l'écran, choisissez le groupe dans Région AWS lequel vous avez créé votre groupe Auto Scaling.
3. Cochez la case à côté du groupe Auto Scaling.

   Un volet fractionné s'ouvre en bas de la page.
4. Dans l'onglet Intégrations, sous ARC zonal Shift, choisissez Modifier.
5. Cochez la case pour activer le décalage de zone.
6. Pour le comportement du bilan de santé, choisissez Ignorer un comportement malsain ou Remplacer un comportement malsain.

   - Si le comportement de vérification de l'état est configuré pour ignorer les défaillances, les instances défectueuses ne sont pas remplacées dans la zone de disponibilité par le décalage de zone actif.
   - Si le comportement de vérification de l'état est défini pour remplacer les instances défectueuses, les instances défectueuses sont remplacées dans la zone de disponibilité par le décalage de zone actif.
7. Choisissez Mettre à jour.

AWS CLI

Pour activer le décalage de zone sur un groupe existant ()AWS CLI

Ajoutez le paramètre `--availability-zone-impairment-policy` à la commande update-auto-scaling-group.

Le `--availability-zone-impairment-policy` paramètre comporte deux options :

- ZonalShiftEnabled— Si ce paramètre est défini sur`TRUE`, Auto Scaling enregistre le groupe Auto Scaling avec le décalage de zone ARC et vous pouvez démarrer, mettre à jour ou annuler un décalage de zone sur la console ARC. S'il est défini sur`FALSE`, Auto Scaling annule l'enregistrement du groupe Auto Scaling du décalage de zone ARC. Le décalage de zone doit déjà être activé pour le définir `FALSE` sur.

- ImpairedZoneHealthCheckBehavior— Si ce paramètre est défini sur`replace-unhealthy`, les instances défectueuses seront remplacées dans la zone de disponibilité par le décalage de zone actif. Si ce paramètre est défini sur`ignore-unhealthy`, les instances défectueuses ne seront pas remplacées dans la zone de disponibilité par le décalage de zone actif.

L'exemple suivant active le décalage de zone sur le groupe Auto Scaling spécifié.

```
aws autoscaling update-auto-scaling-group --auto-scaling-group-name my-asg \
  --availability-zone-impairment-policy '{
      "ZonalShiftEnabled": true,
      "ImpairedZoneHealthCheckBehavior": IgnoreUnhealthy
    }'
```

Pour démarrer un changement de zone, voirDémarrer, mettre à jour ou annuler un changement de zone.

Comment fonctionne le décalage de zone pour les groupes Auto Scaling

Supposons que vous disposiez d'un groupe Auto Scaling avec les zones de disponibilité suivantes :

- `us-east-1a`
- `us-east-1b`
- `us-east-1c`

Vous remarquez des défaillances `us-east-1a` et commencez un changement de zone. Les comportements suivants se produisent lorsqu'un changement de zone est initié dans`us-east-1a`.

- Scaling out — Auto Scaling lance toutes les nouvelles demandes de capacité dans les zones de disponibilité saines (`us-east-1b`et`us-east-1c`).
- Dimensionnement dynamique : Auto Scaling empêche les politiques de dimensionnement de réduire la capacité souhaitée. Auto Scaling n'empêche pas les politiques de dimensionnement d'augmenter la capacité souhaitée.
- Actualisation de l'instance — Auto Scaling prolonge le délai d'expiration de tout processus d'actualisation d'instance retardé lors d'un changement de zone actif.

Sélection du comportement de vérification de l'état de la zone de disponibilité altérée	Comportement du bilan de santé
Remplacez les produits mal	Les instances qui semblent défectueuses seront remplacées dans toutes les zones de disponibilité (`us-east-1a us-east-1b` ,, et`us-east-1c`).
Ignorez les mauvaises	Les instances qui semblent défectueuses seront remplacées dans `us-east-1b` et`us-east-1c` . Les instances ne sont pas remplacées dans la zone de disponibilité par le décalage zonal actif (`us-east-1a`).

Bonnes pratiques pour utiliser le décalage de zone

Pour maintenir la haute disponibilité de vos applications lorsque vous utilisez le changement de zone, nous vous recommandons de suivre les meilleures pratiques suivantes.

- Surveillez EventBridge les notifications pour déterminer s'il existe un événement de détérioration continue de la zone de disponibilité. Pour plus d'informations, consultez Automatiser Amazon EC2 Auto Scaling avec. EventBridge
- Utilisez des politiques de dimensionnement avec des seuils appropriés pour vous assurer que vous disposez d'une capacité suffisante pour tolérer la perte d'une zone de disponibilité.
- Définissez une politique de maintenance des instances avec un pourcentage d'instances saines minimum de 100. Avec ce paramètre, Auto Scaling attend qu'une nouvelle instance soit prête à être utilisée avant de mettre fin à une instance défectueuse.

Pour les clients prédimensionnés, nous recommandons également ce qui suit :

- Sélectionnez Ignorer les instances défectueuses comme comportement de contrôle de santé pour la zone de disponibilité altérée, car vous n'avez pas besoin de remplacer l'instance défectueuse lors de l'événement de défaillance.
- Utilisez l'autoshift zonal dans ARC pour vos groupes Auto Scaling. La fonction de transfert automatique zonal Amazon Contrôleur de récupération d’application (ARC) permet de déplacer

le trafic AWS vers une ressource hors d'une zone de disponibilité lorsqu'une déficience est AWS détectée dans une zone de disponibilité. Pour de plus amples informations, veuillez consulter Changement de zone automatique dans ARC.

Pour les clients utilisant des équilibreurs de charge désactivés entre zones, nous recommandons également :

- Utilisez le mode équilibré uniquement pour la distribution de votre zone de disponibilité.
- Si vous utilisez le décalage de zone à la fois sur votre groupe Auto Scaling et sur vos équilibreurs de charge, assurez-vous d'annuler d'abord le décalage de zone sur votre groupe Auto Scaling. Attendez ensuite que la capacité soit équilibrée entre toutes les zones de disponibilité avant d'annuler le changement de zone sur l'équilibreur de charge.
- En raison de la possibilité d'un déséquilibre de capacité lorsque vous activez le décalage de zone et que vous utilisez un équilibreur de charge désactivé entre zones, Auto Scaling dispose d'une validation supplémentaire. Si vous suivez les meilleures pratiques, vous pouvez reconnaître cette possibilité en cochant la case AWS Management Console ou en utilisant le `skip-zonal-shift-validation` drapeau dans `CreateAutoScalingGroup`, `UpdateAutoScalingGroup`, ou`AttachTrafficSources`.

Amazon Elastic Kubernetes Service

Amazon EKS fournit des fonctionnalités qui vous permettent de rendre vos applications plus résilientes face à des événements tels que la détérioration de l'état de santé ou la détérioration d'une zone de disponibilité. Lorsque vous exécutez vos charges de travail dans un cluster Amazon EKS, vous pouvez améliorer encore la tolérance aux pannes de votre environnement applicatif et la restauration des applications en utilisant le décalage zonal ou le décalage automatique zonal.

Utilisation du décalage zonal avec Amazon Elastic Kubernetes Service

Pour activer le décalage zonal, appliquez l'une des méthodes suivantes. Pour plus d'informations, consultez la section En savoir plus sur le décalage zonal ARC dans le guide de l'utilisateur d'Amazon Elastic Kubernetes Service.

Console

Pour activer le changement de zone sur un nouveau cluster Amazon EKS (console)

1. Recherchez le nom et la région du cluster Amazon EKS que vous souhaitez enregistrer auprès de l'ARC.
2. Ouvrez la console Amazon EKS à l'adresse https://console.aws.amazon.com/eks/home#/clusters.
3. Sélectionnez votre cluster.
4. Sur la page Informations sur le cluster, sélectionnez l'onglet Vue d'ensemble.
5. Sous Zonal Shift, sélectionnez Gérer.
6. Pour EKS Zonal Shift, choisissez Activer ou Désactiver.

AWS CLI

Pour activer le changement de zone sur un nouveau cluster Amazon EKS ()AWS CLI

- Entrez la commande suivante :

```
aws eks create-cluster --name my-eks-cluster --role-
arn my-role-arn-to-create-cluster --resources-vpc-config
 subnetIds=string,string,securityGroupIds=string,string,endpointPublicAccess=boolean,end
 --zonal-shift-config enabled=true
```

Pour activer le changement de zone sur un cluster Amazon EKS existant ()AWS CLI

- Entrez la commande suivante :

```
aws eks update-cluster-config --name my-eks-cluster --zonal-shift-config
 enabled=true
```

Vous pouvez démarrer un changement de zone pour un cluster Amazon EKS, ou vous pouvez autoriser AWS à le faire pour vous, en activant le changement automatique de zone. Une fois le changement de zone de votre cluster Amazon EKS activé avec ARC, vous pouvez démarrer un changement de zone ou activer le décalage automatique de zone à l'aide de la console ARC, de la AWS CLI ou du décalage de zone et de décalage automatique de zone. APIs

Pour plus d'informations sur le démarrage d'un changement de zone, consultezDémarrer, mettre à jour ou annuler un changement de zone.

Pour plus d'informations sur l'activation d'Amazon EKS avec le changement de zone, consultez le guide de l'utilisateur d'Amazon Elastic Kubernetes Service pour en savoir plus sur le changement de zone ARC dans Amazon EKS.

Comment fonctionne le changement de zone pour Amazon Elastic Kubernetes Service

Lors d'un changement de zone Amazon EKS, les opérations suivantes se produisent automatiquement :

- Tous les nœuds de la zone de disponibilité affectée sont isolés. Cela empêche le planificateur Kubernetes de planifier de nouveaux pods sur les nœuds de l'AZ malsaine.
- Si vous utilisez des groupes de nœuds gérés, le rééquilibrage des zones de disponibilité est suspendu et votre groupe Auto Scaling est mis à jour pour garantir que les nouveaux nœuds du plan de données Amazon EKS ne soient lancés qu'en bon AZs état.
- Les nœuds de l'AZ malsain ne sont pas interrompus et les pods ne sont pas expulsés de ces nœuds. Cela permet de garantir qu'en cas d'expiration ou d'annulation d'un changement de zone, votre trafic puisse être renvoyé en toute sécurité vers l'AZ qui est encore à pleine capacité.
- Le EndpointSlice contrôleur trouve tous les points de terminaison du Pod dans la zone AZ altérée et les retire de la zone correspondanteEndpointSlices. Cela garantit que seuls les terminaux Pod sains AZs sont ciblés pour recevoir du trafic réseau. Lorsqu'un décalage de zone est annulé ou expire, le EndpointSlice contrôleur le met à jour EndpointSlices pour inclure les points de terminaison dans l'AZ restaurée.

Pour plus d'informations, consultez le blog AWS Containers.

Application Load Balancers

Utilisation du décalage de zone pour les équilibreurs de charge d'application

Pour utiliser les équilibreurs de charge d'application avec décalage de zone, vous devez activer l'intégration du décalage de zone ARC dans les attributs d'Application Load Balancer. Application Load Balancer prend en charge le décalage de zone avec des configurations entre zones activées ou désactivées entre zones.

Avant d'activer l'intégration ARC et de commencer à utiliser le décalage de zone, consultez les informations suivantes :

- Vous pouvez démarrer un changement de zone pour un équilibreur de charge spécifique uniquement pour une zone de disponibilité unique. Vous ne pouvez pas commencer un changement de zone pour plusieurs zones de disponibilité.
- AWS supprime de manière proactive les adresses IP des équilibreurs de charge zonaux du DNS lorsque plusieurs problèmes d'infrastructure ont un impact sur les services. Vérifiez toujours la capacité actuelle de la zone de disponibilité avant de commencer un changement de zone.
- Le changement de zone ne fonctionnera pas pour les groupes cibles mono-AZ.
- Lorsqu'un Application Load Balancer est la cible d'un Network Load Balancer, commencez toujours le changement de zone à partir du Network Load Balancer. Si vous commencez un changement de zone à partir de l'Application Load Balancer, le Network Load Balancer ne reconnaît pas le changement et continue à envoyer du trafic vers l'Application Load Balancer.

Vous pouvez démarrer un changement de zone pour un équilibreur de charge dans la console Elastic Load Balancing (dans la plupart des cas Régions AWS) ou dans la console ARC.

Console

Pour activer le décalage de zone sur un équilibreur de charge (console)

1. Ouvrez la console Amazon EC2 à l'adresse https://console.aws.amazon.com/ec2/.
2. Sur la page de navigation, sous Équilibrage de charge, choisissez Load balancers.
3. Sélectionnez le nom de l'Application Load Balancer.
4. Dans l'onglet Attributs, cliquez sur Modifier.
5. Sous Configuration du routage de la zone de disponibilité, pour >Intégration du décalage zonal ARC, sélectionnez Activer.
6. Choisissez Enregistrer.

AWS CLI

Pour activer le décalage de zone sur un équilibreur de charge ()AWS CLI

- Entrez la commande suivante :

```
aws elbv2 modify-load-balancer-attributes --load-balancer-arn my-alb-arn --
attributes Key=zonal_shift.config.enabled,Value=true
```

Pour plus d'informations sur le démarrage d'un changement de zone, consultezDémarrer, mettre à jour ou annuler un changement de zone.

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.

Comment fonctionne le décalage de zone pour les équilibreurs de charge d'application

Lorsqu'un changement de zone est lancé sur un Application Load Balancer avec l'équilibrage de charge entre zones activé, tout le trafic vers les cibles est bloqué dans la zone de disponibilité concernée, et le changement de zone supprime l'adresse IP zonale du DNS.

Pour plus d'informations, consultez la section Intégrations pour votre Application Load Balancer dans le Guide de l'utilisateur de l'Application Load Balancer.

Network Load Balancers

Utilisation du décalage de zone pour les équilibreurs de charge réseau

Pour utiliser les Network Load Balancers avec décalage zonal, vous devez activer l'intégration du décalage zonal ARC dans les attributs Network Load Balancer. Network Load Balancer prend en charge le décalage de zone avec des configurations activées entre zones ou désactivées entre zones.

Vous pouvez choisir les ressources que vous souhaitez utiliser pour utiliser le changement de zone et le décalage automatique de zone, et à quel moment vous souhaitez ne pas sortir d'une zone de disponibilité altérée. Les équilibreurs de charge réseau internes et connectés à Internet sont pris en charge.

Pour activer le décalage de zone pour votre Network Load Balancer compatible entre zones, tous les groupes cibles attachés à l'équilibreur de charge doivent répondre aux exigences suivantes.

- L'équilibrage de charge entre zones doit être activé ou défini sur. `use_load_balancer_configuration`

  - Pour plus d'informations sur l'équilibrage de charge entre zones du groupe cible, voir Équilibrage de charge entre zones pour les groupes cibles.
- Le protocole du groupe cible doit être TCP ou TLS.
  - Pour plus d'informations sur les protocoles du groupe cible Network Load Balancer, consultez la section Configuration du routage.
- La terminaison de connexion pour les cibles défectueuses doit être désactivée.
  - Pour plus d'informations sur la terminaison de la connexion au groupe cible, voir Interruption de connexion pour les cibles défectueuses.
- Le groupe cible ne doit pas avoir d'équilibreur de charge d'application comme cible.
  - Pour plus d'informations sur les équilibreurs de charge d'application en tant que cibles, voir Utiliser les équilibreurs de charge d'application en tant que cibles d'un Network Load Balancer.

Vous pouvez amorcer un changement de zone pour un Network Load Balancer à l'aide AWS CLI du widget, du ou AWS Management Console du Elastic Load Balancing. Lorsqu'un Application Load Balancer est la cible d'un Network Load Balancer, vous devez commencer 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'arrêtera pas d'envoyer du trafic vers l'Application Load Balancer et ses cibles.

Console

Pour activer le décalage de zone sur un équilibreur de charge (console)

1. Ouvrez la console Amazon EC2 à l’adresse https://console.aws.amazon.com/ec2/.
2. Sur la page de navigation, sous Équilibrage de charge, choisissez Load balancers.
3. Sélectionnez le nom du Network Load Balancer.
4. Dans l'onglet Attributes, choisissez Edit.
5. Sous Configuration du routage de la zone de disponibilité, pour l'intégration du décalage zonal ARC, sélectionnez Activer.
6. Choisissez Enregistrer.

AWS CLI

Pour activer le décalage de zone sur un équilibreur de charge ()AWS CLI

- Entrez la commande suivante :

```
aws elbv2 modify-load-balancer-attributes --load-balancer-arn my-nlb-arn --
attributes Key=zonal_shift.config.enabled,Value=true
```

Pour plus d'informations sur le démarrage d'un changement de zone, consultezDémarrer, mettre à jour ou annuler un changement de zone.

Comment fonctionne le décalage de zone pour les équilibreurs de charge réseau

ARC crée un échec de vérification de l'état du Network Load Balancer enregistré, de sorte que le nœud Network Load Balancer situé dans la zone AZ altérée est supprimé du DNS lorsque vous commencez un changement de zone. Le Network Load Balancer désactive les cibles de la zone affectée afin qu'elles cessent de recevoir du trafic, et Elastic Load Balancing traite ces cibles comme des cibles désactivées pour le changement de zone. Les cibles handicapées continuent de faire l'objet de bilans de santé. Lorsque les cibles sont saines et que le décalage de zone expire (ou est annulé), le routage vers les cibles situées dans la zone précédemment altérée reprend.

Lors du changement de zone sur les équilibreurs de charge réseau lorsque l'équilibrage de charge entre zones est activé, les adresses IP des équilibreurs de charge zonaux sont supprimées du DNS. Les connexions existantes aux cibles situées dans la zone de disponibilité altérée sont maintenues jusqu'à leur fermeture organique, tandis que les nouvelles connexions ne sont plus acheminées vers les cibles situées dans la zone de disponibilité altérée.

Pour plus d'informations, consultez la section Zonal Shift pour votre Network Load Balancer dans le guide de l'utilisateur du Network Load Balancer.

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.

Lancement d’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 Application Recovery Controller (ARC). 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 ARC, vous pouvez également lancer 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 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 à partir de laquelle vous souhaitez déplacer le trafic.
5. Sélectionnez une ressource prise en charge dans le tableau des ressources pour laquelle vous souhaitez transférer 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.

Mise à jour ou annulation d’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 Application

Recovery Controller (ARC). 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 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 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 de zone dans Amazon Application Recovery Controller (ARC)

Vous pouvez l'utiliser AWS CloudTrail pour surveiller le changement de zone dans Amazon Application Recovery Controller (ARC), afin d'analyser les modèles et de résoudre les problèmes.

Rubriques

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

Zonal Shift for ARC est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans 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 ARC et des appels de code vers les opérations de l'API 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 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 dans l'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 environnement Compte AWS, y compris les événements liés au changement de zone dans 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 sont enregistrées CloudTrail et documentées dans le Guide de référence de l'API de contrôle de routage pour Amazon 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 Gestion des identités et des accès AWS (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 de plus amples informations, veuillez consulter l'élément userIdentity CloudTrail .

Afficher les événements 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"
      }
    }
```

Identity and Access Management pour le changement de zone dans ARC

Gestion des identités et des accès AWS (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. 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 Application Recovery Controller (ARC), découvrez quelles fonctionnalités IAM peuvent être utilisées avec le décalage de zone.

Fonctionnalités IAM que vous pouvez utiliser avec le changement de zone

Fonctionnalité IAM	Support de changement de zone
Politiques basées sur l'identité	Oui
Politiques basées sur les ressources	Non
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition de politique	Oui
ACLs	Non
ABAC (identifications dans les politiques)	Partielle
Informations d'identification temporaires	Oui
Autorisations de principal	Oui
Rôles 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 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 Définition d'autorisations IAM personnalisées avec des politiques gérées par le client 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. 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 ARC, consultez. Exemples de politiques basées sur l'identité dans Amazon Application Recovery Controller (ARC)

Politiques basées sur les ressources au sein d'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. Par exemple, les politiques de confiance de rôle IAM et les politiques de compartiment Amazon S3 sont des politiques basées sur les ressources. 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. Intégration d'actions dans une politique afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour consulter la liste des actions ARC relatives au changement de zone, consultez la section Actions définies par Amazon Route 53 Zonal Shift dans le manuel Service Authorization Reference.

Les actions politiques dans ARC pour le 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 voir des exemples de politiques basées sur l'identité ARC pour le changement de zone, voir. Exemples de politiques basées sur l'identité pour le changement de zone dans l'ARC

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. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, 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 leurs actions ARNs, ainsi que les actions que vous pouvez spécifier à l'aide de 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 voir des exemples de politiques basées sur l'identité ARC pour le changement de zone, voir. Exemples de politiques basées sur l'identité pour le changement de zone dans l'ARC

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` indique à quel moment les instructions s'exécutent en fonction de critères définis. 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. 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 voir des exemples de politiques basées sur l'identité ARC pour le changement de zone, voir. Exemples de politiques basées sur l'identité pour le changement de zone dans l'ARC

Listes de contrôle d'accès (ACLs) dans ARC

Supports ACLs : Non

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLs 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 ARC

Prend en charge ABAC (identifications dans les politiques) : partiellement

Le contrôle d’accès par attributs (ABAC) est une stratégie d’autorisation qui définit les autorisations en fonction des attributs nommés balise. Vous pouvez associer des balises aux entités et aux AWS ressources IAM, puis concevoir des politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de la ressource.

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 ABAC, consultez Définition d’autorisations avec l’autorisation 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.

ARC inclut le support partiel suivant pour ABAC :

- Le changement de zone prend en charge l'ABAC pour les ressources gérées enregistrées dans 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 ARC

Prend en charge les informations d’identification temporaires : oui

Les informations d'identification temporaires fournissent un accès à court terme aux AWS ressources et sont automatiquement créées lorsque vous utilisez la fédération ou que vous changez de rôle. 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 et Services AWS compatibles avec IAM dans le Guide de l’utilisateur IAM.

Autorisations principales interservices pour 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 des 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 ARC

Prend en charge les rôles de service : Non

Un rôle de service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer un rôle de service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.

Rôles liés à un service pour 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.

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 Application Recovery Controller (ARC),

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 avec IAM et les autorisations en général, consultez les informations de la rubrique de présentation,Identity and Access Management pour le changement de zone dans ARC.

Zonal Shift prend en charge les équilibreurs de charge d'application, les équilibreurs de charge réseau, les groupes Amazon EC2 Auto Scaling et Amazon EKS. Vous pouvez utiliser les clés de condition IAM pour étendre une politique d'autorisation IAM à ces ressources. Voici un exemple de politique utilisant une clé de condition avec plusieurs ressources de différents types :

```
{
    "Condition": {
        "StringLike": {
            "arc-zonal-shift:ResourceIdentifier": [
                "arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/net/
*",
                "arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/app/
*",
                "arn:aws:eks:us-east-1:123456789012:cluster/*"
            ]
        }
    },
    "Action": [
        "arc-zonal-shift:StartZonalShift"
    ],
    "Resource": "*",
    "Effect": "Allow"
}
```

Pour de plus amples informations, veuillez consulter Ressources prises en charge.

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 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 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 l'ARC

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier des ressources ARC. 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.

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 IAM (console) dans le Guide de l’utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par ARC, y compris le ARNs format de chaque type de ressource, consultez la section Actions, ressources et clés de condition pour Amazon Application Recovery Controller (ARC) 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 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.

- Accordez 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 d'IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utilisez 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 CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez l'Analyseur d'accès IAM pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : l'Analyseur d'accès IAM 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 politiques avec 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 la MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Sécurisation de l'accès aux API avec 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 Application Recovery Controller (ARC), 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 votre Compte AWS. Si vous créez une politique 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 politique.

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 :

JSON

```
{
    "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 :

JSON

```
{
    "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": "*"
        }
    ]
}
```

Changement de zone automatique dans ARC

Avec l'autoshift zonal, vous autorisez AWS le transfert du trafic des ressources d'une application depuis une zone de disponibilité (AZ) 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 l'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 ARC pour les essais vous aident à vous assurer que le transfert du trafic d'une zone de disponibilité pendant un transfert 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 votre application 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.

Après avoir activé le changement automatique de zone, nous vous recommandons de vérifier, en lançant et en évaluant un changement de zone d'exécution à la demande, que votre application peut continuer à fonctionner normalement même si le trafic est transféré hors d'une zone de disponibilité. Ensuite, les séances d'entraînement régulières effectuées par ARC vous aident à confirmer, de façon continue, que vous disposez d'une capacité suffisante pour effectuer un changement automatique.

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. Par exemple, 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.

Vous pouvez activer l'autoshift zonal, pour une ressource prise en charge, dans la console ARC. Ou, dans la console Amazon EC2, vous avez la possibilité d'activer l'autoshift zonal pour une ressource d'équilibreur de charge spécifique. 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 EventBridge les notifications Amazon pour vous avertir des changements automatiques et des essais. Pour de plus amples informations, veuillez consulter 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 Application Recovery Controller (ARC) 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 déficience 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 séances d'entraînement, au cours desquelles l'ARC déplace régulièrement le trafic vers la ressource hors d'une zone de disponibilité. L'ARC planifie des séances d'entraînement environ une fois par semaine pour chaque ressource associée à une configuration d'exécution d'entraînement. Les séances d'entraînement pour chaque ressource sont planifiées indépendamment.

Pour chaque séance d'entraînement, l'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 de plus amples informations, veuillez consulter Utilisation de l'autoshift zonal avec Amazon EventBridge.

Table des matières

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 devez activer manuellement le changement automatique de zone pour les ressources prises en charge AWS .

Lorsque vous déployez et exécutez AWS des applications sur des équilibreurs de charge dans plusieurs (généralement trois) AZs 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 AZ en transférant le trafic grâce à un transfert automatique. En transférant le trafic des ressources vers d'autres AZs sites 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 AZ ou d'autres déficiences.

Les ressources prises en charge par l'ARC fournissent des intégrations qui marquent l'AZ spécifié comme étant en mauvais état, ce qui entraîne le déplacement du trafic vers l'AZ altéré.

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 AZs ne possèdent aucune instance, ou si toutes les instances ne fonctionnent pas correctement, l'équilibreur de charge est dans un état d'ouverture défaillante et vous ne pouvez pas déplacer l'un des. AZs

Pour en savoir plus sur l'autoshift zonal, voir. Changement de zone automatique dans ARC

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.

Quand l'ARC planifie, commence et termine les entraînements

L'ARC planifie une séance d'entraînement pour une ressource chaque semaine, pendant environ 30 minutes. L'ARC planifie, démarre et gère les essais pour chaque ressource de manière indépendante. L'ARC ne regroupe pas les essais d'entraînement pour les ressources d'un même compte. Vous pouvez également démarrer vous-même des séances d'entraînement à la demande, afin de vérifier que votre configuration est sûre pour un événement de changement automatique zonal.

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`,`INTERRUPTED`, `CAPACITY_CHECK_FAILED` et`PENDING`. Les valeurs et les descriptions des résultats sont incluses dans la section Résultats des essais.

Dans certains cas, l'ARC interrompt une séance d'entraînement et y met fin. Par exemple, si un changement automatique démarre pendant un exercice d'entraînement, ARC interrompt le cycle d'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, ARC interrompt également l'entraînement et y met fin.

En outre, il existe plusieurs scénarios dans lesquels ARC ne lance pas d'entraînement de planification pour une ressource.

En réponse à des exercices d'entraînement interrompus ou bloqués pour une ressource, ARC effectue les opérations suivantes :

- Si un entraînement pour une ressource est interrompu alors qu'il est en cours, l'ARC considère que le cycle d'entraînement hebdomadaire est terminé et planifie un nouvel 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 exercice d'entraînement pour une ressource, ARC ne démarre pas le cycle d'entraînement. L'ARC poursuit une surveillance régulière, afin de déterminer s'il existe toujours une ou plusieurs contraintes de blocage. Lorsqu'il n'y a aucune contrainte de blocage, ARC lance l'entraînement pour la ressource.

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

- L'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 l'ARC a planifié le début d'un exercice d'entraînement, ARC ne démarre pas le cycle d'entraînement. L'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'un entraînement est actif, l'ARC met fin à l'entraînement et n'essaie pas d'en démarrer un autre avant le prochain entraînement régulier prévu pour la ressource.
- S'il y a un AWS événement en cours dans une région, l'ARC ne lance pas de courses d'entraînement pour les ressources et met fin aux séries d'entraînement actives dans la région.

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

Contrôles de capacité pour les essais

Lorsqu'une séance d'entraînement commence, pour déplacer temporairement le trafic hors d'une zone de disponibilité, ARC vérifie que vous disposez d'une capacité suffisante dans les autres zones de disponibilité pour déplacer le trafic en toute sécurité hors de l'AZ. Si la capacité disponible est insuffisante, le transfert de trafic pour le cycle d'entraînement n'est pas lancé et le cycle d'entraînement prend fin.

En outre, l'ARC effectue un contrôle de capacité pour les ressources de l'équilibreur de charge lorsqu'un changement automatique de zone est terminé, avant que l'ARC ne mette fin au changement de trafic entamé par le changement automatique. Si le contrôle de capacité échoue à la fin du transfert automatique, le trafic n'est pas redirigé vers la zone de disponibilité dont il a été éloigné.

Les contrôles de capacité équilibrée ne sont effectués que pour les équilibreurs de charge et les groupes Auto Scaling.

Pour une ressource d'équilibreur de charge, les contrôles de capacité permettent de vérifier que les hôtes sains associés à l'équilibreur de charge sont répartis entre les zones de disponibilité. Plus précisément, les contrôles de capacité garantissent que le nombre d'hôtes sains dans toutes les

zones de disponibilité où la ressource est enregistrée est équilibré. Pour les contrôles de capacité, équilibré signifie que la capacité saine de chaque zone de disponibilité est égale à celle des autres zones, avec un léger écart.

Notez que les contrôles de capacité ne sont pas appliqués aux équilibreurs de charge avec des groupes cibles de type Lambda ni aux équilibreurs de charge d'application, car ces cibles ne sont pas configurées par zone.

Les contrôles de capacité sont également effectués pour les groupes Auto Scaling. Pour un groupe Auto Scaling, les contrôles de capacité valident que la capacité zonale saine totale d'un groupe Auto Scaling, c'est-à-dire le nombre total d'hôtes sains dans toutes les zones de disponibilité, correspond à la capacité définie pour ce groupe Auto Scaling.

En cas d'échec d'une vérification de capacité

Lorsqu'un contrôle de capacité révèle que la capacité disponible n'est pas équilibrée pour une ressource, le résultat de l'essai est le suivant`CAPACITY_CHECK_FAILED`. Pour en savoir plus sur les raisons pour lesquelles un contrôle de capacité a échoué, consultez le champ de commentaire du`ZonalShiftSummary`. Pour trouver le champ de commentaire correspondant à votre exercice de course par zone, procédez comme suit :

1. À l'aide de AWS CLI, listez les décalages de zone pour la ressource que vous avez spécifiée lors de l'entraînement effectué à l'aide de l'opération ListZonalShiftsAPI.

   FOr Par exemple, pour renvoyer les décalages de zone, vous pouvez exécuter une commande similaire à la suivante :

   ```
   aws arc-zonal-shift start-practice-run
       --resource-
   identifier="arn:aws:elasticloadbalancing:Region:111122223333:ExampleALB123456890"
   ```

2. Passez en revue le tableau d'`ZonalShiftSummary`objets renvoyé pour trouver le décalage de zone correspondant à l'essai qui a échoué en raison de contrôles de capacité.
3. Pour connaître le décalage de zone applicable, consultez les informations du `Comment` champ.

Notification pour les essais et les changements automatiques

Vous pouvez choisir d'être informé des essais et des changements automatiques pour votre ressource en configurant EventBridge les notifications Amazon. Vous pouvez configurer EventBridge

des notifications même si vous n'avez activé le décalage automatique zonal pour aucune ressource, ce que l'on appelle la notification automatique par les observateurs. Avec la notification Autoshift Observer, vous êtes informé de tous les changements automatiques lancés par ARC lorsqu'une zone de disponibilité est potentiellement altérée. Notez que vous devez configurer cette option dans chaque cas pour Région AWS lequel vous souhaitez recevoir des notifications.

Pour connaître les étapes à suivre pour activer la notification automatique des observateurs, reportez-vous Activation ou désactivation de la notification automatique des observateurs à. Pour en savoir plus sur les options de notification et sur la façon de les configurer EventBridge, consultezUtilisation de l'autoshift zonal avec Amazon EventBridge.

Priorité pour les décalages de zone

Il ne peut y avoir qu'un seul décalage de zone appliqué à un moment donné. En d'autres termes, un seul cabinet exécute un changement de zone, un changement de zone initié par le client, un décalage automatique ou AWS FIS un test pour la ressource. Lorsqu'un deuxième décalage de zone est lancé, l'ARC suit une priorité pour déterminer le type de décalage de zone en vigueur pour une ressource.

Le principe général de priorité est que les changements de zone que vous commencez en tant que client ont priorité sur les autres types de quarts de travail. Sachez toutefois qu'un exercice d'entraînement AWS initié en cours d'exécution vous empêche de démarrer un entraînement à la demande.

Pour illustrer la priorité dans ARC, voici comment fonctionne la priorité dans des exemples de scénarios :

Type de décalage zonal appliqué	Type de changement de zone initié	Résultat
AWS FIS expérience	Course d'entraînement	Le cycle d'entraînement ne pourra pas démarrer, car l' AWS FIS expérience a la priorité.
AWS FIS expérience	Déplacement de zone manuel	L' AWS FIS expérience sera annulée et le décalage de zone manuel sera appliqué.

Type de décalage zonal appliqué	Type de changement de zone initié	Résultat
AWS FIS expérience	Changement de zone automatique	L' AWS FIS expérience sera annulée et l'autoshift zonal sera appliqué.
AWS FIS expérience	AWS FIS expérience	L' AWS FIS expérienc e initiée ne pourra pas démarrer car une expérienc e en cours d'exécution a déclenché l'action de AWS FIS changement automatique.
Course d'entraînement	Déplacement de zone manuel	La séance d'entraînement sera annulée, le résultat fixé à`INTERRUPTED` , et le décalage de zone sera appliqué.
Course d'entraînement	AWS FIS expérience	La séance d'entraînement sera annulée, le résultat fixé à`INTERRUPTED` , et l' AWS FIS expérience sera appliquée .
Course d'entraînement	Changement de zone automatique	La séance d'entraînement sera annulée et le résultat défini sur`INTERRUPTED` , et le changement automatique de zone sera appliqué.
Déplacement de zone manuel	Course d'entraînement	La course d'entraînement ne démarrera pas.
Déplacement de zone manuel	AWS FIS expérience	L' AWS FIS expérience ne démarrera pas ou échouera si elle est déjà en cours.

Type de décalage zonal appliqué	Type de changement de zone initié	Résultat
Déplacement de zone manuel	Changement de zone automatique	L'autoshift zonal se fera `ACTIVE` mais pas `APPLIED` sur la ressource. Le décalage de zone manuel est prioritaire.
Changement de zone automatique	AWS FIS expérience	L' AWS FIS expérience ne démarrera pas ou échouera si elle est en cours.
Changement de zone automatique	Déplacement de zone manuel	L'autoshift zonal se fera `ACTIVE` mais pas `APPLIED` sur la ressource. Le décalage de zone manuel est prioritaire.
Changement de zone automatique	Course d'entraînement	La séance d'entraînement ne démarrera pas, car l'autoshift zonal a la priorité.

Le changement de trafic actuellement en cours pour la ressource a un statut de changement de zone appliqué défini sur `APPLIED`. Un seul quart de travail est défini sur `APPLIED` à la fois. Les autres changements en cours sont définis comme tels`NOT_APPLIED`, mais restent `ACTIVE` inchangés.

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

Pour arrêter un changement automatique en cours pour une ressource, vous devez annuler le changement de zone.

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 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 plus d'informations, consultez Annulation d'un changement automatique zonal et Activation et utilisation de l'autoshift zonal.

Comment le trafic est redirigé

Dans le cas des changements de zone automatiques et des 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 l'ARC pour les changements de zone initiés par le client. En cas de mauvais état de santé, Amazon Route 53 retire 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 .

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

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. L'ARC utilise des bilans de santé pour éloigner le trafic des zones de disponibilité, en demandant que les bilans de santé soient définis sur un état défectueux, puis rétablit les bilans de santé à la normale lorsqu'il met fin à un changement automatique ou à un changement de zone.

Alarmes pour les séances d'entraînement

Vous pouvez spécifier deux types d' CloudWatch alarmes pour les essais en mode automatique zonal : les alarmes de résultat et les alarmes de blocage.

Alarmes de résultat (obligatoire)

> Pour le premier type d'alarme, l'alarme de résultat, au moins une alarme doit être spécifiée. Vous devez configurer les alarmes 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 essai soit efficace, spécifiez comme alarmes de résultat au moins une CloudWatch alarme répondant aux deux critères suivants :

L'alarme surveille les métriques de la ressource ou de votre application

AND

L'alarme émet un `ALARM` état lorsque votre application est affectée 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.

Les alarmes de résultat fournissent également des informations sur le résultat de l'exercice d'entraînement que l'ARC rapporte pour chaque entraînement. Si une alarme de résultat passe à un `ALARM` état, ARC met fin à l'essai et renvoie le résultat d'un essai de`FAILED`. Si l'essai pratique termine la période de test de 30 minutes et qu'aucune des alarmes de résultat que vous avez spécifiées n'entre dans un `ALARM` état, le résultat renvoyé est`SUCCEEDED`. Une liste de toutes les valeurs de résultats, avec des descriptions, est fournie dans la section Résultats des essais.

Alarmes de blocage (facultatif)

Vous pouvez éventuellement définir un deuxième type d'alarme, l'alarme de blocage. La pratique du blocage des alarmes commence à démarrer ou à se poursuivre lorsqu'une ou plusieurs alarmes sont en `ALARM` état. Les alarmes de blocage bloquent la pratique d'exécuter les changements de trafic dès le démarrage et d'arrêter toute exécution d'entraînement en cours lorsqu'au moins une des alarmes est active. `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. Pour ce faire, vous pouvez ajouter une alarme de blocage dans ARC.

Fenêtres bloquées et fenêtres autorisées (en UTC)

Vous avez la possibilité de bloquer ou d'autoriser les séances d'entraînement pour des dates calendaires spécifiques, ou pour des créneaux horaires spécifiques, c'est-à-dire des jours et des heures, spécifiés 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 entraînent une diminution du 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`.

Vous pouvez également décider que les mercredis et vendredis de midi à 17 h sont les meilleurs moments pour que l'ARC commence ses essais, afin de tester votre configuration. Pour ce scénario, vous pouvez définir les jours et heures récurrents suivants comme fenêtres autorisées, par exemple, en UTC :`WED-12:00-17:00 FRI-12:00-17:00`.

Région AWS disponibilité de l'autoshift zonal

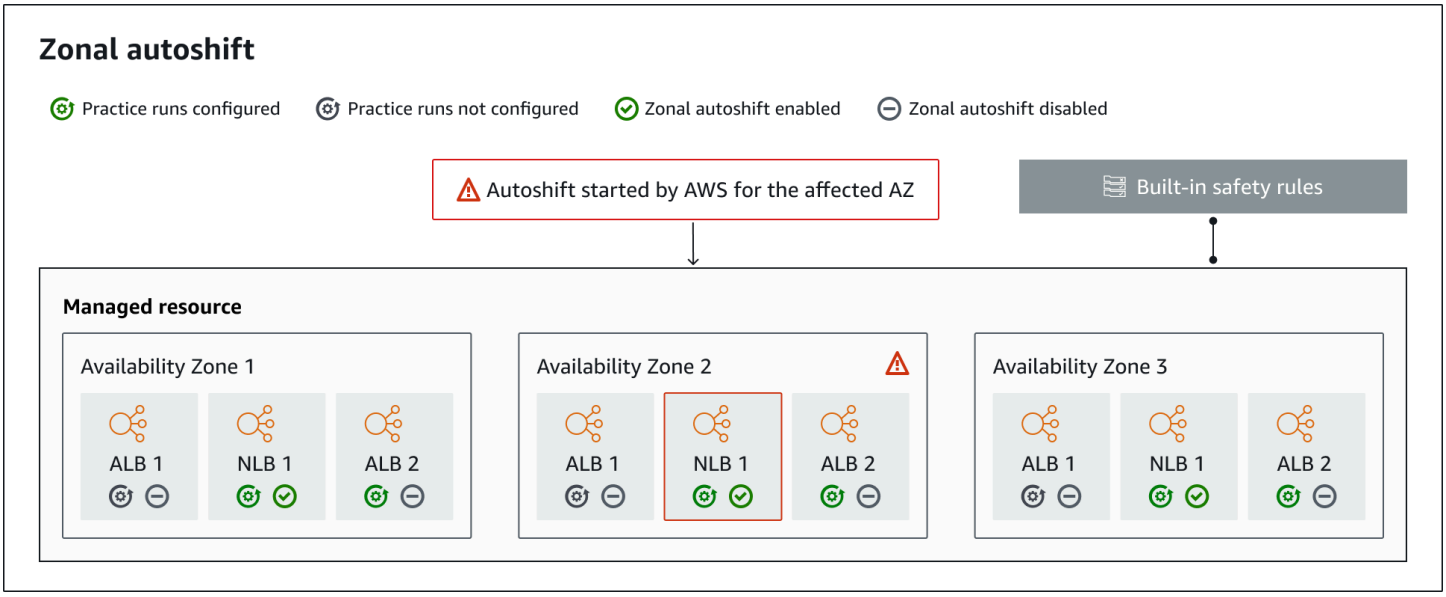
Le changement de zone et le changement automatique de zone sont actuellement disponibles dans les régions commerciales Régions AWS, ainsi que dans les régions de Chine, à savoir la région de Chine (Pékin) et la région de Chine (Ningxia).

Les ressources qui utilisent Amazon Application Recovery Controller (ARC) peuvent inclure des considérations supplémentaires. Pour de plus amples informations, veuillez consulter Ressources prises en charge.

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

Composants du changement de zone automatique

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 d'ARC.

Changements automatiques zonaux

L'autoshift zonal déplace le trafic vers une ressource, sans que vous ayez à effectuer aucune action. L'autoshift zonal est une fonctionnalité d'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. Vous pouvez également planifier des séances d'entraînement à la demande.

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 les configurations

Avec une configuration d'exécution d'entraînement, vous pouvez définir les délais (fenêtres bloquées ou autorisées) pendant lesquels ARC peut démarrer une exécution d'entraînement pour une ressource avec un décalage automatique zonal. Vous définissez également les CloudWatch

alarmes pour un AWS exercice d'entraînement. Vous pouvez modifier la configuration d'un exercice d'entraînement à tout moment, pour ajouter ou modifier des fenêtres bloquées ou autorisées, ou pour mettre à jour les alarmes relatives à l'entraînement.

Pour activer l'autoshift zonal, vous devez disposer d'une configuration d'exécution par entraînement pour une ressource.

Vous pouvez supprimer une séance d'entraînement, mais vous devez d'abord désactiver le changement automatique de zone.

Entraînez-vous à exécuter des al

Lorsque vous configurez des exercices pratiques, vous spécifiez les CloudWatch alarmes (que vous créez d'abord dans CloudWatch), en fonction de vos 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, ARC met fin au décalage de zone pour l'essai, de sorte que le trafic de la ressource n'est plus déplacé hors de la zone de disponibilité.

Vous pouvez spécifier deux types d'alarmes pour les exercices pratiques : les alarmes de résultat, destinées à surveiller l'état de votre ressource et de votre application pendant l'entraînement, et les alarmes de blocage, que vous pouvez configurer pour empêcher le démarrage des essais ou pour arrêter un entraînement en cours. Au moins une alarme de résultat est requise ; les alarmes de blocage sont facultatives.

Résultats de la course d'entraînement

L'ARC rapporte un résultat pour chaque entraînement. Les résultats possibles des tests pratiques sont les suivants :

- EN ATTENTE : Le changement de zone pour la course d'entraînement est actif (en cours). Il n’y a pas encore de résultat à transmettre.
- 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. Un test pratique peut être interrompu 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 résultat `INTERRUPTED`, consultez Résultats des tests pratiques.

- ÉCHEC : l'alarme de résultat s'est vu affecter l'état `ALARM` pendant le test pratique.
- ÉCHEC DE LA VÉRIFICATION DE CAPACITÉ : la vérification de l'équilibre de capacité entre les zones de disponibilité pour vos ressources de répartition de charge et de groupe Auto Scaling a échoué.

Règles de sécurité intégrées

Les règles de sécurité intégrées à l'ARC empêchent plusieurs transferts de trafic pour une ressource d'être en vigueur à la fois. En d'autres termes, un seul changement de zone initié par le client, un changement de zone par entraînement (initié par AWS ou par un client) ou un changement automatique pour la ressource peuvent déplacer activement le 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 Priorité pour les décalages de zone.

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 ARC.

Ressource gérée

Les équilibreurs de charge d'application enregistrent automatiquement les ressources auprès d'ARC pour le décalage automatique zonal. Vous devez activer manuellement d'autres ressources pour le changement automatique zonal.

Nom de la ressource

Le nom d'une ressource gérée dans 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.

Type de quart de travail

Définit le type de décalage zonal. Les décalages zonaux peuvent être de l'un des types suivants :

- ZONAL_SHIFT
- ZONAL_AUTOSHIFT
- PRACTICE_RUN
- FIS_EXPERIMENT

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 ARC

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.

Pour obtenir des informations détaillées sur la tarification de l'ARC et des exemples de tarification, consultez la section Tarification de l'ARC.

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 Application Recovery Controller (ARC).

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.
- Lors des essais, l'ARC lance un changement de zone en votre nom ou vous lancez un entraînement par changement de zone. L' AWS entraînement par changement de zone permet de déplacer 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 Application Recovery Controller (ARC) 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 ARC pour déplacer le trafic de votre application est une mise à jour du 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 changement 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 d'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. Exécutez vos propres tests pratiques à la demande pour vous assurer que votre configuration est correctement dimensionnée. 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 ARC.

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. 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 (insalubres).

Pour en savoir plus sur les ressources prises en charge, y compris toutes les exigences et exceptions à connaître, consultezRessources prises en charge.

Spécifiez les alarmes pour les essais

Vous devez configurer au moins un type d'alarme (une alarme de résultat) pour les essais avec changement automatique zonal. En option, vous pouvez également configurer un deuxième type d'alarme (alarme de blocage).

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

- Vous devez configurer au moins une alarme de résultat pour une configuration d'entraînement. Pour les alarmes de résultat, nous vous recommandons de configurer les CloudWatch alarmes de manière à ce qu'elles passent 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 les alarmes appropriées qui AWS mettent fin à l'entraînement et renvoient 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 (KPIs) sous forme d' CloudWatchalarmes. 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, ARC lance des essais la prochaine fois qu'un entraînement est planifié pour la ressource.
- Pour les alarmes de blocage des entraînements, si vous choisissez d'en configurer une (ou plusieurs), vous pouvez choisir de suivre des indicateurs spécifiques que vous utilisez pour indiquer que vous ne souhaitez pas qu'un AWS entraînement commence, par exemple lorsqu'une alarme indique qu'un incident est en cours.
- Pour vous entraîner à exécuter des alarmes, vous devez spécifier le nom de ressource Amazon (ARN) pour chaque alarme. Vous devez donc d'abord configurer l'alarme 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. Vous pouvez également configurer des alarmes distinctes, puis spécifier plusieurs alarmes de chaque type pour la configuration de votre entraînement. 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

L'ARC rapporte un résultat pour chaque 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 des tests pratiques sont les suivants :

- SUCCÈS : Aucune alarme de résultat n'est entrée dans un `ALARM` état pendant l'essai, et le cycle d'entraînement a terminé la période de test complète de 30 minutes.
- ÉCHEC : Au moins une 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'essai a été interrompu car il n'était plus possible d'accéder à une CloudWatch alarme spécifiée pour la configuration du cycle d'entraînement.
  - La séance d'entraînement a pris fin car une alarme de blocage spécifiée pour l'essai est entrée dans un `ALARM` état.
  - La course d'entraînement a été interrompue pour une raison inconnue.
  - La séance d'entraînement a pris fin car un changement automatique de zone avec priorité a été initié. Voir Priorité pour les changements de zone.
- ÉCHEC DE LA VÉRIFICATION DE CAPACITÉ : la vérification de l’équilibre de capacité entre les zones de disponibilité pour vos ressources de répartition de charge et de groupe Auto Scaling a échoué.
- EN ATTENTE : La séance d'entraînement est active (en cours). Il n’y a pas encore de résultat à transmettre.

Opérations de l'API Zonal Autoshift

Le tableau suivant répertorie les opérations de l'API ARC 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 ARC	Utilisation de l'API ARC
Création d'une configuration d'exécution d'entraînement	Consultez Activation ou désactivation du changement de zone automatique	Consultez CreatePracticeRunConfiguration
Supprimer une configuration d'exécution d'entraînement	Consultez Configuration, modification ou suppression d'une configuration d'entraînement	Consultez DeletePracticeRunConfiguration
Répertorier les changements automatiques	Consultez Changement de zone automatique dans ARC	Consultez ListAutoshifts
Répertorier les ressources pour l'autoshift zonal	Consultez Ressources prises en charge	Consultez ListManagedResources
Obtenez des ressources pour le changement automatique par zone	Consultez Ressources prises en charge	Consultez GetManagedResource
Modifier la configuration d'une exécution d'entraînement	Consultez Configuration, modification ou suppression d'une configuration d'entraînement	Consultez UpdatePracticeRunConfiguration
Activer ou désactiver l'autoshift zonal	Consultez Activation ou désactivation du changement de zone automatique	Consultez UpdateZonalAutoshiftConfiguration
Activer ou désactiver la notification AutoShift Observer	Consultez Activation et utilisation de l'autoshift zonal	Consultez UpdateAutoshiftObserverNotificationStatus
Commencez une course d'entraînement	Consultez Commencer une course d'entraînement : changement de zone	Consultez StartPracticeRun

Action	Utilisation de la console ARC	Utilisation de l'API ARC
Annuler une séance d'entraînement	Consultez Annulation d'un entraînement : changement de zone	Consultez CancelPracticeRun

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 d'Amazon Application Recovery Controller (ARC) 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 d'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. Pour plus d'informations sur les ressources que vous pouvez utiliser avec le changement automatique zonal, consultez. Ressources prises en charge

L'autoshift zonal inclut des essais pratiques, qui déplacent également le trafic hors des zones de disponibilité, afin de vérifier que les changements automatiques sont sûrs pour votre application.

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 Pour plus d'informations sur l'utilisation du AWS CLI, consultez la référence des AWS CLI commandes.

Table des matières

Création d'une configuration d'exécution d'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 ou de fenêtres bloquées ou autorisées est facultative.

Vous créez une configuration d'exécution pratique à l'aide de 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"
}
```

Démarrez une séance d'entraînement à la demande

Vous pouvez démarrer un changement de zone d'entraînement à la demande à l'aide de la CLI à l'aide de la `start-practice-run` commande.

Par exemple, pour démarrer un exercice d'entraînement pour une ressource, utilisez une commande comme celle-ci :

```
aws arc-zonal-shift start-practice-run
    --resource-
identifier="arn:aws:elasticloadbalancing:Region:111122223333:ExampleALB123456890" \
    "awayFrom": "usw2-az1",
```

```
{
    "awayFrom": "usw2-az1",
    "comment": "Practice run started. Shifting traffic away from Availability Zone
 usw2-az1.",
}
```

Annuler une séance d'entraînement en cours

Vous pouvez annuler une séance d'entraînement en cours avec la CLI à l'aide de la `cancel-practice-run` commande.

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

```
aws arc-zonal-shift cancel-practice-run \
   --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 canceled"
}
```

Annuler un changement automatique en cours

Vous pouvez annuler un changement automatique en cours à l'aide de la CLI en annulant le décalage automatique zonal pour la ressource. Pour annuler un changement automatique zonal, utilisez le. `cancel-zonal-shift command`

```
aws arc-zonal-shift cancel-zonal-shift --zonal-shift-id
 9ac9ec1e-1df1-0755-3dc5-8cf573cd9c38
```

```
{
    "awayFrom": "usw2-az1",
    "comment": "Zonal autoshift started. Shifting traffic away from Availability Zone
 usw2-az1.",
    "expiryTime": "2024-12-17T22:29:38-08:00",
    "resourceIdentifier": "arn:aws:elasticloadbalancing:us-
east-1:111122223333:loadbalancer/app/Testing/5a19403ecd42dc05",
    "startTime": "2024-12-17T21:27:26-08:00",
    "status": "CANCELED",
    "zonalShiftId": "9ac9ec1e-1df1-0755-3dc5-8cf573cd9c38"
}
```

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 ARC ne démarre pas les exercices d'entraînement. 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 Application Recovery Controller (ARC). Après avoir activé l'autoshift zonal, vous pouvez apporter des modifications aux configurations des essais, démarrer un entraînement à la demande, annuler un quart de travail en cours, y compris les essais, ou activer les notifications de décalage automatique pour les observateurs.

Activation ou désactivation du changement de zone automatique

Les étapes décrites ici expliquent comment activer ou désactiver l'autoshift zonal sur la console Amazon Application Recovery Controller (ARC). 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 ARC à l'adressehttps://console.aws.amazon.com/route53recovery/zonalshift/home#/autoshift.
2. Sous Configurations de transfert automatique par zone de ressources, sélectionnez une ressource.
3. Dans le menu Actions, choisissez Activer le changement automatique par zone, 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.

Table des matières

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 Application Recovery Controller (ARC). 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 ARC à l'adressehttps://console.aws.amazon.com/route53recovery/zonalshift/home#/autoshift.
2. Choisissez Configurer l'autoshift zonal.
3. Choisissez une ressource à configurer pour l'autoshift zonal.
4. 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.
5. Choisissez des options pour les séances d'entraînement pour la ressource. Pour les alarmes, vous pouvez effectuer les opérations suivantes :

   - (Obligatoire) Spécifiez au moins une alarme de résultat pour surveiller les essais pour cette ressource.
   - (Facultatif) Spécifiez une ou plusieurs alarmes 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.
6. Spécifiez éventuellement des fenêtres bloquées ou autorisées, pour empêcher ARC de démarrer des essais ou permettre à ARC de démarrer des essais pour cette ressource. Toutes les dates et heures sont exprimées en UTC.
7. Cochez la case pour confirmer que vous avez lu l'accusé de réception.

8. Choisissez Créer.

Pour modifier la configuration d'une exécution d'entraînement

1. Ouvrez la console ARC à l'adressehttps://console.aws.amazon.com/route53recovery/zonalshift/home#/autoshift.
2. Sous Configurations de transfert automatique par zone de ressources, sélectionnez une ressource.
3. Dans le menu Actions, choisissez Modifier la configuration des essais pratiques.
4. 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 bloquer les alarmes, vous pouvez ajouter une ou plusieurs alarmes ou supprimer des alarmes.
     - Pour les alarmes de résultat, vous pouvez ajouter une ou plusieurs alarmes ou supprimer des alarmes. Au moins une alarme de résultat est requise, vous ne pouvez donc pas supprimer toutes les alarmes de résultat d'une configuration.
   - Pour les fenêtres bloquées et les fenêtres autorisées, 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.
5. Choisissez Enregistrer.

Pour supprimer une configuration d'entraînement

1. Ouvrez la console ARC à l'adressehttps://console.aws.amazon.com/route53recovery/zonalshift/home#/autoshift.
2. Sous Configurations de transfert automatique par zone de ressources, sélectionnez une ressource.
3. Dans le menu Actions, choisissez Supprimer la configuration d'exécution d'exercices pratiques.
4. 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 changement automatique zonal

Pour arrêter un changement automatique de zone en cours pour une ressource, vous devez annuler le changement automatique de zone.

Pour arrêter un changement automatique zonal en cours

1. Ouvrez la console ARC à l'adressehttps://console.aws.amazon.com/route53recovery/zonalshift/home#/.
2. Sélectionnez le décalage automatique de zone que vous souhaitez annuler, puis choisissez Annuler le décalage de zone.
3. Dans la boîte de dialogue modale de confirmation, choisissez Confirmer.

Commencer une course d'entraînement : changement de zone

Les étapes décrites dans cette section expliquent comment démarrer un changement de zone d'entraînement à la demande sur la console ARC. 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 démarrer un exercice d'entraînement par changement de zone après avoir configuré le changement automatique de zone et créé une configuration d'exécution d'entraînement.

Pour commencer un entraînement, exécutez le changement de zone

1. Ouvrez la console ARC à l'adressehttps://console.aws.amazon.com/route53recovery/zonalshift/home#/.
2. Sous Ressources de décalage automatique zonal, accédez à une ressource individuelle pour laquelle le décalage automatique zonal est configuré.
3. Sur la page d'aperçu des ressources, choisissez Start practice run.
4. Sélectionnez une zone de disponibilité, puis entrez un commentaire pour votre séance d'entraînement. L'essai va déplacer le trafic hors de la zone de disponibilité que vous avez sélectionnée.
5. Sélectionnez Démarrer.

Annulation d'un entraînement : changement de zone

Les étapes décrites dans cette section expliquent comment annuler un changement de zone sur la console ARC. 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 ou vous entraîner à des courses que vous avez vous-même initiées. 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 ARC à l'adressehttps://console.aws.amazon.com/route53recovery/zonalshift/home#/.
2. Sélectionnez le décalage de zone d'entraînement que vous souhaitez annuler, puis choisissez Annuler le décalage de zone ou Annuler l'entraînement.
3. Dans la boîte de dialogue modale de confirmation, choisissez Confirmer.

Activation ou désactivation de la notification automatique des observateurs

Vous pouvez configurer l'autoshift zonal pour vous avertir, via Amazon EventBridge, chaque fois qu'un changement automatique AWS démarre afin de déplacer le trafic hors d'une zone de disponibilité potentiellement altérée. Vous devez configurer cette option dans chaque cas pour Région AWS lequel vous souhaitez recevoir des notifications. Il n'est pas nécessaire de configurer des ressources spécifiques avec le changement automatique par zone pour activer ces notifications distinctes. Pour de plus amples informations, veuillez consulter Utilisation de l'autoshift zonal avec Amazon EventBridge.

Les étapes décrites dans cette section expliquent comment activer la notification Autoshift des observateurs à l'aide de la console Amazon Application Recovery Controller (ARC). Pour utiliser l'autoshift zonal par programmation, consultez le guide de référence de l'API Zonal Shift et Zonal Autoshift.

Pour activer ou désactiver la notification automatique des observateurs

1. Ouvrez la console ARC à l'adressehttps://console.aws.amazon.com/route53recovery/zonalshift/home#/.

2. Sous Mise en route, choisissez Activer la notification automatique des observateurs.
3. Dans la boîte de dialogue de confirmation, choisissez Activer la notification aux observateurs.

Test de l'autoshift zonal avec AWS FIS

Vous pouvez l'utiliser AWS Fault Injection Service pour configurer et exécuter des expériences qui vous aident à simuler des conditions réelles, telles que le scénario AZ Availability : Power Interruption, qui démontrera ce qui se passe lorsque AWS démarre un changement automatique zonal sur vos ressources activées par le changement automatique lors d'une altération potentiellement étendue de l'AZ.

L'action Start `aws:arc:start-zonal-autoshift` Recovery vous permet de démontrer comment déplacer AWS automatiquement le trafic, pour les ressources activées par le transfert automatique zonal, hors d'une zone de zone potentiellement altérée et de le rediriger vers une zone saine AZs dans cette zone Région AWS pendant l'exécution du scénario de disponibilité de la zone de disponibilité.

Par exemple, vous pouvez utiliser la bibliothèque de AWS FIS scénarios pour simuler une altération de l'AZ provoquée par une coupure de courant. Dans cette expérience, cinq minutes après le début de la coupure de courant de l'AZ, l'action de restauration déplace `aws:arc:start-zonal-autoshift` automatiquement le trafic des ressources vers l'AZ spécifié. Le trafic est décalé pendant les 25 minutes restantes de la coupure de courant, afin de montrer comment le changement automatique serait déclenché en cas de défaillance potentiellement généralisée de l'AZ. Lorsque l'expérience est terminée, le changement de trafic prend fin et le trafic AZs recommence à circuler vers tous. Ce processus démontre un rétablissement complet après un incident d'alimentation ayant un impact sur un AZ.

En quoi les expériences diffèrent-elles des essais pratiques de changement automatique zonaux

AWS FIS les expériences diffèrent des essais pratiques de changement automatique zonal en ce sens que, pendant les essais, l'ARC déplace le trafic vers vos ressources d'une zone de zone dans le cadre d'un processus normal afin de garantir que votre application peut tolérer la perte d'une zone de zone de zone. Cependant, au cours d'une AWS FIS expérience, AWS FIS montre comment une altération de l'AZ et un changement automatique seraient déclenchés pour vos ressources activées par le changement automatique en votre nom, puis annule le changement automatique une fois le décalage automatique résolu.

Vous ne pouvez pas mettre à jour un changement de AWS zone initié par FIS lorsqu'il est en cours d'exécution. De plus, si vous annulez un décalage de zone en dehors de AWS FIS, l' AWS FIS expérience prend fin.

AWS FIS mécanisme de sécurité basé sur l'expiration

AWS FIS gère le décalage de zone à l'aide des opérations StartZonalShiftUpdateZonalShift,, et CancelZonalShiftAPI, le `expiresIn` champ pour ces demandes étant défini sur 1 minute comme mécanisme de sécurité. Cela permet d' AWS FIS annuler rapidement le décalage de zone en cas d'événements inattendus, tels que des pannes de réseau ou des problèmes système. Dans la console ARC, le champ du délai d'expiration affiche AWS FIS-managed, et l'expiration prévue réelle est déterminée par la durée spécifiée dans l'action de changement de zone. Pour plus d'informations sur les essais, reportez-vous à la section Fonctionnement du changement automatique de zone et des essais d'entraînement

Il ne peut y avoir qu'un seul décalage de zone appliqué à un moment donné. En d'autres termes, un seul cabinet exécute un changement de zone, un changement de zone initié par le client, un décalage automatique ou AWS FIS un test pour la ressource. Lorsqu'un deuxième décalage de zone est lancé, l'ARC suit une priorité pour déterminer le type de décalage de zone en vigueur pour une ressource. Pour plus d'informations sur la priorité des décalages de zone, voir. Priorité pour les décalages de zone

Pour plus d'informations sur les actions de AWS FIS restauration, reportez-vous à l'action AWS FIS de restauration dans le Guide de AWS Fault Injection Service l'utilisateur.

Journalisation et surveillance pour le changement automatique de zone dans Amazon Application Recovery Controller (ARC)

Vous pouvez utiliser AWS CloudTrail Amazon EventBridge pour surveiller l'autoshift zonal dans Amazon Application Recovery Controller (ARC), 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

Zonal Autoshift for ARC est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans 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 ARC et des appels de code vers les opérations de l'API 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 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 dans 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 environnement Compte AWS, y compris les événements liés au changement automatique de zone dans 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 sont enregistrées CloudTrail et documentées dans le Guide de référence de l'API de contrôle de routage pour Amazon 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 Gestion des identités et des accès AWS (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 de plus amples informations, veuillez consulter l'élément userIdentity CloudTrail .

Afficher les événements 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 l'autoshift zonal spécifie les informations d'état relatives aux essais ou aux changements automatiques, par exemple, lorsqu'un entraînement est lancé. Vous pouvez configurer l'autoshift zonal pour vous informer des événements de décalage automatique zonal pour les ressources que vous activez pour le service.

Vous pouvez également choisir, en plus ou à la place des autres notifications, d'activer la notification Autoshift Observer, qui fournit un événement de notification chaque fois qu'un changement automatique AWS démarre pour une zone de disponibilité potentiellement altérée. Les notifications d'observation Autoshift sont distinctes des notifications que vous recevez lorsque le trafic des ressources que vous avez activées pour le transfert automatique zonal est transféré hors d'une zone de disponibilité. Il n'est pas nécessaire de configurer les ressources avec le changement automatique par zone pour activer la notification automatique des observateurs. Pour de plus amples informations, veuillez consulter Activation et utilisation de l'autoshift zonal.

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 transmis d'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 l'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`
- `FIS Experiment Autoshift In Progress`
- `FIS Experiment Autoshift Completed`
- `FIS Experiment Autoshift Canceled`
- `Manual Shift Started`
- `Manual Shift Updated`
- `Manual Shift Canceled`

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

Vous pouvez choisir de surveiller tous les AWS changements automatiques en activant les notifications d'observation des changements automatiques. Après avoir activé la notification Autoshift Observer, pour recevoir les notifications, choisissez d'être averti pour le type de détail de décalage automatique zonal. `Autoshift In Progress` Pour connaître les étapes à suivre pour activer la notification automatique des observateurs, reportez-vous Activation et utilisation de l'autoshift zonal à.

Pour des exemples, consultez la section Exemples d'événements de décalage automatique zonal.

- Sélectionnez tous les événements du changement automatique de zone où un changement automatique a commencé.

  Notez ce qui suit :

  - Si la notification automatique des observateurs est activée, ARC renvoie tous les événements de décalage automatique.
  - Si la notification automatique des observateurs n'est pas activée, ARC renvoie les événements de décalage automatique uniquement lorsqu'une ressource que vous avez configurée pour le décalage automatique zonal est incluse dans un décalage automatique.

```
{
    "source": [
```

```
        "aws.arc-zonal-shift"
    ],
    "detail-type": [
        "Autoshift In Progress"
    ]
}
```

- 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

Cette section contient des exemples d'événements pour les actions de changement automatique par zone.

Voici un exemple d'événement pour cette `Autoshift In Progress` action, lorsque 1) la notification automatique des observateurs est activée et 2) que vous n'avez pas configuré une ressource avec un décalage automatique zonal incluse dans un changement automatique :

```
{
```

```
    "version": "0",
    "id": "05d4d2d5-9c76-bfea-72d2-d4614802adb4",
    "detail-type": "Autoshift In Progress",
    "source": "aws.arc-zonal-shift",
    "account": "111122223333",
    "time": "2023-11-16T23:38:14Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "version": "0.0.1",
        "data": "",
        "metadata": {
            "awayFrom": "use1-az2",
            "notes":"AWS has started an autoshift for an impaired Availability Zone.
 This notification
            is separate from autoshift notifications for resources, if any, that you
 have configured for
            zonal autoshift. For details, see the Developer Guide."
        }
    }
}
```

Voici un exemple d'événement pour cette `Autoshift In Progress` action, lorsque 1) la notification automatique par l'observateur est désactivée et 2) vous avez configuré une ressource avec un décalage automatique zonal qui est incluse dans un changement automatique :

```
{
    "version": "0",
    "id": "05d4d2d5-9c76-bfea-72d2-d4614802adb4",
    "detail-type": "Autoshift In Progress",
    "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": "",
        "metadata": {
            "awayFrom": "use1-az2",
            "notes":""
```

```
        }
    }
}
```

Voici un exemple d'événement pour cette `Practice Run Interrupted` action :

```
{
    "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"
        }
    }
}
```

Voici un exemple d'événement pour cette `FIS Experiment Autoshift In Progress` action :

```
{
    "version": "0",
    "id": "05d4d2d5-9c76-bfea-72d2-d4614802adb4",
    "detail-type": "FIS Experiment Autoshift In Progress",
    "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": "",
        "metadata": {
            "awayFrom": "use1-az2",
            "notes":""
        }
    }
}
```

Voici un exemple d'événement pour cette `Manual Shift Started` action. Il est émis lorsque l'`StartZonalShift`API est appelée sur une ressource :

```
{
    "version": "0",
    "id": "05d4d2d5-9c76-bfea-72d2-d4614802adb4",
    "detail-type": "Manual Shift Started",
    "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": "",
        "metadata": {
            "awayFrom": "use1-az2",
            "notes":""
        }
    }
}
```

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 :

JSON

```
{
    "Version":"2012-10-17",

    "Statement": [
        {
            "Action": [
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "events.amazonaws.com",
                    "delivery.logs.amazonaws.com"
```

```
                ]
            },
            "Resource": "arn:aws:logs:us-east-1:222222222222:log-group:/aws/
events/*:*",
            "Sid": "TrustEventsToStoreLogEvent"
        }
    ]
}
```

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 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 automatique de zone dans ARC

Gestion des identités et des accès AWS (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. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Table des matières

- Exemples de politiques basées sur l'identité pour le changement automatique de zone dans ARC
- Utilisation du rôle lié au service pour le changement automatique de zone dans ARC
- AWS politiques gérées pour l'autoshift zonal dans ARC

Comment fonctionne le changement automatique de zone dans ARC avec IAM

Avant d'utiliser IAM pour gérer l'accès à l'autoshift zonal dans Amazon Application Recovery Controller (ARC), découvrez quelles fonctionnalités IAM peuvent être utilisées avec l'autoshift zonal.

Fonctionnalités IAM que vous pouvez utiliser avec le changement automatique de zone dans ARC

Fonctionnalité IAM	Support de changement automatique par zone
Politiques basées sur l’identité	Oui
Politiques basées sur les ressources	Non
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition de politique	Oui
ACLs	Non
ABAC (identifications dans les politiques)	Partielle
Informations d’identification temporaires	Oui
Autorisations de principal	Oui
Rôles 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 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 Définition d’autorisations IAM personnalisées avec des politiques gérées par le client 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. 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 ARC, consultez. Exemples de politiques basées sur l'identité dans Amazon Application Recovery Controller (ARC)

Politiques basées sur les ressources au sein d'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. Par exemple, les politiques de confiance de rôle IAM et les politiques de compartiment Amazon S3 sont des politiques basées sur les ressources. 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 l'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. Intégration d’actions dans une politique afin d’accorder l’autorisation d’exécuter les opérations associées.

Pour consulter la liste des actions ARC relatives à l'autoshift zonal, consultez la section Actions définies par Amazon Route 53 Zonal Shift dans le Service Authorization Reference.

Les actions de stratégie dans 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 voir des exemples de politiques basées sur l'identité ARC pour le changement automatique zonal, voir. Exemples de politiques basées sur l'identité pour le changement automatique de zone dans ARC

Ressources relatives aux politiques relatives au changement automatique par zone dans 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. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, 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 leurs actions ARNs, 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 voir des exemples de politiques basées sur l'identité ARC pour le changement automatique zonal, voir. Exemples de politiques basées sur l'identité pour le changement automatique de zone dans ARC

Clés de condition de politique pour le changement automatique zonal dans 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` indique à quel moment les instructions s'exécutent en fonction de critères définis. 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. 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 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 voir des exemples de politiques basées sur l'identité ARC pour le changement automatique zonal, voir. Exemples de politiques basées sur l'identité pour le changement automatique de zone dans ARC

Listes de contrôle d'accès (ACLs) dans ARC

Supports ACLs : Non

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLs 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 ARC

Prend en charge ABAC (identifications dans les politiques) : partiellement

Le contrôle d'accès par attributs (ABAC) est une stratégie d'autorisation qui définit les autorisations en fonction des attributs nommés balise. Vous pouvez associer des balises aux entités et aux AWS ressources IAM, puis concevoir des politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de la ressource.

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 ABAC, consultez Définition d'autorisations avec l'autorisation 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 dans ARC inclut la prise en charge partielle suivante pour ABAC :

- L'autoshift zonal prend en charge l'ABAC pour les ressources gérées enregistrées dans 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 ARC

Prend en charge les informations d’identification temporaires : oui

Les informations d'identification temporaires fournissent un accès à court terme aux AWS ressources et sont automatiquement créées lorsque vous utilisez la fédération ou que vous changez de rôle. 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 et Services AWS compatibles avec IAM dans le Guide de l’utilisateur IAM.

Autorisations principales interservices pour 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 des 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 ARC

Prend en charge les rôles de service : Non

Un rôle de service est un rôle IAM qu’un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer un rôle de service à partir d’IAM. Pour plus d’informations, consultez Création d’un rôle pour la délégation d’autorisations à un Service AWS dans le Guide de l’utilisateur IAM.

Rôles liés à un service pour 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 aux services ARC, consultez. Utilisation du rôle lié au service pour le changement automatique de zone dans 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 de zone dans ARC

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier des ressources ARC. 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.

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 IAM (console) dans le Guide de l'utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par ARC, y compris le ARNs format de chaque type de ressource, consultez la section Actions, ressources et clés de condition pour Amazon Application Recovery Controller (ARC) dans le Service Authorization Reference.

Rubriques

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

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer des ressources 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 le AWS client 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.

- Accordez 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 d'IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utilisez 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 CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez l'Analyseur d'accès IAM pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : l'Analyseur d'accès IAM 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 politiques avec 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 la MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Sécurisation de l'accès aux API avec 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 Application Recovery Controller (ARC), 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 votre Compte AWS. Si vous créez une politique 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 politique.

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 ARC. Pour en savoir plus, veuillez consulter la section Utilisation du rôle lié au service pour le changement automatique de zone dans 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 :

JSON

```
{
    "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

Vous pouvez utiliser une politique pour garantir qu'un utilisateur peut utiliser les actions de l'API ARC 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 un trafic sain AZs 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 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 ARC.

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

JSON

```
{
    "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 ARC

L'autoshift zonal dans Amazon Application Recovery Controller utilise un rôle lié à un Gestion des identités et des accès AWS service (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié à un service, dans ce cas, ARC. Le rôle lié au service est prédéfini par l'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 d'ARC, car vous n'avez pas à ajouter manuellement les autorisations nécessaires. L'ARC définit les autorisations pour le rôle lié au service et, sauf

indication contraire, seul l'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 de zone 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 AWSService RoleForZonalAutoshiftPracticeRun

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

- Surveillez les CloudWatch alarmes et les Tableau de bord Health 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 AWSService RoleForZonalAutoshiftPracticeRun

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

Le rôle lié à un service AWSServiceRoleForZonalAutoshiftPracticeRun approuve le fait que le service suivant endosse le rôle :

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

Pour voir les autorisations de cette stratégie, consultez AWSZonalAutoshiftPracticeRunSLRPolicy dans le AWS Guide de référence des stratégies gérées par.

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 ARC

Vous n'avez pas besoin de créer manuellement un rôle lié au service AWSServiceRoleForZonalAutoshiftPracticeRun. Lorsque vous créez la première configuration d'exécution dans le SDK AWS Management Console AWS CLI, le ou un AWS SDK, 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, ARC crée à nouveau le rôle lié au service pour vous.

Modification du rôle AWSServiceRoleForZonalAutoshiftPracticeRunlié à un service pour ARC

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 IAM Guide de l'utilisateur.

Suppression du rôle AWSServiceRoleForZonalAutoshiftPracticeRunlié à un service pour 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 ARC.

> **Note**
>
> Si le service 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 AWSService RoleForZonalAutoshiftPracticeRun 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 ARC pour le changement automatique zonal

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

AWS politiques gérées pour l'autoshift zonal dans ARC

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

AWS politique gérée : AWSZonal AutoshiftPracticeRun SLRPolicy

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 Application Recovery Controller (ARC) d'effectuer les opérations suivantes pour le transfert automatique zonal :

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

- Gérez des contrôles de capacité équilibrés pour les essais et les changements automatiques

Pour de plus amples informations, veuillez consulter Utilisation du rôle lié au service pour le changement automatique de zone dans 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 l'autoshift zonal dans ARC depuis que ce service a commencé à suivre ces modifications, voir. Mises à jour des politiques AWS gérées pour Amazon Application Recovery Controller (ARC) Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au flux RSS sur la page d'historique du document ARC.

Quotas pour l'autoshift zonal

L'autoshift zonal dans Amazon Application Recovery Controller (ARC) est soumis aux quotas suivants.

Entité	Quota
Nombre d'alarmes de résultat par configuration d'exécution d'entraînement	10 Vous pouvez demander une augmentation de quota.
Nombre d'alarmes de blocage par configuration d'entraînement	10 Vous pouvez demander une augmentation de quota.

Utiliser le contrôle de routage pour restaurer des applications multirégionales dans ARC

Cette section explique comment utiliser la fonctionnalité de contrôle du routage d'Amazon Application Recovery Controller (ARC) 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 d'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 ARC

Pour transférer le trafic vers plusieurs répliques d'applications Régions AWS, vous pouvez utiliser les contrôles de routage d'Amazon Application Recovery Controller (ARC) 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 dans 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 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 dans ARC est un plan de données composé de points de terminaison répartis sur 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 préparer l'utilisation de l'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 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 l'ARC l'a mis à jour pour le définir comme sain ou non sain, en fonction de l'état du 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 de plus amples informations, veuillez consulter 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 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 associé aux contrôles de santé de Route 53 et aux ensembles d'enregistrements DNS, en utilisant des enregistrements DNS dotés de 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 Application Recovery Controller (ARC), 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.

Avantages du contrôle de routage

Un contrôle de routage dans ARC présente plusieurs avantages par rapport au réacheminement du trafic avec les contrôles 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 Application Recovery Controller (ARC), consultez la section Points de terminaison et quotas Amazon Application Recovery Controller (ARC) dans le manuel Amazon Web Services General Reference.

> **Note**
>
> Le contrôle du routage dans Amazon Application Recovery Controller (ARC) est une fonctionnalité globale. Toutefois, vous devez spécifier la région USA Ouest (Oregon) (spécifiez le paramètre`--region us-west-2`) dans AWS CLI les commandes ARC régionales. 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 est un on/off commutateur qui modifie l'état d'un bilan de santé 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 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 ARC pour le basculement lors de scénarios de reprise après sinistre. Pour de plus amples informations, veuillez consulter Obtenir et mettre à jour les états de contrôle de routage à l'aide de l'API ARC (recommandé).

L'ARC gère les états de contrôle du routage dans un cluster, qui est un ensemble de cinq points de terminaison régionaux redondants. 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 ARC un état de contrôle de routage, à l'aide de l'API et du plan de données hautement fiable, il renvoie la vue consensuelle.

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`. 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.

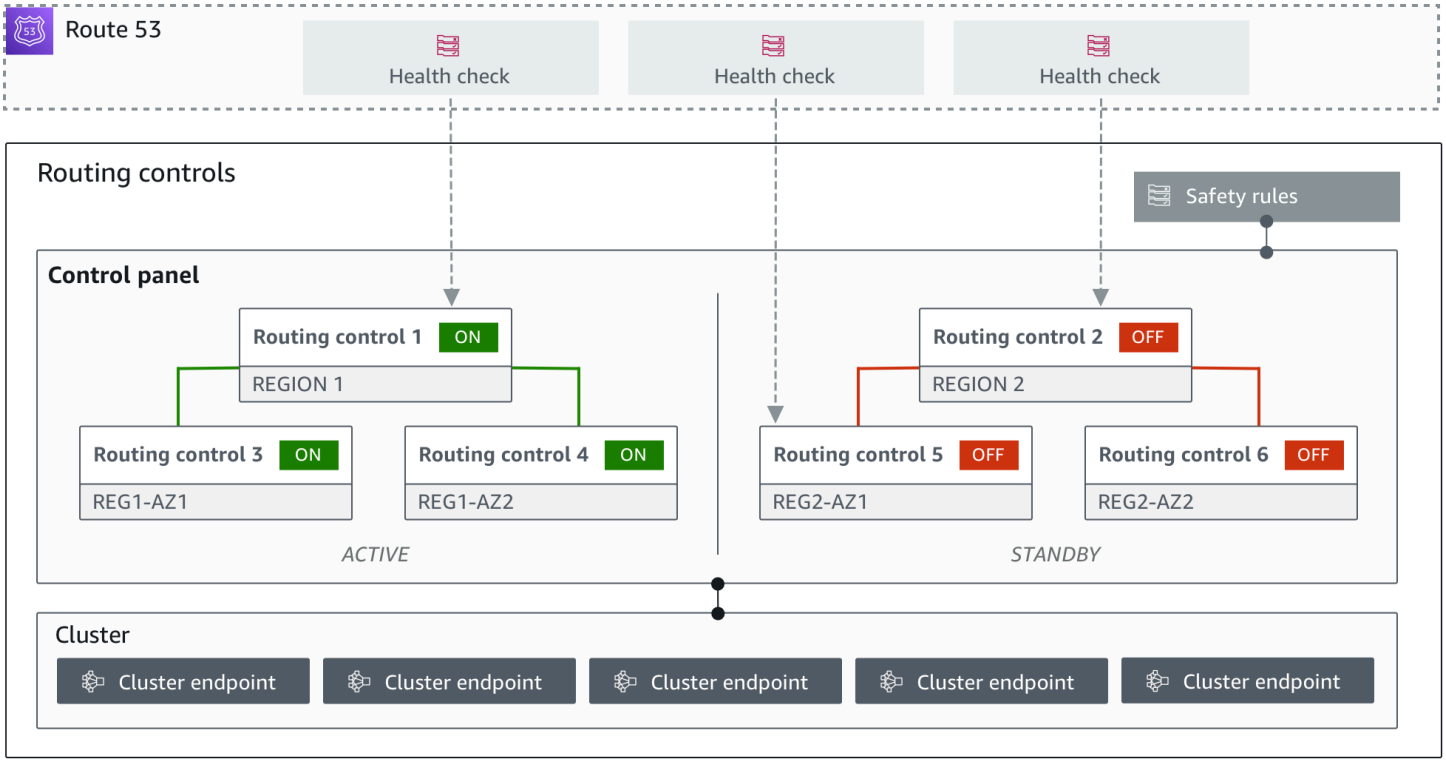
ARC offre une fiabilité extrême grâce à son plan de données qui vous permet de basculer manuellement entre les cellules de votre application. L'ARC garantit qu'au moins trois des cinq points de terminaison du cluster sont toujours accessibles pour effectuer des modifications de l'état du contrôle de routage. Notez que chaque cluster ARC est à locataire unique, afin de ne pas être affecté par les « voisins bruyants » susceptibles de ralentir vos modèles 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 participent au 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 fonction de contrôle de routage dans 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 de contrôle du routage, 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 dans 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 on/off commutateur, 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 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 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, 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, 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 d'ARC possède cinq points de terminaison régionaux que vous pouvez utiliser pour définir et récupérer les états du contrôle de routage. Votre processus d'accès aux points de terminaison doit partir du principe qu'ARC active et arrête régulièrement les points de terminaison à des fins de maintenance. Vous devez donc essayer chaque point de terminaison l'un après l'autre jusqu'à ce que vous vous connectiez à un. 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 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 Application Recovery Controller (ARC)

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 de routage dans ARC :

- Clusters
- Panneaux de commande
- Règles de sécurité

Le balisage dans ARC est uniquement disponible 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 Application Recovery Controller (ARC).

Tarification du contrôle de routage dans ARC

Pour le contrôle du routage dans 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 de plus amples informations, veuillez consulter Support de comptes croisés pour les clusters dans ARC.

Pour obtenir des informations détaillées sur la tarification de l'ARC et des exemples de tarification, consultez la section Tarification de l'ARC.

Commencer à utiliser la restauration multirégionale dans Amazon Application Recovery Controller (ARC)

Pour faire basculer vos applications à l'aide du contrôle de routage dans Amazon Application Recovery Controller (ARC), 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 de plus amples informations, veuillez consulter Utilisez le décalage de zone et le décalage automatique de zone pour récupérer des applications dans ARC.

Afin de pouvoir utiliser le contrôle de routage ARC 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 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 Application Recovery Controller (ARC) 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 des actions ARC, 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 CloudFormation modèles pour simplifier le processus, ainsi qu'un CloudFormation modèle téléchargeable afin que vous puissiez rapidement explorer vous-même la configuration et l'utilisation d'ARC.

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

Pour commencer avec un exemple d'application et des CloudFormation modèles, consultez les instructions README du GitHubréférentiel ARC. Pour en savoir plus sur l'utilisation CloudFormation des modèles, consultez CloudFormation les concepts du Guide de AWS CloudFormation l'utilisateur.

Meilleures pratiques pour le contrôle du routage dans ARC

Nous recommandons les meilleures pratiques suivantes en matière de restauration et de préparation au basculement pour le contrôle du routage dans ARC.

Rubriques

- Conservez les informations d' AWS identification spécialement conçues et durables, sécurisées et toujours accessibles
- Choisissez des valeurs TTL inférieures pour les enregistrements DNS impliqués dans le basculement
- Limitez le temps pendant lequel les clients restent connectés à vos terminaux
- Ajoutez à vos favoris ou codez en dur vos cinq points de terminaison du cluster régional et le contrôle du routage ARNs
- Choisissez l'un de vos points de terminaison au hasard pour mettre à jour vos états de contrôle de routage
- 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

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

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 Application Recovery Controller (ARC) 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 le contrôle du routage ARNs

Nous vous recommandons de conserver une copie locale des points de terminaison de votre cluster régional ARC, dans des signets 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 qui ne sont pas hébergées sur le cluster de plans de données extrêmement fiable. Vous pouvez répertorier les points de terminaison de vos clusters 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

Les contrôles de routage fournissent cinq points de terminaison régionaux pour garantir une haute disponibilité, même en cas de panne. Pour atteindre leur résilience totale, il est important de disposer d'une logique de nouvelle tentative capable d'utiliser les cinq points de terminaison selon les besoins. Pour plus d'informations sur l'utilisation d'exemples de code avec le AWS SDK, y compris des exemples pour essayer des points de terminaison de cluster, consultez. Exemples de code pour Application Recovery Controller utilisant AWS SDKs

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, visualisez vos contrôles et états de routage avec l'ListRoutingControlsopération et mettez à jour les états des contrôles de routage pour rediriger le trafic en vue d'un basculement avec l'UpdateRoutingControlStateopération. Vous pouvez utiliser le AWS CLI (comme dans ces exemples) ou le code que vous écrivez à l'aide de l'un des AWS SDKs. 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 qu'ARC utilise 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 de plus amples informations, veuillez consulter Dérogation aux règles de sécurité pour réacheminer le trafic.

Tester le basculement avec ARC

Testez régulièrement le basculement avec le contrôle de routage ARC, 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 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 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 défaillance 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 Application Recovery Controller (ARC), 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, voirExemples d'utilisation des opérations de l'API de contrôle de routage ARC avec AWS CLI.

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

Action	Utilisation de la console ARC	Utilisation de l'API ARC
Créer un cluster	Consultez Création de composants de contrôle de routage dans ARC	Consultez CreateCluster
Description d'un cluster	Consultez Création de composants de contrôle de routage dans ARC	Consultez DescribeCluster
Supprimer un cluster	Consultez Création de composants de contrôle de routage dans ARC	Consultez DeleteCluster
Répertorier les clusters d'un compte	Consultez Création de composants de contrôle de routage dans ARC	Consultez ListClusters
Création d'un contrôle de routage	Consultez Création de composants de contrôle de routage dans ARC	Consultez CreateRoutingControl

Action	Utilisation de la console ARC	Utilisation de l'API ARC
Décrire un contrôle de routage	Consultez Création de composants de contrôle de routage dans ARC	Consultez DescribeRoutingControl
Mettre à jour un contrôle de routage	Consultez Création de composants de contrôle de routage dans ARC	Consultez UpdateRoutingControl
Supprimer un contrôle de routage	Consultez Création de composants de contrôle de routage dans ARC	Consultez DeleteRoutingControl
Lister les contrôles de routage	Consultez Création de composants de contrôle de routage dans ARC	Consultez ListRoutingControls
Création d'un panneau de commande	Consultez Création de composants de contrôle de routage dans ARC	Consultez CreateControlPanel
Décrire un panneau de commande	Consultez Création de composants de contrôle de routage dans ARC	Consultez DescribeControlPanel
Mettre à jour un panneau de commande	Consultez Création de composants de contrôle de routage dans ARC	Consultez UpdateControlPanel
Supprimer un panneau de commande	Consultez Création de composants de contrôle de routage dans ARC	Consultez DeleteControlPanel
Lister les panneaux de commande	Consultez Création de composants de contrôle de routage dans ARC	Consultez ListControlPanels

Action	Utilisation de la console ARC	Utilisation de l'API ARC
Création d'une règle de sécurité	Consultez Création de règles de sécurité pour le contrôle du routage	Consultez CreateSafetyRule
Décrire une règle de sécurité	Consultez Création de règles de sécurité pour le contrôle du routage	Consultez DescribeSafetyRule
Mettre à jour une règle de sécurité	Consultez Création de règles de sécurité pour le contrôle du routage	Consultez UpdateSafetyRule
Supprimer une règle de sécurité	Consultez Création de règles de sécurité pour le contrôle du routage	Consultez DeleteSafetyRule
Énumérer les règles de sécurité	Consultez Création de règles de sécurité pour le contrôle du routage	Consultez ListSafetyRules
Répertorier les bilans de santé associés à Route 53	Consultez Création d'un contrôle de santé du contrôle de routage dans ARC	Voir ListAssociatedRoute53 HealthChecks
Répertorier les politiques de AWS RAM ressources pour le partage de clusters	Consultez Support de comptes croisés pour les clusters dans ARC	Voir GetResourcePolicy

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

Action	Utilisation de la console ARC	Utilisation de l'API ARC
Obtenir un état de contrôle de routage	Consultez Obtenir et mettre à jour les états de contrôle	Consultez GetRoutingControlS tate

Action	Utilisation de la console ARC	Utilisation de l'API ARC
	de routage dans AWS Management Console	
Lister les contrôles de routage	N/A	Consultez ListRoutingControls
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	Consultez 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	Consultez UpdateRoutingControlStates

Utilisation de ce service avec un AWS SDK

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

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

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

Pour voir des exemples spécifiques à ce service, consultez Exemples de code pour Application Recovery Controller utilisant AWS SDKs.

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

Exemples d'utilisation des opérations de l'API de contrôle de routage ARC 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 Application Recovery Controller (ARC) 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 Application Recovery Controller (ARC), 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 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**
>
> ARC est un service mondial qui prend en charge plusieurs Régions AWS terminaux. 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 l'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, 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 etOpérations 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 est un ensemble de cinq points de terminaison, un dans chacun des cinq points différents Régions AWS. L'infrastructure ARC permet à ces terminaux de fonctionner de manière coordonnée afin de garantir une haute disponibilité et une cohérence séquentielle des opérations de basculement.

1. Créer un cluster

1a. Créer un cluster. `network-type`C'est facultatif et peut être `IPV4` ou`DUALSTACK`. La valeur par défaut est `IPV4`.

```
aws route53-recovery-control-config create-cluster --cluster-name test --network-type
 DUALSTACK
```

```
"Cluster": {
    "ClusterArn": "arn:aws:route53-recovery-
control::123456789123:cluster/12341234-1234-1234-1234-123412341234",
    "Name": "test",
    "Status": "PENDING",
    "Owner": "123456789123",
    "NetworkType": "DUALSTACK"
}
```

Lorsque vous créez une ressource ARC 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::123456789123:cluster/12341234-1234-1234-1234-123412341234",
    "Name": "test",
    "Status": "DEPLOYED",
    "Owner": "123456789123",
    "NetworkType": "DUALSTACK"
}
```

Lorsque le statut est DÉPLOYÉ, 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`.

1c. Répertoriez vos clusters.

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

```
"Cluster": {
```

```
    "ClusterArn": "arn:aws:route53-recovery-
control::123456789123:cluster/12341234-1234-1234-1234-123412341234",
    "Name": "test",
    "Status": "DEPLOYED",
    "Owner": "123456789123",
    "NetworkType": "DUALSTACK"
}
```

1d. Mettez à jour le type de réseau pour vos clusters. Les options sont `IPV4` ou `DUALSTACK`.

```
aws route53-recovery-control-config update-cluster \
--cluster-arn arn:aws:route53-recovery-
control::123456789123:cluster/12341234-1234-1234-1234-123412341234 \
--network-type DUALSTACK
```

```
"Cluster": {
    "ClusterArn": "arn:aws:route53-recovery-
control::123456789123:cluster/12341234-1234-1234-1234-123412341234",
    "Name": "test",
    "Status": "PENDING",
    "Owner": "123456789123",
   "NetworkType": "DUALSTACK"
}
```

2. Création d'un panneau de commande

Un panneau de commande est un regroupement logique permettant d'organiser vos commandes de routage ARC. Lorsque vous créez un cluster, 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 pour la première fois, son statut est `PENDING` alors qu'elle est 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. 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, comme 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 Routing Control pour Amazon 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 Routing Control pour Amazon 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
0123456bbbbbbb0123456bbbbbb0123456333333444444
```

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. Création de surveillances de l’état

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 définit le contrôle de santé sur échec, de sorte que 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 l'ARC CLI pour créer un contrôle de routage pour chaque cellule.
2. Utilisez la CLI Route 53 pour créer un contrôle de santé 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 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-fffff22222",
    "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 de la référence de AWS CLI commande Amazon Route 53 pour la change-resource-record-setscommande. 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 vos ressources Amazon Application Recovery Controller (ARC), 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, 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 utilisant AWS SDKs.

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, consultezOpérations 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. L'ARC offre une fiabilité extrême grâce au plan de données de contrôle de routage ARC permettant de rediriger le trafic et de basculer entre les cellules. Pour plus de recommandations sur l'utilisation d'ARC pour le basculement, consultezMeilleures pratiques pour le contrôle du routage dans 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 d'API de configuration du contrôle de restauration. Nous vous recommandons de conserver une copie locale des points de terminaison de votre cluster régional 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.

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 ARC

Rubriques

Création de composants de contrôle de routage dans 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 Application Recovery Controller (ARC).

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 ARC détenues par plusieurs Comptes AWS. Pour en savoir plus sur le partage de ressources dans ARC,Support de comptes croisés pour les clusters dans ARC. Pour plus d'informations sur les tarifs, consultez la section Tarification d'Amazon Application Recovery Controller (ARC).

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 de plus amples informations, veuillez consulter Création de règles de sécurité pour le contrôle du routage.

Les étapes de création des composants pour le contrôle du routage sur la console 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 ARC, consultez leOpérations de l'API de contrôle du routage.

Création d'un cluster dans ARC

Vous devez créer un cluster pour héberger les commandes de routage et les panneaux de commande dans 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 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 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 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 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 Application Recovery Controller

(ARC) 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 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 qu'ARC puisse 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, consultezObtenir et mettre à jour les états de contrôle de routage à l'aide de l'API 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 ARC, consultezExemples d'utilisation des opérations de l'API de contrôle de routage ARC avec AWS CLI.

Création d'un panneau de commande dans ARC

Un panneau de configuration dans Amazon Application Recovery Controller (ARC) 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, 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 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 ARC, consultez leOpérations de l'API de contrôle du routage.

Pour créer un panneau de commande

1. Ouvrez la console 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 ARC

Cette section explique comment afficher et mettre à jour les états du contrôle de routage dans Amazon Application Recovery Controller (ARC). 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 ARC ou à l'aide de l'API ARC. Nous vous recommandons de mettre à jour les états du contrôle de routage à l'aide de l'API. Tout d'abord, ARC offre une fiabilité extrême grâce à l'API située dans le 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 `Off` 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 de routage à l'aide de l'API ARC (recommandé)

Nous vous recommandons d'utiliser les opérations d'API d'Amazon Application Recovery Controller (ARC) pour obtenir ou mettre à jour les états de contrôle de routage, à l'aide d'une AWS CLI commande ou d'un code que vous avez développé pour utiliser les opérations d'API ARC avec l'un des AWS SDKs. 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.

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. L'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 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 utilisant AWS SDKs.
- Pour plus d'informations sur l'utilisation du AWS CLI pour obtenir et mettre à jour les états de contrôle de routage, consultezRépertoriez 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 à l'aide de l'API Amazon Application Recovery Controller (ARC). De plus, la console n'est pas très disponible alors que le plan de données ARC offre une fiabilité extrême. Pour ces raisons, nous vous recommandons d'utiliser l'API ARC pour obtenir et mettre à jour les états de contrôle de routage pour les opérations de production.

Pour plus de recommandations sur l'utilisation d'ARC pour le basculement, consultezMeilleures pratiques pour le contrôle du routage dans 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 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 la https://console.aws.amazon.com/route53/maison.
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'`Off`ils soient ou`On`, 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 ARC, vous créez 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

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, 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 dansExemples d'utilisation des opérations de l'API de contrôle de routage ARC 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 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 dansExemples d'utilisation des opérations de l'API de contrôle de routage ARC 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 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 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 du routage avec Amazon Application Recovery Controller (ARC), consultezOpérations de l'API de contrôle du routage.

Pour créer une règle de sécurité

1. Ouvrez la console 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 à son AssertionRulefonctionnement dans le Guide de référence de l'API de

contrôle de routage pour Amazon 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 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 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 Application Recovery Controller (ARC), consultez leOpérations de l'API de contrôle du routage.

Pour supprimer une règle de sécurité

1. Ouvrez la console 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 séparée par des virgules ARNs pour annuler deux ou plusieurs 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 une règle de sécurité ARNs à la liste des règles à remplacer dans la commande de mise à jour, séparées 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 SDKs voir 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 de comptes croisés pour les clusters dans ARC

Amazon Application Recovery Controller (ARC) 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 le contrôle du routage 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 utilisant AWS Resource Access Manager pour partager les ressources du cluster entre les comptes dans ARC, vous pouvez utiliser un cluster pour héberger des panneaux de contrôle et des contrôles de routage appartenant à plusieurs comptes différents 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 (OUs) dans AWS Organizations, en 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 l'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 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 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 des opérations de l'API ARC à l'aide du AWS Command Line Interface ou AWS SDKs.

Cette rubrique explique comment partager les ressources que vous possédez et comment utiliser les ressources qui sont partagées avec vous.

Table des matières

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 .
- AWS RAM les partages de ressources pour les ressources mondiales telles que les clusters doivent être créés dans la région USA Est (Virginie du Nord) (us-east-1).

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 dans le cluster.

Pour partager un cluster, vous devez l'ajouter à un partage de ressources. Un partage de ressources est une ressource AWS RAM qui vous permet de partager vos ressources entre des Comptes AWS. Un partage de ressources 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 les opérations AWS RAM d'API avec le AWS Command Line Interface ou AWS SDKs.

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 à l'aide d'opérations d' AWS RAM API avec le AWS CLI ou SDKs.

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.

Octroi d'autorisations pour partager des clusters

Le partage de clusters entre comptes nécessite des autorisations pour le principal IAM qui partage le cluster via AWS RAM.

Nous vous recommandons d'utiliser la politique IAM `AmazonRoute53RecoveryControlConfigFullAccess` gérée pour garantir que vos principaux IAM disposent des autorisations requises pour partager et utiliser des clusters partagés.

Le partage d'un cluster à l'aide d'une politique IAM personnalisée nécessite `route53-recovery-control-config:PutResourcePolicyroute53-recovery-control-config:GetResourcePolicy`, et `route53-recovery-control-config:DeleteResourcePolicy` des autorisations pour ce cluster. `PutResourcePolicy`et `DeleteResourcePolicy` sont des actions IAM avec autorisation uniquement. Toute tentative de partage d'un cluster AWS RAM sans disposer de ces autorisations entraînera une erreur.

Pour plus d'informations sur le mode d' AWS Resource Access Manager utilisation de l'IAM, voir Comment AWS Resource Access Manager utilise l'IAM dans le guide de l'AWS RAM utilisateur.

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 le AWS CLI ou SDKs.

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 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.

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 ARC à l'aide de la commande AWS Command Line Interface ou AWS SDKs.

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 contrôle 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 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 section Tarification d'Amazon Application Recovery Controller (ARC).

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 des 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 Application Recovery Controller (ARC)

Vous pouvez l'utiliser AWS CloudTrail pour surveiller le contrôle du routage dans Amazon Application Recovery Controller (ARC), afin d'analyser les modèles et de résoudre les problèmes.

Rubriques

- Journalisation des appels d'API ARC à l'aide de AWS CloudTrail

Journalisation des appels d'API ARC à l'aide de AWS CloudTrail

Amazon Application Recovery Controller (ARC) est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions effectuées par un utilisateur, un rôle ou un AWS service dans ARC. CloudTrail capture tous les appels d'API pour ARC sous forme d'événements. Les appels capturés incluent des appels provenant de la console ARC et des appels de code vers les opérations de l'API 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 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 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 ARC dans CloudTrail

CloudTrail est activé sur votre compte Compte AWS lorsque vous créez le compte. Lorsqu'une activité se produit dans 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 l'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 ARC sont enregistrées CloudTrail et documentées dans le Guide de référence de l'API Recovery Readiness pour Amazon Application Recovery Controller, le Guide de référence de l'API de configuration de Recovery Control pour Amazon Application Recovery Controller et le Guide de référence de l'API de contrôle du routage pour Amazon 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 Gestion des identités et des accès AWS (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 de plus amples informations, veuillez consulter l'élément userIdentity CloudTrail .

Afficher les événements 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, 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

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 dans

Gestion des identités et des accès AWS (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. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Table des matières

Comment fonctionne le contrôle du routage dans Amazon Application Recovery Controller (ARC) avec IAM

Avant d'utiliser IAM pour gérer l'accès au contrôle de routage dans Amazon Application Recovery Controller (ARC), découvrez quelles fonctionnalités IAM sont disponibles pour le contrôle de routage.

Fonctionnalités IAM que vous pouvez utiliser avec le contrôle du routage dans Amazon Application Recovery Controller (ARC)

Fonctionnalité 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 de politique	Oui
ACLs	Non
ABAC (identifications dans les politiques)	Partielle
Informations d’identification temporaires	Oui
Autorisations de principal	Oui
Rôles 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 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 Définition d'autorisations IAM personnalisées avec des politiques gérées par le client 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. 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 voir des exemples de politiques basées sur l'identité ARC pour le contrôle du routage, consultez. Exemples de politiques basées sur l'identité pour le contrôle du routage dans ARC

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. Par exemple, les politiques de confiance de rôle IAM et les politiques de compartiment Amazon S3 sont des politiques basées sur les ressources. 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. Intégration d'actions dans une politique afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour consulter la liste des actions ARC pour le contrôle du routage, consultez les sections Actions définies par Amazon Route 53 Recovery Controls et Actions définies par Amazon Route 53 Recovery Cluster dans le Service Authorization Reference.

Les actions de politique dans 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 voir des exemples de politiques basées sur l'identité ARC pour le contrôle du routage, consultez. Exemples de politiques basées sur l'identité pour le contrôle du routage dans ARC

Ressources politiques pour l'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. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, 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 l'ARC :

Pour consulter la liste des types de ressources et leurs actions ARNs, 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 voir des exemples de politiques basées sur l'identité ARC pour le contrôle du routage, consultez. Exemples de politiques basées sur l'identité pour le contrôle du routage dans ARC

Clés de conditions de politique pour 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` indique à quel moment les instructions s'exécutent en fonction de critères définis. 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. 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 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 leurs caractéristiques ARNs, 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 ARC pour le contrôle du routage, voir Exemples de politiques basées sur l'identité pour le contrôle du routage dans ARC

Listes de contrôle d'accès (ACLs) dans ARC

Supports ACLs : Non

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLs 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 ARC

Prend en charge ABAC (identifications dans les politiques) : partiellement

Le contrôle d'accès par attributs (ABAC) est une stratégie d'autorisation qui définit les autorisations en fonction des attributs nommés balise. Vous pouvez associer des balises aux entités et aux AWS ressources IAM, puis concevoir des politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de la ressource.

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 ABAC, consultez Définition d'autorisations avec l'autorisation 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 inclut le support suivant 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 ARC

Prend en charge les informations d'identification temporaires : oui

Les informations d'identification temporaires fournissent un accès à court terme aux AWS ressources et sont automatiquement créées lorsque vous utilisez la fédération ou que vous changez de rôle. 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 et Services AWS compatibles avec IAM dans le Guide de l'utilisateur IAM.

Autorisations principales interservices pour 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 des 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 ARC

Prend en charge les rôles de service : Non

Un rôle de service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer un rôle de service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.

Rôles liés à un service pour ARC

Prend en charge les rôles liés aux services :

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 ARC

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier des ressources ARC. 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.

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 IAM (console) dans le Guide de l’utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par ARC, y compris le ARNs format de chaque type de ressource, consultez la section Actions, ressources et clés de condition pour Amazon Application Recovery Controller (ARC) dans le Service Authorization Reference.

Rubriques

- Bonnes pratiques en matière de politiques
- Exemple : accès à la console ARC pour le contrôle du routage
- Exemples : actions de l'API ARC pour la configuration du contrôle de routage

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer des ressources 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.
- Accordez 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 d'IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.

- Utilisez 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 CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez l'Analyseur d'accès IAM pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : l'Analyseur d'accès IAM 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 politiques avec 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 la MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Sécurisation de l'accès aux API avec 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 ARC pour le contrôle du routage

Pour accéder à la console Amazon Application Recovery Controller (ARC), 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 votre Compte AWS. Si vous créez une politique 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 politique.

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 ARC lorsque vous n'autorisez l'accès qu'à des opérations d'API spécifiques, associez également une politique `ReadOnly` AWS gérée pour ARC aux entités. Pour plus d'informations, consultez la page des politiques gérées par ARC ARC ou l'ajout d'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 ARC via la console, associez une politique telle que la suivante à l'utilisateur, afin de lui donner toutes les autorisations nécessaires pour configurer les ressources et les opérations de contrôle de routage ARC :

JSON

```
{
    "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 pour la configuration du contrôle de routage

Pour garantir qu'un utilisateur peut utiliser les actions de l'API ARC pour travailler avec la configuration du contrôle de routage 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 :

JSON

```
{
    "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 de contrôle de routage ARC 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 ARC IAM 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 de plus amples informations, veuillez consulter 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`

JSON

```
{
    "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 Application Recovery Controller (ARC)

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 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 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 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 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 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.

AWS politique gérée : AmazonApplicationRecoveryControllerRegionSwitchPlanExecutionPolicy

Vous pouvez attacher `AmazonApplicationRecoveryControllerRegionSwitchPlanExecutionPolicy` à vos entités IAM. Cette politique accorde des autorisations pour l'exécution et l'évaluation du plan de changement de la région ARC. Associez-le aux rôles IAM utilisés pour l'exécution du plan de changement de région.

Détails de l’autorisation

Cette politique inclut les autorisations suivantes :

- `arc-region-switch:GetPlan`— Permet aux principaux de récupérer les détails de configuration d'un plan de changement de région.
- `arc-region-switch:GetPlanExecution`— Permet aux principaux de récupérer des informations sur l'exécution d'un plan de changement de région spécifique.

- `arc-region-switch:ListPlanExecutions`— Permet aux principaux de répertorier toutes les exécutions des plans de changement de région.
- `iam:SimulatePrincipalPolicy`— Permet aux directeurs de simuler et d'évaluer les actions qu'un rôle IAM peut effectuer. Cette autorisation est limitée aux rôles IAM uniquement et est utilisée lors de l'évaluation du plan pour vérifier que les autorisations nécessaires sont en place avant d'exécuter un plan de changement de région.
- `cloudwatch:DescribeAlarms`— Permet aux directeurs de récupérer des informations sur les CloudWatch alarmes Amazon.
- `cloudwatch:DescribeAlarmHistory`— Permet aux principaux de récupérer l'historique des changements d'état des CloudWatch alarmes Amazon.
- `cloudwatch:GetMetricStatistics`— Permet aux principaux de récupérer des données statistiques pour les CloudWatch métriques Amazon.

Pour plus de détails sur cette politique, y compris la dernière version du document sur la politique JSON, consultez AmazonApplicationRecoveryControllerRegionSwitchPlanExecutionPolicy dans le Guide de référence de la politique gérée par AWS .

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 ARC depuis que ce service a commencé à suivre ces modifications, voirMises à jour des politiques AWS gérées pour Amazon Application Recovery Controller (ARC). Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au flux RSS sur la page d'historique du document ARC.

Quotas pour le contrôle du routage

Le contrôle du routage dans Amazon Application Recovery Controller (ARC) est soumis aux quotas suivants (anciennement appelés limites).

Entité	Quota
Nombre de clusters par compte	2
Nombre de panneaux de commande par cluster	50

Entité	Quota
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
Nombre d'appels d'API mutants vers un point de terminaison du cluster, par seconde	3

Vérification de l'état de préparation dans ARC

> **Note**
>
> La fonctionnalité de vérification du niveau de préparation d'Amazon Application Recovery Controller (ARC) ne sera plus ouverte aux nouveaux clients à compter du 30 avril 2026. Les clients existants peuvent continuer à utiliser le service normalement. Pour plus d'informations, consultez la section Modification de la disponibilité du test de disponibilité d'Amazon Application Recovery Controller (ARC).

Grâce au contrôle du niveau de préparation d'Amazon Application Recovery Controller (ARC), vous pouvez savoir si vos applications et ressources sont prêtes à être restaurées. Une fois que vous avez AWS modélisé votre application dans 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 ARC afin de configurer la structure permettant aux contrôles de disponibilité de fonctionner, en créant un groupe de récupération 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 l'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 Application Recovery Controller (ARC) ?

Note

La fonctionnalité de vérification du niveau de préparation d'Amazon Application Recovery Controller (ARC) ne sera plus ouverte aux nouveaux clients à compter du 30 avril 2026. Les clients existants peuvent continuer à utiliser le service normalement. Pour plus d'informations, consultez la section Modification de la disponibilité du test de disponibilité d'Amazon Application Recovery Controller (ARC).

Un contrôle de l'état de préparation effectué dans ARC permet de vérifier en permanence (à intervalles d'une minute) les incohérences en AWS termes de capacité allouée, de quotas de service, de limites d'accélération 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, lorsqu'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 supérieur. 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 pour 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 (AZs)).

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 contrôleurs ARC 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 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 d'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

ARC audite vos répliques d'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. 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 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, ARC détecte la non-concordance 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 préparation à l'ARC ne sont pas hautement disponibles, vous ne devez donc pas vous fier à ce qu'ils 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 de plus amples informations, veuillez consulter Utilisation du contrôle de préparation dans 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 de plus amples informations, veuillez consulter Opérations de l'API de contrôle de préparation.

Comment fonctionne le contrôle de préparation

ARC audite vos répliques d'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. 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 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, ARC détecte la non-concordance 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 préparation à l'ARC ne sont pas hautement disponibles, vous ne devez donc pas vous fier à ce qu'ils 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 de plus amples informations, veuillez consulter Utilisation du contrôle de préparation dans 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 de plus amples informations, veuillez consulter Opérations de l'API de contrôle de préparation.

Comment les règles de préparation déterminent l'état de préparation

> **Note**
>
> La fonctionnalité de vérification du niveau de préparation d'Amazon Application Recovery Controller (ARC) ne sera plus ouverte aux nouveaux clients à compter du 30 avril 2026. Les clients existants peuvent continuer à utiliser le service normalement. Pour plus d'informations, consultez la section Modification de la disponibilité du test de disponibilité d'Amazon Application Recovery Controller (ARC).

Les contrôles de préparation 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. L'ARC inclut un groupe de règles pour chaque type de ressource qu'il prend en charge. Par exemple, ARC dispose de 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 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, l'ARC prend une mesure supplémentaire en matière de quotas. Si un contrôle de préparation détecte une incompatibilité entre les cellules pour les quotas de service (valeur maximale pour la création de ressources et les opérations) pour une ressource prise en charge, 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 de plus amples informations, veuillez consulter Utilisation du contrôle de préparation dans ARC avec Amazon EventBridge.

Comment les contrôles de préparation, les ensembles de ressources et les périmètres de préparation fonctionnent ensemble

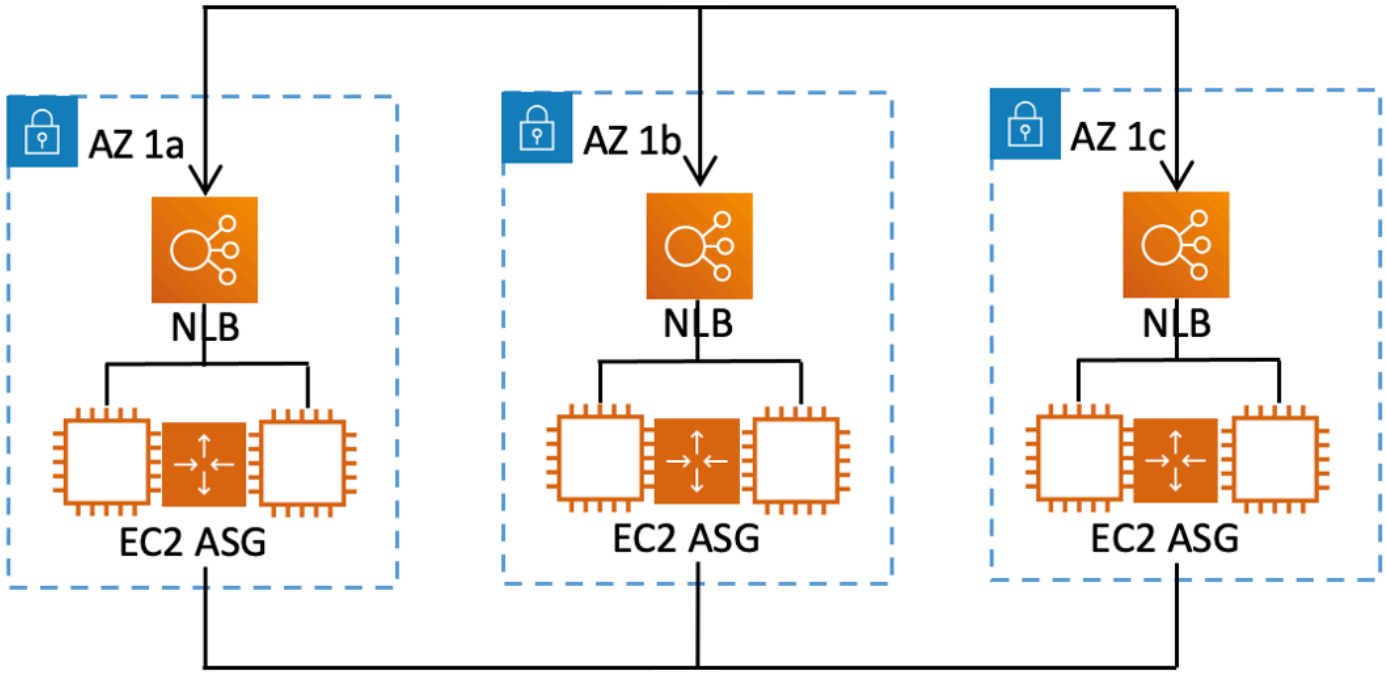
> **Note**
>
> La fonctionnalité de vérification du niveau de préparation d'Amazon Application Recovery Controller (ARC) ne sera plus ouverte aux nouveaux clients à compter du 30 avril 2026. Les clients existants peuvent continuer à utiliser le service normalement. Pour plus d'informations, consultez la section Modification de la disponibilité du test de disponibilité d'Amazon Application Recovery Controller (ARC).

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 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 préparation 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 le jeu 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 étendues de préparation permettent à l'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 limites de préparation, l'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

> **Note**
>
> La fonctionnalité de vérification du niveau de préparation d'Amazon Application Recovery Controller (ARC) ne sera plus ouverte aux nouveaux clients à compter du 30 avril 2026. Les clients existants peuvent continuer à utiliser le service normalement. Pour plus d'informations, consultez la section Modification de la disponibilité du test de disponibilité d'Amazon Application Recovery Controller (ARC).

Grâce aux contrôles de disponibilité des ressources cibles du DNS dans 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, 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.

L'ARC détecte automatiquement le nombre et l'étendue des cellules (représentant les répliques ou les unités de confinement des défaillances) dans votre application, et indique si les cellules sont cloisonnées par zone de disponibilité ou par région. ARC identifie ensuite et vous fournit des informations sur les ressources de l'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 de plus amples informations, veuillez consulter Obtenir des recommandations d'architecture dans ARC.

Contrôles de préparation et scénarios de reprise après sinistre

> **Note**
>
> La fonctionnalité de vérification du niveau de préparation d'Amazon Application Recovery Controller (ARC) ne sera plus ouverte aux nouveaux clients à compter du 30 avril 2026. Les clients existants peuvent continuer à utiliser le service normalement. Pour plus d'informations, consultez la section Modification de la disponibilité du test de disponibilité d'Amazon Application Recovery Controller (ARC).

Les tests de préparation à l'ARC vous permettent de savoir si vos applications et 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 l'ARC sont hébergés dans une seule AWS région, à savoir l'ouest des États-Unis (Oregon), et qu'en cas de panne ou de sinistre, les informations des contrôles de préparation peuvent devenir périmées ou ne plus être disponibles. Pour de plus amples informations, veuillez consulter Plans de données et de contrôle pour le contrôle du routage.

AWS Disponibilité de la région pour le contrôle de préparation

> **Note**
>
> La fonctionnalité de vérification du niveau de préparation d'Amazon Application Recovery Controller (ARC) ne sera plus ouverte aux nouveaux clients à compter du 30 avril 2026. Les clients existants peuvent continuer à utiliser le service normalement. Pour plus d'informations, consultez la section Modification de la disponibilité du test de disponibilité d'Amazon Application Recovery Controller (ARC).

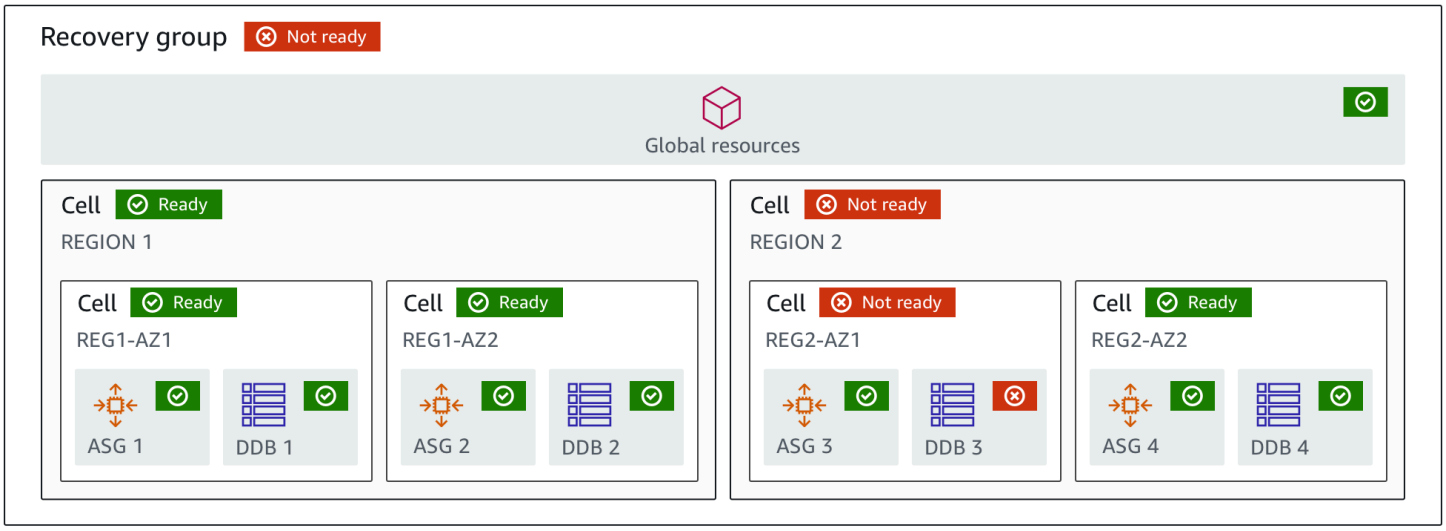
Pour obtenir des informations détaillées sur le support régional et les points de terminaison de service pour Amazon Application Recovery Controller (ARC), consultez la section Points de terminaison et quotas Amazon Application Recovery Controller (ARC) dans le manuel Amazon Web Services General Reference.

> **Note**
>
> Le contrôle du niveau de préparation dans Amazon Application Recovery Controller (ARC) 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 AWS CLI les commandes ARC régionales, par exemple, lorsque vous créez des ressources telles que des ensembles de ressources et des contrôles de disponibilité.

Composants de contrôle de préparation

> **Note**
>
> La fonctionnalité de vérification du niveau de préparation d'Amazon Application Recovery Controller (ARC) ne sera plus ouverte aux nouveaux clients à compter du 30 avril 2026. Les clients existants peuvent continuer à utiliser le service normalement. Pour plus d'informations, consultez la section Modification de la disponibilité du test de disponibilité d'Amazon Application Recovery Controller (ARC).

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 dans 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 AZs 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 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 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 l'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 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 comprenant les deux équilibreurs de charge, puis créer un contrôle de disponibilité pour l'ensemble de ressources. L'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 l'ARC effectue par rapport à un ensemble de ressources d'un ensemble de ressources. L'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 expliquant les raisons pour lesquelles l'ARC inspecte les ressources.

Contrôle de préparation

Un contrôle du niveau de préparation surveille un ensemble de ressources de votre application, tel qu'un ensemble d'instances Amazon Aurora, pour lequel 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 comprenant deux ARNs ressources, une pour chaque groupe Auto Scaling. Ensuite, pour s'assurer que chaque groupe est dimensionné de la même manière, 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 l'ARC, définissez le niveau de préparation au niveau du groupe de rétablissement ou de la ressource globale. Par exemple, un bilan de santé de la Route 53 est une ressource globale dans ARC 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

> **Note**
>
> La fonctionnalité de vérification du niveau de préparation d'Amazon Application Recovery Controller (ARC) ne sera plus ouverte aux nouveaux clients à compter du 30 avril 2026. Les clients existants peuvent continuer à utiliser le service normalement. Pour plus d'informations, consultez la section Modification de la disponibilité du test de disponibilité d'Amazon Application Recovery Controller (ARC).

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 Application Recovery Controller (ARC)

> **Note**
>
> La fonctionnalité de vérification du niveau de préparation d'Amazon Application Recovery Controller (ARC) ne sera plus ouverte aux nouveaux clients à compter du 30 avril 2026. Les clients existants peuvent continuer à utiliser le service normalement. Pour plus d'informations, consultez la section Modification de la disponibilité du test de disponibilité d'Amazon Application Recovery Controller (ARC).

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 ARC :

- Ensembles de ressources
- Contrôles de préparation

Le balisage dans ARC n'est disponible que par le biais de 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 TagResourcele Guide de référence de l'API Recovery Readiness pour Amazon Application Recovery Controller (ARC).

Tarification du contrôle de l'état de préparation dans ARC

> **Note**
>
> La fonctionnalité de vérification du niveau de préparation d'Amazon Application Recovery Controller (ARC) ne sera plus ouverte aux nouveaux clients à compter du 30 avril 2026. Les clients existants peuvent continuer à utiliser le service normalement. Pour plus d'informations, consultez la section Modification de la disponibilité du test de disponibilité d'Amazon Application Recovery Controller (ARC).

Vous payez un coût horaire pour chaque contrôle de disponibilité que vous configurez.

Pour obtenir des informations détaillées sur la tarification de l'ARC et des exemples de tarification, consultez la section Tarification de l'ARC.

Configurez un processus de restauration résilient pour votre application

Pour utiliser Amazon Application Recovery Controller (ARC) 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 fournies par 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 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 de plus amples informations, veuillez consulter Changement de zone dans ARC.

Pour en savoir plus sur la mise en route des configurations de basculement résilientes, consultezCommencer à utiliser la restauration multirégionale dans Amazon Application Recovery Controller (ARC).

Meilleures pratiques en matière de vérification de l'état de préparation dans l'ARC

Note

La fonctionnalité de vérification du niveau de préparation d'Amazon Application Recovery Controller (ARC) ne sera plus ouverte aux nouveaux clients à compter du 30 avril 2026. Les clients existants peuvent continuer à utiliser le service normalement. Pour plus d'informations, consultez la section Modification de la disponibilité du test de disponibilité d'Amazon Application Recovery Controller (ARC).

Nous recommandons de suivre les bonnes pratiques suivantes pour vérifier l'état de préparation dans Amazon Application Recovery Controller (ARC).

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 de plus amples informations, veuillez consulter Utilisation du contrôle de préparation dans ARC avec Amazon EventBridge.

Opérations de l'API de contrôle de préparation

> **Note**
>
> La fonctionnalité de vérification du niveau de préparation d'Amazon Application Recovery Controller (ARC) ne sera plus ouverte aux nouveaux clients à compter du 30 avril 2026. Les clients existants peuvent continuer à utiliser le service normalement. Pour plus d'informations, consultez la section Modification de la disponibilité du test de disponibilité d'Amazon Application Recovery Controller (ARC).

Le tableau suivant répertorie les opérations ARC que vous pouvez utiliser pour vous préparer à la restauration (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, voirExemples d'utilisation des opérations de l'API de vérification de l'état de préparation ARC avec le AWS CLI.

Action	Utilisation de la console ARC	Utilisation de l'API ARC
Création d'une cellule	Consultez Création, mise à jour et suppression de groupes de récupération dans ARC	Consultez CreateCell
Obtenez un téléphone portable	Consultez Création, mise à jour et suppression de groupes de récupération dans ARC	Consultez GetCell
Supprimer une cellule	Consultez Création, mise à jour et suppression de	Consultez DeleteCell

Action	Utilisation de la console ARC	Utilisation de l'API ARC
	groupes de récupération dans ARC	
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 ARC	Consultez ListCells
Création d'un groupe de récupération	Consultez Création, mise à jour et suppression de groupes de récupération dans ARC	Consultez CreateRecoveryGroup
Obtenez un groupe de rétablissement	Consultez Création, mise à jour et suppression de groupes de récupération dans ARC	Consultez GetRecoveryGroup
Mettre à jour un groupe de récupération	Consultez Création, mise à jour et suppression de groupes de récupération dans ARC	Consultez UpdateRecoveryGroup
Supprimer un groupe de récupération	Consultez Création, mise à jour et suppression de groupes de récupération dans ARC	Consultez DeleteRecoveryGroup
Lister les groupes de restauration	Consultez Création, mise à jour et suppression de groupes de récupération dans ARC	Consultez ListRecoveryGroups

Action	Utilisation de la console ARC	Utilisation de l'API ARC
Création d'un ensemble de ressources	Consultez Création et mise à jour des contrôles de préparation dans ARC	Consultez CreateResourceSet
Obtenir un ensemble de ressources	Consultez Création et mise à jour des contrôles de préparation dans ARC	Consultez GetResourceSet
Mettre à jour un ensemble de ressources	Consultez Création et mise à jour des contrôles de préparation dans ARC	Consultez UpdateResourceSet
Supprimer un ensemble de ressources	Consultez Création et mise à jour des contrôles de préparation dans ARC	Consultez DeleteResourceSet
Lister les ensembles de ressources	Consultez Création et mise à jour des contrôles de préparation dans ARC	Consultez ListResourceSets
Créez un contrôle de préparation	Consultez Création et mise à jour des contrôles de préparation dans ARC	Consultez CreateReadinessCheck
Faites une vérification de l'état de préparation	Consultez Création et mise à jour des contrôles de préparation dans ARC	Consultez GetReadinessCheck
Mettre à jour un test de préparation	Consultez Création et mise à jour des contrôles de préparation dans ARC	Consultez UpdateReadinessCheck
Supprimer un contrôle de préparation	Consultez Création et mise à jour des contrôles de préparation dans ARC	Consultez DeleteReadinessCheck

Action	Utilisation de la console ARC	Utilisation de l'API ARC
Lister les contrôles de préparation	Consultez Création et mise à jour des contrôles de préparation dans ARC	Consultez ListReadinessChecks
Règles de préparation de la liste	Consultez Descriptions des règles de préparation dans ARC	Consultez ListRules
Vérifier l'état d'un contrôle de préparation complet	Consultez Surveillance de l'état de préparation dans ARC	Consultez GetReadinessCheckStatus
Vérifier le statut d'une ressource	Consultez Surveillance de l'état de préparation dans ARC	Consultez GetReadinessCheckResourceStatus
Vérifier l'état d'une cellule	Consultez Surveillance de l'état de préparation dans ARC	Consultez GetCellReadinessSummary
Vérifier l'état d'un groupe de restauration	Consultez Surveillance de l'état de préparation dans ARC	Consultez GetRecoveryGroupReadinessSummary

Exemples d'utilisation des opérations de l'API de vérification de l'état de préparation ARC avec le AWS CLI

> **Note**
>
> La fonctionnalité de vérification du niveau de préparation d'Amazon Application Recovery Controller (ARC) ne sera plus ouverte aux nouveaux clients à compter du 30 avril 2026. Les clients existants peuvent continuer à utiliser le service normalement. Pour plus d'informations, consultez la section Modification de la disponibilité du test de disponibilité d'Amazon Application Recovery Controller (ARC).

Cette section présente des exemples d'applications simples utilisant les fonctionnalités de vérification du AWS Command Line Interface niveau de préparation d'Amazon Application Recovery Controller (ARC) 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 pour détecter les incohérences entre les ressources contenues 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 des cellules ARC 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 de l'ouest des États-Unis (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, consultezOpérations de l'API de contrôle de préparation.

Les cellules de l'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**
>
> ARC est un service mondial qui prend en charge plusieurs points de terminaison Régions AWS , mais vous devez spécifier la région ouest des États-Unis (Oregon) (c'est-à-dire spécifier le paramètre`--region us-west-2`) dans la plupart des commandes de la CLI 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": {}
}
```

1c. 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 ressource de premier niveau pour la préparation au rétablissement dans l'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 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 qu'elle 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 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. Créez un contrôle 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 différentes règles 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 dans ARC, utilisez `list-rules` ou consultezDescriptions des règles de préparation dans ARC. 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

> **Note**
>
> La fonctionnalité de vérification du niveau de préparation d'Amazon Application Recovery Controller (ARC) ne sera plus ouverte aux nouveaux clients à compter du 30 avril 2026. Les

clients existants peuvent continuer à utiliser le service normalement. Pour plus d'informations, consultez la section Modification de la disponibilité du test de disponibilité d'Amazon Application Recovery Controller (ARC).

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 ARC

> **Note**
>
> La fonctionnalité de vérification du niveau de préparation d'Amazon Application Recovery Controller (ARC) ne sera plus ouverte aux nouveaux clients à compter du 30 avril 2026. Les clients existants peuvent continuer à utiliser le service normalement. Pour plus d'informations, consultez la section Modification de la disponibilité du test de disponibilité d'Amazon Application Recovery Controller (ARC).

Un groupe de récupération représente votre application dans Amazon Application Recovery Controller (ARC). 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 noms des ressources Amazon (ARNs) 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 dans ARC vous aident à déterminer si votre application est prête à passer d'une réplique à une autre. Toutefois, vous devez prendre la décision d'abandonner 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 disponibilité ARC

pour les ressources de votre application. ARC peut ainsi garantir que les répliques ont la même configuration au fil du temps.

Rubriques

- Création de groupes de récupération
- Mise à jour et suppression de groupes et de cellules de récupération

Création de groupes de récupération

Les étapes décrites dans cette section expliquent comment créer un groupe de récupération sur la console ARC. Pour en savoir plus sur l'utilisation des opérations d'API de préparation à la restauration avec Amazon Application Recovery Controller (ARC), consultezOpérations de l'API de contrôle de préparation.

Pour créer un groupe de récupération

1. Ouvrez la console 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 ajoutez le nom d'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 ARC. Pour en savoir plus sur l'utilisation des opérations d'API de préparation à la restauration avec Amazon Application Recovery Controller (ARC), consultezOpérations 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 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 ARC

> **Note**
>
> La fonctionnalité de vérification du niveau de préparation d'Amazon Application Recovery Controller (ARC) ne sera plus ouverte aux nouveaux clients à compter du 30 avril 2026. Les clients existants peuvent continuer à utiliser le service normalement. Pour plus d'informations, consultez la section Modification de la disponibilité du test de disponibilité d'Amazon Application Recovery Controller (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 disponibilité sur la console ARC. Pour en savoir plus sur l'utilisation des opérations d'API de préparation à la restauration avec Amazon Application Recovery Controller (ARC), consultezOpérations 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 une vérification de l'état de préparation

1. Ouvrez la console 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 Amazon Resource Names (ARNs) 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 ARC pour chaque type de ressource, consultezTypes de ressources et formats ARN dans ARC.

7. Si vous le souhaitez, consultez les règles de préparation qui seront utilisées lorsque l'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, 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 une vérification de l'état de préparation

1. Ouvrez la console 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

ARC. Pour en savoir plus sur l'utilisation des opérations d'API de préparation à la restauration avec Amazon Application Recovery Controller (ARC), consultezOpérations de l'API de contrôle de préparation.

Pour créer un ensemble de ressources

1. Ouvrez la console Route 53 à la https://console.aws.amazon.com/route53/maison.
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 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 dans ARC

> **Note**
>
> La fonctionnalité de vérification du niveau de préparation d'Amazon Application Recovery Controller (ARC) ne sera plus ouverte aux nouveaux clients à compter du 30 avril 2026. Les clients existants peuvent continuer à utiliser le service normalement. Pour plus d'informations, consultez la section Modification de la disponibilité du test de disponibilité d'Amazon Application Recovery Controller (ARC).

Vous pouvez vérifier l'état de préparation de votre application dans Amazon Application Recovery Controller (ARC) 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 à l'aide des commandes 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 et de vous informer des modifications de l'état de préparation. Pour de plus amples informations, veuillez consulter Utilisation du contrôle de préparation dans ARC avec Amazon EventBridge.

Surveillance de l'état de préparation dans la console ARC

La procédure suivante décrit comment contrôler l'état de préparation à la restauration dans le AWS Management Console.

1. Ouvrez la console 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 ARC

> **Note**
>
> La fonctionnalité de vérification du niveau de préparation d'Amazon Application Recovery Controller (ARC) ne sera plus ouverte aux nouveaux clients à compter du 30 avril 2026. Les clients existants peuvent continuer à utiliser le service normalement. Pour plus d'informations, consultez la section Modification de la disponibilité du test de disponibilité d'Amazon Application Recovery Controller (ARC).

Si vous possédez déjà une application, Amazon Application Recovery Controller (ARC) peut évaluer l'architecture de votre application et ses 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 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, 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, 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 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 qu'ARC puisse fournir des recommandations en matière 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 dansTypes de ressources et formats ARN dans ARC.

   Facultativement, mais fortement recommandé, choisissez Ajouter un attribut facultatif et fournissez un ARN Network Load Balancer 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. 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 ARC

> **Note**
>
> La fonctionnalité de vérification du niveau de préparation d'Amazon Application Recovery Controller (ARC) ne sera plus ouverte aux nouveaux clients à compter du 30 avril 2026. Les clients existants peuvent continuer à utiliser le service normalement. Pour plus d'informations, consultez la section Modification de la disponibilité du test de disponibilité d'Amazon Application Recovery Controller (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 Application Recovery Controller (ARC), vous pouvez utiliser l'autorisation entre comptes.

L'autorisation entre comptes dans ARC fonctionne avec la fonction de vérification de l'état de préparation. Avec l'autorisation multicompte, 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 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). ARC peut vous autoriser à surveiller les deux ensembles de ressources à partir d'un seul compte, us-west-2, en utilisant l'autorisation entre comptes.

Supposons, par exemple, que vous ayez 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 ARC.

> **Note**
>
> 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 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

> **Note**
>
> La fonctionnalité de vérification du niveau de préparation d'Amazon Application Recovery Controller (ARC) ne sera plus ouverte aux nouveaux clients à compter du 30 avril 2026. Les clients existants peuvent continuer à utiliser le service normalement. Pour plus d'informations, consultez la section Modification de la disponibilité du test de disponibilité d'Amazon Application Recovery Controller (ARC).

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 (ARNs) que vous utilisez pour les ensembles de ressources.

Descriptions des règles de préparation dans ARC

> **Note**
>
> La fonctionnalité de vérification du niveau de préparation d'Amazon Application Recovery Controller (ARC) ne sera plus ouverte aux nouveaux clients à compter du 30 avril 2026. Les clients existants peuvent continuer à utiliser le service normalement. Pour plus d'informations, consultez la section Modification de la disponibilité du test de disponibilité d'Amazon Application Recovery Controller (ARC).

Cette section répertorie les descriptions des règles de préparation pour tous les types de ressources pris en charge par Amazon Application Recovery Controller (ARC). Pour consulter la liste des types de ressources pris en charge par l'ARC, consultezTypes de ressources et formats ARN dans ARC.

Vous pouvez également consulter les descriptions des règles de préparation sur la console 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 ARC
- Afficher les règles de préparation sur la console

Règles de préparation dans ARC

Cette section répertorie l'ensemble des règles de préparation pour chaque type de ressource pris en charge par ARC.

En parcourant les descriptions des règles, vous pouvez constater que la plupart d'entre elles incluent les termes Inspecte tout ou Inspecte chacune d'elles. Pour comprendre comment ces termes expliquent le fonctionnement d'une règle dans le contexte d'un contrôle de disponibilité, et pour obtenir d'autres informations sur la manière dont l'ARC définit l'état de préparation, voir Comment les règles de préparation déterminent l'état de préparation.

Règles de préparation

L'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 qu' TTLs elles sont inférieures ou égales 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 input/output opérations 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 a 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 HTTP2 (ENABLED ou DISABLED).

- 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 de certificats d'autorisation client. ARNs
- 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 utilisés 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 VPCs

- VpcCidrBlock: Inspecte tout VPCs pour s'assurer qu'ils ont tous la même valeur pour la taille du réseau de blocs CIDR.
- VpcCidrBlocksSameProtocolVersion: Inspecte tous ceux VPCs qui ont les 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 VPCs pour s'assurer qu'ils contiennent tous des blocs CIDR dans un état. `ASSOCIATED`
- VpcIpv6CidrBlocksStateInAssociationSets: Inspecte tous les ensembles d'associations de blocs CIDR pour s' VPCs assurer qu'ils contiennent tous des blocs d'adresse CIDR avec le même nombre d'adresses.
- VpcCidrBlocksInAssociationSets: Inspecte tous les ensembles d'associations de blocs CIDR VPCs pour s'assurer qu'ils ont tous la même taille.
- VpcIpv6CidrBlocksInAssociationSets: Inspecte tous les ensembles d'associations de blocs IPv6 CIDR pour s' VPCs assurer qu'ils ont la même taille.
- VpcState: Inspecte chaque VPC pour s'assurer qu'il est dans `AVAILABLE` un état.
- VpcInstanceTenancy: inspecte tous VPCs pour s'assurer qu'ils ont tous la même valeur pour`Instance Tenancy`.
- VpcIsDefault: inspecte tous VPCs 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.

Site-to-Site 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`.

Site-to-Site 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 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 ARC

> **Note**
>
> La fonctionnalité de vérification du niveau de préparation d'Amazon Application Recovery Controller (ARC) ne sera plus ouverte aux nouveaux clients à compter du 30 avril 2026. Les clients existants peuvent continuer à utiliser le service normalement. Pour plus d'informations, consultez la section Modification de la disponibilité du test de disponibilité d'Amazon Application Recovery Controller (ARC).

Lorsque vous créez un ensemble de ressources dans Amazon Application Recovery Controller (ARC), vous spécifiez le type de ressource à inclure dans l'ensemble et le nom des ressources Amazon (ARNs) pour chacune des ressources à inclure. L'ARC attend un format d'ARN spécifique pour chaque type de ressource. Cette section répertorie les types de ressources pris en charge par ARC et les formats d'ARN associés pour chacun d'entre eux.

Le format spécifique dépend de la ressource. Lorsque vous fournissez un ARN, remplacez le *italicized* texte par les informations spécifiques à votre ressource.

> **Note**
>
> Sachez que le format ARN requis par l'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 l'ARC a besoin pour prendre en charge les fonctionnalités du service 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 Amazon Resource Names (ARNs) 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'identifiant du compte dans la zone hébergée ARNs, comme indiqué ici. L'ID de compte est requis pour que l'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 Application Recovery Controller (ARC)

> **Note**
>
> La fonctionnalité de vérification du niveau de préparation d'Amazon Application Recovery Controller (ARC) ne sera plus ouverte aux nouveaux clients à compter du 30 avril 2026. Les clients existants peuvent continuer à utiliser le service normalement. Pour plus d'informations, consultez la section Modification de la disponibilité du test de disponibilité d'Amazon Application Recovery Controller (ARC).

Vous pouvez utiliser Amazon CloudWatch et Amazon EventBridge pour contrôler le niveau de préparation dans Amazon Application Recovery Controller (ARC), afin d'analyser les modèles et de résoudre les problèmes. AWS CloudTrail

> **Note**
>
> Vous devez consulter CloudWatch les métriques et les journaux d'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 ARC
- Journalisation des appels d'API de vérification de l'état de préparation AWS CloudTrail
- Utilisation du contrôle de préparation dans ARC avec Amazon EventBridge

Utilisation d'Amazon CloudWatch avec vérification de l'état de préparation dans ARC

> **Note**
>
> La fonctionnalité de vérification du niveau de préparation d'Amazon Application Recovery Controller (ARC) ne sera plus ouverte aux nouveaux clients à compter du 30 avril 2026. Les clients existants peuvent continuer à utiliser le service normalement. Pour plus d'informations, consultez la section Modification de la disponibilité du test de disponibilité d'Amazon Application Recovery Controller (ARC).

Amazon Application Recovery Controller (ARC) 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
- Statistiques pour les métriques ARC
- Afficher CloudWatch les métriques dans ARC

Métriques ARC

L'espace de noms `AWS/Route53RecoveryReadiness` inclut les métriques suivantes.

Métrique	Description
`ReadinessChecks`	Représente le nombre de contrôles de préparation traités par l'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 ARC, qui peuvent être dimensionnées 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 évaluées par l'ARC Par exemple : `AWS::CloudWatch::Alarm`

Statistiques pour les métriques ARC

CloudWatch fournit des statistiques basées sur les points de données métriques publiés par l'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 name/value paire qui identifie une métrique de manière unique.

Voici des exemples de metric/dimension combinaisons qui pourraient vous être utiles :

- Afficher le nombre de contrôles de préparation évalués par l'ARC.
- Afficher le nombre total de ressources pour un type d'ensemble de ressources donné évalué par ARC.

Afficher CloudWatch les métriques dans ARC

Vous pouvez consulter les CloudWatch métriques d'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 relatives à l'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 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

> **Note**
>
> La fonctionnalité de vérification du niveau de préparation d'Amazon Application Recovery Controller (ARC) ne sera plus ouverte aux nouveaux clients à compter du 30 avril 2026. Les clients existants peuvent continuer à utiliser le service normalement. Pour plus d'informations, consultez la section Modification de la disponibilité du test de disponibilité d'Amazon Application Recovery Controller (ARC).

est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans ARC. CloudTrail capture tous les appels d'API pour ARC sous forme d'événements. Les appels capturés incluent des appels provenant de la console ARC et des appels de code vers les opérations de l'API 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 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 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 ARC dans CloudTrail

CloudTrail est activé sur votre compte Compte AWS lorsque vous créez le compte. Lorsqu'une activité se produit dans 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 l'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 ARC sont enregistrées CloudTrail et documentées dans le Guide de référence de l'API Recovery Readiness pour Amazon Application Recovery Controller, le Guide de référence de l'API de configuration de Recovery Control pour Amazon Application Recovery Controller et le Guide de référence de l'API de contrôle du routage pour Amazon 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 Gestion des identités et des accès AWS (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 de plus amples informations, veuillez consulter l'élément userIdentity CloudTrail .

Afficher les événements 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, 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

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 ARC avec Amazon EventBridge

> **Note**
>
> La fonctionnalité de vérification du niveau de préparation d'Amazon Application Recovery Controller (ARC) ne sera plus ouverte aux nouveaux clients à compter du 30 avril 2026. Les clients existants peuvent continuer à utiliser le service normalement. Pour plus d'informations, consultez la section Modification de la disponibilité du test de disponibilité d'Amazon Application Recovery Controller (ARC).

À l'aide d'Amazon EventBridge, vous pouvez configurer des règles basées sur les événements qui surveillent vos ressources de vérification de l'état de préparation dans Amazon Application Recovery Controller (ARC), 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**
>
> L'ARC publie uniquement des EventBridge événements pour le contrôle de 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 de vérification du niveau de préparation à l'ARC suivant :

- 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 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 transmis d'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 l'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 l'ARC.

Les modèles d'événements suivants fournissent des exemples que vous pouvez utiliser EventBridge pour la fonctionnalité de vérification de l'état de préparation dans ARC.

- Sélectionnez tous les événements à partir du contrôle de préparation de l'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 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 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 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 :

JSON

```
{
    "Version":"2012-10-17",

    "Statement": [
        {
            "Action": [
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "events.amazonaws.com",
                    "delivery.logs.amazonaws.com"
                ]
            },
            "Resource": "arn:aws:logs:us-east-1:222222222222:log-group:/aws/
events/*:*",
            "Sid": "TrustEventsToStoreLogEvent"
        }
    ]
}
```

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 de préparation, voir Surveiller une ressource de vérification de l'état 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 l'état de préparation dans ARC

> **Note**
>
> La fonctionnalité de vérification du niveau de préparation d'Amazon Application Recovery Controller (ARC) ne sera plus ouverte aux nouveaux clients à compter du 30 avril 2026. Les clients existants peuvent continuer à utiliser le service normalement. Pour plus d'informations, consultez la section Modification de la disponibilité du test de disponibilité d'Amazon Application Recovery Controller (ARC).

Gestion des identités et des accès AWS (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. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Table des matières

Comment fonctionne le contrôle du niveau de préparation dans Amazon Application Recovery Controller (ARC) avec IAM

Avant d'utiliser IAM pour gérer l'accès à ARC, découvrez quelles fonctionnalités IAM peuvent être utilisées avec ARC.

Avant d'utiliser IAM pour gérer l'accès au contrôle de préparation dans Amazon Application Recovery Controller (ARC), 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 Application Recovery Controller (ARC)

Fonctionnalité 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 de politique	Oui
ACLs	Non
ABAC (étiquettes dans les politiques)	Oui
Informations d’identification temporaires	Oui
Autorisations de principal	Oui
Rôles 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 Définition d’autorisations IAM personnalisées avec des politiques gérées par le client 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. 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 ARC, consultez. Exemples de politiques basées sur l'identité dans Amazon Application Recovery Controller (ARC)

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. Par exemple, les politiques de confiance de rôle IAM et les politiques de compartiment Amazon S3 sont des politiques basées sur les ressources. 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. Intégration d’actions dans une politique afin d’accorder l’autorisation d’exécuter les opérations associées.

Pour consulter la liste des actions ARC destinées à vérifier le niveau de préparation, consultez la section Actions définies par Amazon Route 53 Recovery Readiness dans le Service Authorization Reference.

Les actions politiques dans ARC pour le contrôle de 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 voir des exemples de politiques basées sur l'identité 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 ARC

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. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

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

Pour consulter la liste des actions ARC relatives au changement de zone, consultez la section Actions définies par Amazon Route 53 Recovery Readiness.

Pour voir des exemples de politiques basées sur l'identité 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 ARC

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` indique à quel moment les instructions s'exécutent en fonction de critères définis. 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. 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 destinées à vérifier l'état de préparation, 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 voir des exemples de politiques basées sur l'identité 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 ARC

Listes de contrôle d'accès (ACLs) en cours de vérification

Supports ACLs : Non

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLs 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

Prend en charge ABAC (identifications dans les politiques) : partiellement

Le contrôle d'accès par attributs (ABAC) est une stratégie d'autorisation qui définit les autorisations en fonction des attributs nommés balise. Vous pouvez associer des balises aux entités et aux AWS ressources IAM, puis concevoir des politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de la ressource.

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 ABAC, consultez Définition d'autorisations avec l'autorisation 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'identification temporaires : oui

Les informations d'identification temporaires fournissent un accès à court terme aux AWS ressources et sont automatiquement créées lorsque vous utilisez la fédération ou que vous changez de rôle. 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 et Services AWS compatibles avec IAM dans le Guide de l'utilisateur 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 des 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 rôles de service : Non

Un rôle de service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer un rôle de service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.

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 aux services ARC, consultez. Utilisation d'un rôle lié à un service pour vérifier l'état de préparation dans 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 ARC

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier des ressources ARC. 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.

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 IAM (console) dans le Guide de l'utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par ARC, y compris le ARNs format de chaque type de ressource, consultez la section Actions, ressources et clés de condition pour Amazon Application Recovery Controller (ARC) 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 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.
- Accordez 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 d'IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utilisez 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 CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez l'Analyseur d'accès IAM pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : l'Analyseur d'accès IAM 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 politiques avec 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 la MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Sécurisation de l'accès aux API avec 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 Application Recovery Controller (ARC), 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 votre Compte AWS. Si vous créez une politique 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 politique.

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 disponibilité dans ARC. Pour en savoir plus, veuillez consulter la section Utilisation d'un rôle lié à un service pour vérifier l'état de préparation dans 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 :

JSON

```
{
    "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 ARC pour travailler avec le plan de contrôle du niveau de préparation 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 disponibilité dans ARC. Pour en savoir plus, veuillez consulter la section Utilisation d'un rôle lié à un service pour vérifier l'état de préparation dans 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 :

JSON

```
{
    "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 à un service pour vérifier l'état de préparation dans ARC

Amazon Application Recovery Controller utilise des Gestion des identités et des accès AWS rôles 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, ARC. Les rôles liés au service sont prédéfinis par l'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 d'ARC, car vous n'avez pas à ajouter manuellement les autorisations nécessaires. L'ARC définit les autorisations associées à ses rôles liés aux services et, sauf indication contraire, seul l'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 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.

ARC possède les rôles liés aux services suivants, décrits dans ce chapitre :

- ARC utilise le rôle lié au service nommé Route53 RecoveryReadinessServiceRolePolicy pour accéder aux ressources et aux configurations afin de vérifier l'état de préparation.
- ARC utilise le rôle lié au service nommé d'après les essais d'autoshift, pour surveiller les CloudWatch alarmes Amazon et les Tableau de bord Health événements clients fournis par les clients, et pour démarrer les essais.

Autorisations de rôle liées au service pour Route53 RecoveryReadinessServiceRolePolicy

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 lié au RecoveryReadinessServiceRolePolicy service Route53 pour 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 la première autorisation entre comptes dans l' AWS Management Console AWS API AWS CLI, l'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 la première autorisation entre comptes, ARC crée à nouveau le rôle lié au service pour vous.

Modification du rôle lié au RecoveryReadinessServiceRolePolicy service Route53 pour ARC

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 IAM Guide de l'utilisateur.

Suppression du rôle lié au RecoveryReadinessServiceRolePolicy service Route53 pour 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 ARC. Pour plus d'informations sur les autorisations entre comptes, consultez. Création d'autorisations entre comptes dans ARC

> **Note**
>
> Si le service 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 AWS CLI, le 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 ARC pour la vérification de l'état de préparation

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

AWS politiques gérées pour le contrôle de l'état de préparation dans ARC

Une politique AWS gérée est une politique autonome créée et administrée par AWS. AWS les politiques gérées sont conçues pour fournir des autorisations pour de nombreux cas d'utilisation courants afin que vous puissiez commencer à attribuer des autorisations aux utilisateurs, aux groupes et aux rôles.

N'oubliez pas que les politiques AWS gérées peuvent ne pas accorder d'autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont accessibles à tous les AWS clients. Nous vous recommandons de réduire encore les autorisations en définissant des politiques gérées par le client qui sont propres à vos cas d'utilisation.

Vous ne pouvez pas modifier les autorisations définies dans les politiques AWS gérées. Si les autorisations définies dans une politique AWS gérée sont AWS mises à jour, la mise à jour affecte toutes les identités principales (utilisateurs, groupes et rôles) auxquelles la politique est attachée. AWS est le plus susceptible de mettre à jour une politique AWS gérée lorsqu'une nouvelle Service AWS est lancée ou lorsque de nouvelles opérations d'API sont disponibles pour les services existants.

Pour plus d'informations, consultez Politiques gérées par AWS dans le Guide de l'utilisateur IAM.

AWS politique gérée : 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 Application Recovery Controller (ARC) d'accéder aux AWS services et aux ressources utilisés ou gérés par ARC. Pour de plus amples informations, veuillez consulter Utilisation d'un rôle lié à un service pour vérifier l'état de préparation dans ARC.

AWS politique gérée : AmazonRoute 53 RecoveryReadinessFullAccess

Vous pouvez attacher `AmazonRoute53RecoveryReadinessFullAccess` à vos entités IAM. Cette politique donne un accès complet aux actions permettant de travailler sur la préparation au rétablissement (vérification de l'état de préparation) dans l'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 au rétablissement dans 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 ARC depuis que ce service a commencé à suivre ces modifications, voirMises à jour des politiques AWS gérées pour Amazon Application Recovery Controller (ARC). Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au flux RSS sur la page d'historique du document ARC.

Quotas pour le contrôle de préparation

> **Note**
>
> La fonctionnalité de vérification du niveau de préparation d'Amazon Application Recovery Controller (ARC) ne sera plus ouverte aux nouveaux clients à compter du 30 avril 2026. Les clients existants peuvent continuer à utiliser le service normalement. Pour plus d'informations, consultez la section Modification de la disponibilité du test de disponibilité d'Amazon Application Recovery Controller (ARC).

Le contrôle du niveau de préparation dans Amazon Application Recovery Controller (ARC) 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

Changement de région dans ARC

Vous pouvez utiliser le changement de région dans ARC pour orchestrer des tâches de restauration complexes et à grande échelle pour les ressources de vos applications sur tous les AWS comptes, afin de garantir la continuité des activités et de réduire les frais opérationnels. Le changement de région fournit une solution centralisée et observable que vous pouvez exécuter manuellement ou automatiser à l'aide des déclencheurs CloudWatch d'alarme Amazon. Si un Région AWS est altéré, vous pouvez exécuter les plans que vous créez en utilisant le changement de région pour basculer ou transférer vos ressources vers une autre région. Cela garantit que votre application peut continuer à fonctionner et à fonctionner de manière saine Région AWS.

Le changement de région repose sur le concept d'un plan, que vous concevez et configurez en fonction de vos besoins de restauration spécifiques. Chaque plan inclut des flux de travail composés d'étapes. Chaque étape exécute un ou plusieurs blocs d'exécution, que le commutateur de région exécute en parallèle ou en séquence, pour terminer la restauration d'une application. Chaque

bloc d'exécution gère une tâche différente, telle que le transfert de ressources ou la gestion de la redirection du trafic pour votre application. Pour encore plus de flexibilité, vous pouvez créer des forfaits pour parents, en ajoutant des forfaits pour enfants à un plan parental global.

Le changement de région inclut les éléments suivants :

- Support active/passive et active/active configurations. Vous pouvez effectuer un basculement et un retour en arrière si vous avez une configuration active/passive multirégionale, ou passer à une configuration différente et revenir en arrière si votre application est configurée comme dans plusieurs régions. active/active
- Support multicompte pour les ressources applicatives que vous incluez dans la restauration de votre application. Vous pouvez également partager des forfaits de changement de région entre plusieurs comptes.
- Basculement ou basculement automatique, en déclenchant l'exécution du plan en fonction des alarmes Amazon. CloudWatch Vous pouvez également choisir d'exécuter un plan de changement de région manuellement.
- Des tableaux de bord complets qui vous offrent une visibilité en temps réel sur le processus de restauration.
- Un plan de données dans chaque région Région AWS, afin que vous puissiez exécuter votre plan de changement de région sans dépendre de la région que vous désactivez.

Le changement de région est entièrement géré par AWS. L'utilisation de Region Switch vous permet de bénéficier de la résilience d'une plate-forme de restauration qui se concentre sur les exigences spécifiques de votre application, au lieu de créer et de gérer des scripts, et de collecter manuellement des données sur les restaurations.

À propos du changement de région

Avec le changement de région, vous pouvez orchestrer les étapes spécifiques pour changer Région AWS celle dans laquelle s'exécute votre application multirégionale.

Le changement de région repose sur le concept d'un plan, que vous concevez et configurez en fonction de vos besoins de restauration spécifiques. Chaque plan inclut des flux de travail composés d'étapes. Chaque étape exécute un ou plusieurs blocs d'exécution, que le commutateur de région exécute en parallèle ou en séquence, pour terminer la restauration d'une application. Chaque bloc d'exécution gère une tâche différente, telle que le transfert de ressources ou la gestion de la

redirection du trafic pour votre application. Pour encore plus de flexibilité, vous pouvez créer des forfaits pour parents en ajoutant des forfaits pour enfants.

Chaque fois que vous créez ou mettez à jour un plan, Region Switch effectue une évaluation du plan afin de s'assurer qu'il n'y a aucun problème lié aux autorisations IAM, à la configuration des ressources ou à la capacité de fonctionnement. Region Switch effectue régulièrement ces évaluations et génère un avertissement en cas de problème détecté.

Le changement de région calcule également une valeur de temps de reprise réelle pour chaque exécution du plan, afin de vous aider à évaluer si le plan répond à vos objectifs. Vous pouvez consulter le temps de reprise et d'autres informations sur l'exécution des plans dans les tableaux de bord des changements de région dans le AWS Management Console. Pour de plus amples informations, veuillez consulter Tableaux de bord de changement de région.

Pour en savoir plus sur chacun de ces domaines dans Region Switch, consultez les sections suivantes.

Plans de changement de région

Un plan de changement de région est la ressource de premier niveau du changement de région. Vous devez adapter votre plan à une application multirégionale spécifique. Un plan vous permet de créer des flux de travail pour récupérer vos applications en exécutant une série de blocs d'exécution de commutateurs régionaux qui activent ou désactivent votre application et ses ressources, y compris les ressources entre comptes, dans le format Région AWS que vous spécifiez.

Un plan est composé d'un ou de plusieurs flux de travail, afin de vous permettre d'activer ou de désactiver un flux spécifique Région AWS. Vous pouvez configurer des blocs d'exécution dans un flux de travail pour qu'ils s'exécutent de manière séquentielle, ou vous pouvez spécifier que certains blocs s'exécutent en parallèle.

Pour un plan que vous configurez pour une approche active/passive multirégionale, vous créez soit un flux de travail qui peut être utilisé pour activer l'une de vos régions, soit deux flux de travail d'activation distincts, un pour chaque région. Pour un plan que vous configurez pour une approche active/active, vous créez un flux de travail pour activer vos régions et un flux de travail pour désactiver vos régions.

Régions AWS sont des emplacements géographiques dans le monde entier où se AWS regroupent des centres de données. Chaque région est conçue pour être complètement isolée des autres régions, ce qui garantit la tolérance aux pannes et la stabilité. Lorsque vous utilisez le changement de

région, vous devez prendre en compte les régions dans lesquelles votre application est déployée et les régions que vous souhaitez utiliser pour la restauration.

Le changement de région prend en charge le rétablissement entre les deux régions Régions AWS où le service est disponible. Lorsque vous configurez un plan de changement de région, vous spécifiez les régions dans lesquelles votre application est déployée et l'approche de restauration que vous souhaitez utiliser : active/passive ou active/active.

Par exemple, vous pouvez adopter une approche active/passive multirégionale avec us-east-1 comme région principale et us-west-2 comme région de secours. Pour récupérer votre application suite à un problème opérationnel affectant l'application dans us-east-1, vous pouvez exécuter votre plan de changement de région pour activer us-west-2. Cela entraînerait le passage de l'application des ressources de us-east-1 aux ressources de us-west-2.

Les plans de changement de région s'exécutent à l'aide des autorisations associées au rôle IAM que vous spécifiez lors de la création du plan.

Vous pouvez créer plusieurs plans, un pour chacune de vos applications multirégionales, puis orchestrer la restauration entre ces plans dans l'ordre requis en créant un plan parent. Un plan parent est un plan qui utilise les blocs d'exécution du plan de changement de région comme étapes. La hiérarchie des plans est limitée à deux niveaux (parent et enfant), mais vous pouvez inclure plusieurs plans pour enfants dans le même plan parent.

Flux de travail et blocs d'exécution

Après avoir créé un plan de changement de région, vous devez y ajouter un ou plusieurs flux de travail afin de définir les étapes que le plan doit effectuer pour la restauration de votre application. Pour chaque flux de travail, vous ajoutez des étapes contenant des blocs d'exécution. Chaque bloc d'exécution exécute une action de restauration spécifique, telle que l'augmentation des ressources ou la mise à jour des contrôles de routage pour rediriger le trafic. Les étapes organisent ces blocs d'exécution et déterminent s'ils s'exécutent en parallèle ou en séquence. En créant des forfaits pour parents, vous pouvez également orchestrer l'ordre dans lequel plusieurs applications sont restaurées dans la région que vous activez.

Vous organisez les blocs d'exécution en étapes au sein d'un flux de travail. Chaque étape peut contenir un ou plusieurs blocs d'exécution exécutés en parallèle, et vous pouvez organiser les étapes pour qu'elles s'exécutent de manière séquentielle dans votre flux de travail. De plus, en fonction de la ressource, vous pouvez avoir la possibilité d'exécuter un bloc d'exécution avec une exécution gracieuse (planifiée) ou irrégulière (non planifiée).

- Exécution harmonieuse : un flux de travail d'exécution planifié. Lorsque votre environnement est sain, vous pouvez utiliser le flux de travail élégant pour exécuter toutes les étapes nécessaires à une exécution ordonnée du plan.
- Exécution malhonnête : exécution imprévue. Ce mode de flux de travail peu élégant utilise uniquement les étapes et les actions nécessaires. Ce mode modifie le comportement des blocs d'exécution dans un flux de travail ou ignore des blocs d'exécution spécifiques.
- Exécution après restauration : flux de travail qui s'exécute après une restauration réussie afin de préparer les futurs événements régionaux. Les exécutions après restauration peuvent créer des répliques de lecture, exécuter une logique personnalisée via des fonctions Lambda, ajouter des portes d'approbation manuelles et intégrer des plans enfants pour une orchestration complexe. Ces exécutions nécessitent que les deux régions soient saines et qu'elles fonctionnent dans la région qui était auparavant affaiblie.

Enfin, vous pouvez également configurer des ressources entre comptes pour un bloc d'exécution. Tout d'abord, vous devez configurer les autorisations en suivant les instructions deSupport multicompte lors du changement de région. Après avoir configuré les rôles IAM requis, vous pouvez ajouter des ressources multicomptes dans les blocs d'exécution des flux de travail de votre plan. Pour ajouter des ressources entre comptes, lorsque vous ajoutez une étape, vous spécifiez un rôle IAM cible autorisé à accéder à la ressource d'un autre. Comptes AWS Vous devez également spécifier l'ID externe que vous avez fourni dans la politique de confiance pour le rôle multi-comptes. Pour plus de détails sur la création des rôles IAM requis, consultezAutorisations relatives aux ressources entre comptes.

Pour en savoir plus sur les flux de travail, voirCréation de flux de travail liés au changement de région. Pour plus de détails sur chaque type de bloc d'exécution, notamment les étapes de configuration, son fonctionnement et les éléments évalués dans le cadre de l'évaluation du plan, consultezAjouter des blocs d'exécution.

Évaluation du plan

L'évaluation du plan est un processus automatisé que Region Switch exécute lorsqu'un plan est créé ou mis à jour, puis toutes les 30 minutes, en régime permanent. Le processus d'évaluation vérifie plusieurs aspects critiques de la configuration du plan et des configurations des ressources. Les évaluations incluent la vérification des autorisations IAM, des configurations des ressources et de la capacité de fonctionnement.

Si le changement de région détecte un problème susceptible d'empêcher l'exécution réussie du plan, il génère un avertissement d'évaluation du plan, qui est mis en évidence sur la page des détails du plan de la console. Vous pouvez également consulter les avertissements d'évaluation des plans avec Amazon EventBridge, ou vous pouvez consulter les avertissements à l'aide de l'API de changement de région. Pour plus d'informations sur l'API Plan Evaluation, consultez GetPlanEvaluationStatusle Guide de référence de l'API Region Switch pour Amazon Application Recovery Controller (ARC).

Vous pouvez consulter les détails et les solutions suggérées pour les problèmes liés à l'évaluation du plan dans l'onglet Évaluation du plan sur la page des détails du plan. Nous vous recommandons également de tester la restauration des applications en exécutant votre plan de changement de région, et de ne pas vous fier uniquement à l'évaluation du plan de changement de région pour vérifier que votre plan de reprise fonctionnera comme prévu.

Rapports d'exécution automatique du plan

Le changement de région peut générer automatiquement des rapports PDF complets pour l'exécution des plans afin de vous aider à répondre aux exigences de conformité réglementaire. Ces rapports fournissent des preuves de vos tests de reprise après sinistre et des événements de reprise réels, y compris les délais d'exécution détaillés, les configurations des plans et l'état des ressources.

Lorsque vous configurez la génération automatique de rapports pour un plan, Region Switch crée un rapport PDF une fois l'exécution de chaque plan terminée et le transmet dans un compartiment Amazon S3 que vous spécifiez. Les rapports sont généralement disponibles dans les 30 minutes suivant la fin de l'exécution. Les frais de stockage S3 s'appliquent.

Chaque rapport inclut :

- Résumé avec aperçu des services et date de création du rapport
- Détails de configuration du plan tels qu'ils existaient au moment de l'exécution
- Chronologie d'exécution détaillée avec les étapes, les ressources affectées et les statuts
- Planifier les avertissements présents au début de l'exécution
- États des CloudWatch alarmes Amazon et historique des alarmes associées
- Pour les plans pour parents, les détails de configuration et d'exécution des plans pour enfants
- Glossaire des termes et des concepts

Pour activer la génération automatique de rapports, vous configurez une destination de sortie de rapport lorsque vous créez ou mettez à jour un plan. Vous devez également vous assurer que le rôle

IAM d'exécution de votre plan dispose des autorisations nécessaires pour écrire des rapports dans votre compartiment Amazon S3 et accéder aux ressources nécessaires pour générer le contenu des rapports. Pour plus d'informations sur les autorisations requises, consultez Autorisations relatives aux rapports d'exécution automatique du plan.

Vous pouvez consulter l'état de la génération des rapports et télécharger les rapports terminés à partir de la page des détails de l'exécution du plan de la console. Si la génération du rapport rencontre des erreurs, telles que des autorisations insuffisantes ou des compartiments Amazon S3 mal configurés, Region Switch fournit des informations détaillées sur les erreurs pour vous aider à résoudre le problème.

L'évaluation du plan valide en permanence la configuration de votre rapport, notamment en vérifiant que le rôle d'exécution dispose des autorisations IAM requises. Si le changement de région détecte des problèmes de configuration susceptibles d'empêcher la génération réussie du rapport, il génère des avertissements que vous pouvez consulter sur la page des détails du plan.

Alarmes régionales et temps de rétablissement réel

Le changement de région calcule une valeur de temps de reprise réelle pour chaque exécution du plan, que vous pouvez consulter après l'exécution du plan. Le temps de restauration réel est indiqué sur la page des détails de l'exécution du plan, afin que vous puissiez le comparer à l'objectif de temps de restauration que vous avez spécifié lors de la création du plan.

Le temps de restauration réel est calculé comme le temps total nécessaire à l'exécution d'un plan et le temps supplémentaire qui s'écoule avant que les CloudWatch alarmes Amazon spécifiques que vous configurez ne repassent à l'état vert.

Pour permettre de calculer un temps de restauration réel précis pour l'exécution du plan, vous devez configurer des CloudWatch alarmes Amazon régionales pour un plan de changement de région qui fournissent un signal sur l'état de santé de votre application dans chaque région. Lorsqu'un plan est exécuté, Region Switch utilise ces alarmes d'état de l'application pour déterminer à quel moment votre application est de nouveau saine. Ensuite, Region Switch calcule le temps de restauration réel en fonction du temps nécessaire à l'exécution de votre plan, ajouté au temps nécessaire pour que votre application redevienne saine, en fonction des alarmes de santé de l'application que vous configurez.

Avant d'ajouter des CloudWatch alarmes à un plan de changement de région, assurez-vous que vous avez mis en place la bonne politique IAM. Pour de plus amples informations, veuillez consulter CloudWatch alarmes pour les autorisations relatives à l'état des applications.

Régions AWS

Le changement de région est disponible dans toutes les régions commerciales Régions AWS, ainsi que dans les régions AWS GovCloud (États-Unis).

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

Nom de la région	Région	Point de terminaison	Protocole
US East (Ohio)	us-east-2	arc-region-switch.us-east-2.api.aws arc-region-switch-fips.us-east-2.api.aws	HTTPS HTTPS
USA Est (Virginie du Nord)	us-east-1	arc-region-switch.us-east-1.api.aws arc-region-switch-control-plane-fips.us-east-1.api.aws arc-region-switch-fips.us-east-1.api.aws arc-region-switch-control-plane.us-east-1.api.aws	HTTPS HTTPS HTTPS HTTPS
USA Ouest (Californie du Nord)	us-west-1	arc-region-switch.us-west-1.api.aws arc-region-switch-fips.us-west-1.api.aws	HTTPS HTTPS
USA Ouest (Oregon)	us-west-2	arc-region-switch.us-west-2.api.aws arc-region-switch-fips.us-west-2.api.aws	HTTPS HTTPS
Afrique (Le Cap)	af-south-1	arc-region-switch.af-south-1.api.aws	HTTPS

Nom de la région	Région	Point de terminaison	Protocole	
Asie-Pacifique (Hong Kong)	ap-east-1	arc-region-switch.ap-east-1.api.aws	HTTPS	
Asie-Pacifique (Hyderabad)	ap-south-2	arc-region-switch.ap-south-2.api.aws	HTTPS	
Asie-Pacifique (Jakarta)	ap-southeast-3	arc-region-switch.ap-southeast-3.api.aws	HTTPS	
Asie-Pacifique (Malaisie)	ap-southeast-5	arc-region-switch.ap-southeast-5.api.aws	HTTPS	
Asie-Pacifique (Melbourne)	ap-southeast-4	arc-region-switch.ap-southeast-4.api.aws	HTTPS	
Asia Pacific (Mumbai)	ap-south-1	arc-region-switch.ap-south-1.api.aws	HTTPS	
Asie-Pacifique (Nouvelle Zélande)	ap-southeast-6	arc-region-switch.ap-southeast-6.api.aws	HTTPS	
Asie-Pacifique (Osaka)	ap-northeast-3	arc-region-switch.ap-northeast-3.api.aws	HTTPS	

Nom de la région	Région	Point de terminaison	Protocole	
Asia Pacific (Seoul)	ap-northeast-2	arc-region-switch.ap-northeast-2.api.aws	HTTPS	
Asie-Pacifique (Singapour)	ap-southeast-1	arc-region-switch.ap-southeast-1.api.aws	HTTPS	
Asie-Pacifique (Sydney)	ap-southeast-2	arc-region-switch.ap-southeast-2.api.aws	HTTPS	
Asie-Pacifique (Taipei)	ap-east-2	arc-region-switch.ap-east-2.api.aws	HTTPS	
Asie-Pacifique (Thaïlande)	ap-southeast-7	arc-region-switch.ap-southeast-7.api.aws	HTTPS	
Asie-Pacifique (Tokyo)	ap-northeast-1	arc-region-switch.ap-northeast-1.api.aws	HTTPS	
Canada (Centre)	ca-central-1	arc-region-switch.ca-central-1.api.aws	HTTPS	
Canada-Ouest (Calgary)	ca-west-1	arc-region-switch.ca-west-1.api.aws	HTTPS	
Europe (Francfort)	eu-central-1	arc-region-switch.eu-central-1.api.aws	HTTPS	

Nom de la région	Région	Point de terminaison	Protocole	
Europe (Irlande)	eu-west-1	arc-region-switch.eu-west-1.api.aws	HTTPS	
Europe (Londres)	eu-west-2	arc-region-switch.eu-west-2.api.aws	HTTPS	
Europe (Milan)	eu-south-1	arc-region-switch.eu-south-1.api.aws	HTTPS	
Europe (Paris)	eu-west-3	arc-region-switch.eu-west-3.api.aws	HTTPS	
Europe (Espagne)	eu-south-2	arc-region-switch.eu-south-2.api.aws	HTTPS	
Europe (Stockholm)	eu-north-1	arc-region-switch.eu-north-1.api.aws	HTTPS	
Europe (Zurich)	eu-central-2	arc-region-switch.eu-central-2.api.aws	HTTPS	
Israël (Tel Aviv)	il-central-1	arc-region-switch.il-central-1.api.aws	HTTPS	
Mexique (Centre)	mx-central-1	arc-region-switch.mx-central-1.api.aws	HTTPS	
Moyen-Orient (Bahreïn)	me-south-1	arc-region-switch.me-south-1.api.aws	HTTPS	
Moyen-Orient (EAU)	me-central-1	arc-region-switch.me-central-1.api.aws	HTTPS	

Nom de la région	Région	Point de terminaison	Protocole
Amérique du Sud (São Paulo)	sa-east-1	arc-region-switch.sa-east-1.api.aws	HTTPS
AWS GovCloud (USA Est)	us-gov-east-1	arc-region-switch.us-gov-east-1.api.aws arc-region-switch-fips.us-gov-east-1.api.aws	HTTPS HTTPS
AWS GovCloud (US-Ouest)	us-gov-west-1	arc-region-switch.us-gov-west-1.api.aws arc-region-switch-control-plane-fips.us-gov-west-1.api.aws arc-region-switch-fips.us-gov-west-1.api.aws arc-region-switch-control-plane.us-gov-west-1.api.aws	HTTPS HTTPS HTTPS HTTPS

Composants du commutateur de région

Vous trouverez ci-dessous des composants et des concepts relatifs à la fonctionnalité de changement de région d'Amazon Application Recovery Controller (ARC).

Plan

Un plan est le processus de restauration fondamental de votre application. Vous créez un plan en élaborant un ou plusieurs flux de travail avec des blocs d'exécution à exécuter en séquence ou en parallèle. Ensuite, en cas de défaillance régionale, vous exécutez le plan pour terminer la restauration de votre application en déplaçant l'application pour qu'elle s'exécute dans une région saine.

Plan pour enfants

Un plan enfant est un plan autonome qui peut être exécuté à partir d'un plan parent afin de coordonner des scénarios de restauration d'applications plus complexes. Vous pouvez imbriquer les plans de changement de région à un niveau.

Flux de travail

Un plan de changement de région inclut un ou plusieurs flux de travail. Un flux de travail est composé d'étapes contenant des blocs d'exécution, que vous spécifiez pour être exécutés en parallèle ou en séquence, afin de terminer l'activation ou la désactivation d'une région dans le cadre d'un plan de reprise. Pour un plan que vous configurez pour avoir une active/passive approche, vous créez soit un flux de travail qui peut être utilisé pour activer l'une de vos régions, soit des flux de travail d'activation distincts, un pour chaque région. Pour un plan que vous configurez pour une active/active approche, vous créez un flux de travail pour activer vos régions et un flux de travail pour désactiver vos régions.

Bloc d'exécution

Vous ajoutez des étapes à vos flux de travail de plan de changement de région contenant un bloc d'exécution. Les blocs d'exécution vous permettent de spécifier la restauration de plusieurs applications ou ressources dans une région d'activation. Lorsque vous ajoutez une étape à un flux de travail, vous pouvez l'ajouter en séquence avec d'autres étapes, ou en parallèle avec une ou plusieurs autres étapes.

Configurations gracieuses et disgracieuses

Vous pouvez choisir d'exécuter des blocs d'exécution spécifiques avec une exécution gracieuse (planifiée) ou irrégulière (non planifiée). Lorsque votre environnement est sain, vous pouvez utiliser le flux de travail élégant pour exécuter toutes les étapes nécessaires à une exécution ordonnée du plan. Ce mode de flux de travail peu élégant utilise uniquement les étapes et les actions nécessaires. Lorsque vous exécutez un plan en mode peu élégant, il modifie le comportement des blocs d'exécution dans un flux de travail ou ignore des blocs d'exécution spécifiques, selon le type de bloc d'exécution.

Des types spécifiques de blocs d'exécution ont un comportement différent lorsqu'ils s'exécutent de manière inappropriée. Les détails de ces différences sont décrits dans la section qui inclut des détails sur chaque type de bloc d'exécution. Pour de plus amples informations, veuillez consulter Ajouter des blocs d'exécution.

Configurations Active/active and active/passive

Il existe deux approches principales pour créer une configuration résiliente pour une application dans plusieurs régions : active/passive active/active. Le changement de région prend en charge la restauration des applications pour ces deux approches.

Avec une active/passive configuration, vous déployez deux répliques de votre application dans deux régions différentes, le trafic client n'étant dirigé que vers une seule région.

Avec une active/active configuration, vous déployez deux répliques dans deux régions différentes, mais les deux répliques traitent du travail ou reçoivent du trafic.

Exécution du plan

Lorsqu'un plan de changement de région est exécuté, il met en œuvre la restauration d'une application lorsqu'une région est affectée en activant une région saine pour votre application et le trafic qu'elle reçoit. Avec une active/active configuration, vous exécutez également un plan pour désactiver la région altérée.

Alarmes de santé des applications

Les alarmes d'état de l'application sont des CloudWatch alarmes que vous spécifiez pour un plan afin d'indiquer l'état de santé de votre application dans chaque région. Le changement de région utilise des alarmes relatives à l'état de l'application pour déterminer le temps de restauration réel une fois que vous avez changé de région pour implémenter la restauration.

Triggers

Vous pouvez utiliser des déclencheurs dans Region Switch pour automatiser la restauration des applications. Lorsque vous créez un déclencheur, vous spécifiez une ou plusieurs CloudWatch alarmes Amazon et définissez les conditions d'alarme (telles que « rouge » ou « vert ») qui doivent déclencher l'exécution du plan. Lorsque les conditions spécifiées sont remplies, le changement de région exécute automatiquement le plan. Les déclencheurs sont distincts des alarmes relatives à l'état des applications : les déclencheurs démarrent l'exécution du plan, tandis que les alarmes relatives à l'état des applications aident Region Switch à calculer le temps de restauration réel une fois le plan terminé.

Flux de travail après restauration

Un flux de travail post-restauration est un flux de travail facultatif qui s'exécute après une restauration réussie afin de préparer les futurs événements régionaux. Ces flux de travail nécessitent que les deux régions soient saines et qu'elles s'exécutent dans la région

précédemment altérée. Les exécutions après restauration font référence à l'ID d'exécution de restauration de la dernière exécution de restauration.

Les flux de travail après restauration prennent en charge les blocs d'exécution suivants :

- RDS Create une réplique interrégionale
- Action personnalisée Lambda
- Approbation manuelle
- Plan de changement de région

Tableaux de bord

Le changement de région inclut des tableaux de bord dans lesquels vous pouvez suivre les détails de l'exécution des plans en temps réel.

Plans de données et de contrôle pour le changement de région

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 c'est le cas pour de nombreux AWS services, la fonctionnalité de commutation de région est prise en charge par un plan de contrôle et des plans de données. Bien que les deux types 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 obtenir des informations sur un plan de changement de région lors d'une panne.

Pour le changement de région, les plans de contrôle et les plans de données sont divisés comme suit :

- Le plan de contrôle de Region Switch est situé dans la région USA Est (Virginie du Nord) (us-east-1) AWS GovCloud , dans la région (US-Ouest) us-gov-west (-1) et est destiné uniquement à la gestion des services, c'est-à-dire à la création et à la mise à jour de plans, et non à la restauration, c'est-à-dire à l'exécution de plans. Les opérations de l'API du plan de contrôle de configuration du commutateur de région ne sont pas hautement disponibles.
- Le commutateur de région possède des plans de données indépendants dans chacun d'eux Région AWS. Vous devez utiliser le plan de données pour les actions de restauration, c'est-à-dire pour exécuter des plans de changement de région. Pour obtenir la liste des opérations du plan de données, reportez-vous à la sectionOpérations de l'API de changement de région. Ces opérations du plan de données de commutation de région sont hautement disponibles.

Le commutateur de région fournit une console indépendante dans chacune d'elles Région AWS, qui appelle les opérations de l'API du plan de données pour les tâches de restauration. Vous pouvez donc utiliser la console de la région que vous activez pour exécuter des plans de restauration d'applications. 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 Region Switch, consultezMeilleures pratiques pour le changement de région dans 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.

Marquage pour le changement de région ARC ;

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 la ressource suivante dans le changement de région dans ARC :

- Plans

Le balisage dans ARC est uniquement disponible via l'API, par exemple en utilisant le AWS CLI.

Voici des exemples de balisage dans le changement de région à l'aide du AWS CLI.

```
aws arc-region-switch --region us-east-1 create-plan --plan-name example-plan --tags Region=IAD,Stage=Prod
```

Pour plus d'informations, consultez TagResourcele Guide de référence de l'API Region Switch pour Amazon Application Recovery Controller (ARC).

Tarification du changement de région dans ARC

Vous payez un coût mensuel fixe par plan de changement de région que vous configurez.

Pour obtenir des informations détaillées sur la tarification de l'ARC et des exemples de tarification, consultez la section Tarification de l'ARC.

Meilleures pratiques pour le changement de région dans ARC

Nous recommandons les meilleures pratiques suivantes pour la préparation à la restauration et au basculement avec le changement de région dans Amazon Application Recovery Controller (ARC).

Rubriques

- Conservez les informations d' AWS identification spécialement conçues et durables, sécurisées et toujours accessibles
- Choisissez des valeurs TTL inférieures pour les enregistrements DNS impliqués dans le basculement
- Réservez la capacité requise pour les applications critiques
- Utilisez les opérations extrêmement fiables de l'API du plan de données pour répertorier et obtenir des informations sur les plans de changement de région
- Tester le basculement avec ARC

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 pour les 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.

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.

Réservez la capacité requise pour les applications critiques

Le changement de région inclut des types de blocs d'exécution qui aident à dimensionner les ressources de calcul dans le cadre de la restauration. Si vous utilisez ces blocs d'exécution dans un plan, Region Switch ne garantit pas que la capacité de calcul souhaitée sera atteinte. Si vous avez une application critique et que vous devez garantir l'accès à la capacité, nous vous recommandons de réserver la capacité.

Il existe des stratégies que vous pouvez suivre pour réserver de la capacité de calcul dans une région secondaire tout en limitant les coûts. Pour en savoir plus, voir Pilot light avec capacité réservée : comment optimiser les coûts de reprise après sinistre à l'aide des réservations de capacité à la demande.

Utilisez les opérations extrêmement fiables de l'API du plan de données pour répertorier et obtenir des informations sur les plans de changement de région

Utilisez les opérations de l'API du plan de données pour utiliser et exécuter votre plan de changement de région lors d'un événement. Pour obtenir la liste des opérations du plan de données du changement de région, voirOpérations de l'API de changement de région.

La console de changement de région de chaque région utilise des opérations de plan de données pour exécuter les plans de changement de région. Vous pouvez également appeler les opérations de l'API du plan de données en utilisant AWS CLI ou en exécutant le code que vous écrivez à l'aide de l'un des AWS SDKs. ARC offre une fiabilité extrême grâce à l'API intégrée au plan de données.

Testez la restauration des applications avec ARC

Testez régulièrement la restauration des applications avec le commutateur de région ARC, pour activer une pile d'applications secondaire dans une autre Région AWS, ou pour passer d'une configuration active-active en exécutant un plan de changement de région pour désactiver l'une des régions.

Il est important de vous assurer que les plans de changement de région que vous avez créés correspondent aux bonnes ressources de votre pile et que tout fonctionne comme vous le souhaitez. Vous devez le tester après avoir configuré le changement de région pour votre environnement, et continuer à le tester régulièrement afin de valider le bon fonctionnement de vos processus de restauration. Effectuez ces tests régulièrement, avant de rencontrer une situation de panne, afin d'éviter les temps d'arrêt pour vos utilisateurs.

Basculement du DNS via le commutateur de région ARC et restauration accélérée via Route 53

La restauration accélérée fournit un RTO cible de 60 minutes à APIs utiliser pour mettre à jour les enregistrements de vos zones hébergées publiques activées pour cette fonctionnalité. Si vous devez garder le contrôle de votre RTO et ne pas attendre AWS que le rétablissement soit terminé, vous devez APIs utiliser le contrôle de routage ARC ou le bloc d'exécution du contrôle de santé Route 53 du commutateur de région ARC.

Tutoriel : Création d'un plan de changement de active/passive région

Ce didacticiel vous explique comment créer un plan de changement de active/passive région pour une application exécutée dans us-east-1 et comment récupérer dans us-west-2. L'exemple inclut les instances Amazon EC2 pour le calcul, la base de données mondiale Amazon Aurora pour le stockage et Amazon Route 53 pour le DNS.

Dans ce didacticiel, vous allez effectuer les étapes suivantes :

- Création d'un plan de changement de région
- Créez les flux de travail et les blocs d'exécution du plan
- Création d'un bloc d'exécution de groupe EC2 Auto Scaling

- Créez deux blocs d'exécution d'approbation manuelle
- Créez deux blocs d'exécution Lambda d'actions personnalisés
- Création d'un bloc d'exécution de la base de données globale Amazon Aurora
- Création d'un bloc de contrôle de routage ARC
- Exécuter le plan de changement de région

Conditions préalables

Avant de commencer ce didacticiel, vérifiez que les conditions requises suivantes sont réunies dans les deux régions :

- Rôles IAM dotés des autorisations appropriées
- Groupes EC2 Auto Scaling
- Fonctions Lambda pour la page de maintenance et les clôtures
- Aurora Global Database
- Contrôles de routage ARC

Étape 1 : Création du plan de changement de région

1. Dans la console de changement de région, choisissez Créer un plan de changement de région.
2. Fournissez les informations suivantes :
    - Région principale : Choisissez us-east-1
    - Région de veille : choisissez us-west-2
    - Objectif de temps de rétablissement souhaité (RTO) (facultatif)
    - Rôle IAM : entrez le rôle IAM d'exécution du plan. Ce rôle IAM permet de passer d'une région à un AWS service d'appel pendant l'exécution.
3. Choisissez Créer.

(Facultatif) Ajoutez des ressources provenant de différents AWS comptes à votre plan de changement de région :

1. Créez le rôle multi-comptes :
    - Dans le compte hébergeant la ressource, créez un rôle IAM.

- Ajoutez des autorisations pour les ressources spécifiques auxquelles le plan aura accès.
- Ajoutez une politique de confiance qui permet au rôle d'exécution d'assumer le nouveau rôle.
- Entrez et notez un identifiant externe que vous utiliserez comme secret partagé.

2. Configurez la ressource dans votre plan :
   - Lorsque vous ajoutez la ressource à votre plan, spécifiez deux champs supplémentaires :
     - crossAccountRole: l'ARN du rôle que vous avez créé à l'étape 1
     - ExternalID : ID externe que vous avez saisi à l'étape 1

Exemple de configuration pour un bloc d'exécution EC2 Auto Scaling accédant aux ressources du compte 987654321 :

```
{
  "executionBlock": "EC2AutoScaling",
  "name": "ASG",
  "crossAccountRole": "arn:aws:iam::987654321:role/RegionSwitchCrossAccountRole",
  "externalId": "unique-external-id-123",
  "autoScalingGroupArn": "arn:aws:autoscaling:us-
west-2:987654321:autoScalingGroup:*:autoScalingGroupName/CrossAccountASG"
}
```

Autorisations requises :

- Le rôle d'exécution doit disposer de AssumeRole l'autorisation sts : pour le rôle multi-comptes.
- Le rôle multi-comptes doit disposer d'autorisations uniquement pour les ressources spécifiques auxquelles il accède.
- La politique de confiance du rôle multicompte doit inclure :
  - Le compte du rôle d'exécution en tant qu'entité de confiance.
  - La condition d'identification externe.
- Pour plus d'informations sur la configuration d'un rôle multicompte, consultezAutorisations relatives aux ressources entre comptes.

Avant d'exécuter le plan, Region Switch vérifiera les points suivants :

- Le rôle d'exécution peut assumer le rôle entre comptes.

- Le rôle multi-comptes dispose des autorisations requises.
- L'ID externe correspond à la politique de confiance.

Étape 2 : Création des flux de travail et des blocs d'exécution du plan

1. Sur la page des détails du plan de changement de région, choisissez Créer des flux de travail.
2. Sélectionnez Créer le même flux de travail d'activation pour toutes les régions.
3. Entrez une description du flux de travail d'activation par région (facultatif). Cela sera utilisé pour identifier facilement le flux de travail lors de l'exécution du plan.
4. Choisissez Save and continue (Enregistrer et continuer).

Ajouter le bloc d'exécution EC2 Auto Scaling

Pour plus d'informations sur ce bloc d'exécution, consultezBloc d'exécution du groupe Amazon EC2 Auto Scaling.

1. Choisissez Ajouter une étape, puis sélectionnez Exécuter en séquence.
2. Sélectionnez le bloc d'exécution EC2 Auto Scaling, puis choisissez Ajouter et modifier. Ce bloc vous permettra de commencer à augmenter la capacité de la région passive.
3. Dans le panneau de droite, configurez le bloc :
   - Nom de l'étape : Entrez « Scale »
   - Description de l'étape (facultatif)
   - ARN du groupe Auto Scaling pour us-east-1 : l'ARN de votre ASG dans us-east-1
   - ARN du groupe Auto Scaling pour us-west-2 : l'ARN de votre ASG dans us-west-2
   - Pourcentage correspondant à la capacité de la région source : entrez 100
   - Approche de suivi des capacités : laisser comme « le plus récent »
   - Délai d'expiration (facultatif)

   Pour plus d'informations sur les autorisations IAM requises pour ce bloc d'exécution, consultezExemple de politique d'exécution par blocs d'EC2 Auto Scaling.
4. Choisissez Enregistrer l'étape.

Ajouter un bloc d'exécution des approbations manuelles

Pour plus d'informations sur ce bloc d'exécution, consultezBloc d'exécution de l'approbation manuelle.

1. Choisissez Ajouter une étape.
2. Sélectionnez le bloc d'exécution de l'approbation manuelle et ajoutez-le à la fenêtre de conception. Ce bloc permet une vérification humaine avant de continuer.
3. Dans le panneau de droite, configurez le bloc :

   - Nom de l'étape : Entrez « Approbation manuelle avant la configuration »
   - Description de l'étape (facultatif)
   - Rôle d'approbation IAM : rôle qu'un utilisateur doit assumer pour approuver l'exécution
   - Délai d'expiration (facultatif). Une fois le délai expiré, l'exécution est interrompue et vous pouvez choisir de réessayer, d'ignorer ou d'annuler.

   Pour plus d'informations sur les autorisations IAM requises pour ce bloc d'exécution, consultezExemple de politique d'exécution des approbations manuelles.
4. Choisissez Enregistrer l'étape.

Ajouter un bloc d'exécution Lambda d'action personnalisé pour la page de maintenance

Pour plus d'informations sur ce bloc d'exécution, consultezAction personnalisée : bloc d'exécution Lambda.

1. Choisissez Ajouter une étape.
2. Sélectionnez le bloc d'exécution Lambda de l'action personnalisée, puis choisissez Ajouter et modifier. Ce bloc publie une page de maintenance dans la région en cours d'activation.
3. Dans le panneau de droite, configurez le bloc :

   - Nom de l'étape : Entrez « Afficher la page de maintenance »
   - Description de l'étape (facultatif)
   - ARN Lambda pour activer us-east-1 : ARN de la fonction Lambda de la page de maintenance déployée dans us-east-1
   - ARN Lambda pour activer us-west-2 : ARN de la fonction Lambda de la page de maintenance déployée dans us-west-2

- Région pour exécuter la fonction Lambda : choisissez Exécuter pour activer la région
- Délai d'expiration (facultatif)
- Intervalle entre les tentatives (facultatif)

Pour plus d'informations sur les autorisations IAM requises pour ce bloc d'exécution, consultezExemple de politique de bloc d'exécution Lambda pour les actions personnalisées.

4. Choisissez Enregistrer l'étape.

Ajouter un bloc d'exécution de la base de données globale Aurora

Pour plus d'informations sur ce bloc d'exécution, consultezBloc d'exécution de la base de données globale Amazon Aurora.

1. Choisissez Ajouter une étape.
2. Sélectionnez le bloc d'exécution de la base de données globale Aurora, puis choisissez Ajouter et modifier. Ce bloc déclenche une commutation globale de la base de données Aurora (aucune perte de données). Pour plus d'informations, consultez la section Utilisation du basculement ou du basculement pour la base de données globale Aurora dans le guide de l'utilisateur d'Aurora.
3. Dans le panneau de droite, configurez le bloc :
   - Nom de l'étape : Enter Aurora switchover
   - Description de l'étape (facultatif)
   - Identifiant de base de données global Aurora : nom du cluster Aurora
   - ARN du cluster utilisé pour activer us-east-1 : l'ARN du cluster Aurora dans us-east-1
   - ARN du cluster utilisé pour activer us-west-2 : l'ARN du cluster Aurora dans us-west-2
   - Sélectionnez l'option pour la base de données Aurora : Choisissez Switchover
   - Délai d'expiration (facultatif)

   Pour plus d'informations sur les autorisations IAM requises pour ce bloc d'exécution, consultezExemple de politique d'exécution de la base de données globale Aurora.
4. Choisissez Enregistrer l'étape.

Ajouter un bloc d'exécution du contrôle de routage ARC

Pour plus d'informations sur ce bloc d'exécution, consultezBloc d'exécution du contrôle de routage ARC.

1. Choisissez Ajouter une étape.
2. Sélectionnez le bloc d'exécution du contrôle de routage ARC, puis choisissez Ajouter et modifier. Ce bloc effectue un basculement DNS pour transférer le trafic vers la région passive.
3. Dans le panneau de droite, configurez le bloc :
   - Nom de l'étape : Enter Toggle DNS
   - Description de l'étape (facultatif)
   - Contrôles de routage utilisés pour activer us-east-1 : choisissez Ajouter des contrôles de routage
   - Délai d'expiration : entrez une valeur de délai d'expiration.
4. Choisissez Ajouter un contrôle de routage :
   - ARN du contrôle de routage : ARN du contrôle de routage qui contrôle us-east-1
   - État du contrôle de routage : Choisissez Activé
5. Choisissez à nouveau Ajouter un contrôle de routage :
   - ARN du contrôle de routage : ARN du contrôle de routage qui contrôle us-west-2
   - État du contrôle du routage : choisissez Off
6. Choisissez Enregistrer.
7. Contrôles de routage utilisés pour activer us-west-2 : choisissez Ajouter des contrôles de routage
8. Choisissez Ajouter un contrôle de routage :
   - ARN du contrôle de routage : ARN du contrôle de routage qui contrôle us-west-2
   - État du contrôle de routage : Choisissez Activé
9. Choisissez à nouveau Ajouter un contrôle de routage :
   - ARN du contrôle de routage : ARN du contrôle de routage qui contrôle us-east-1
   - État du contrôle du routage : choisissez Off
10. Choisissez Enregistrer.
11. Choisissez Enregistrer l'étape.

Pour plus d'informations sur les autorisations IAM requises pour ce bloc d'exécution, consultezExemple de politique de bloc d'exécution des contrôles de routage ARC.

12. Choisissez Enregistrer.

Étape 3 : Exécuter le plan

1. Sur la page des détails du plan de changement de région, en haut à droite, choisissez Execute.
2. Entrez les détails de l'exécution :
   - Sélectionnez la région à activer.
   - Sélectionnez le mode d'exécution du plan.
   - (Facultatif) Consultez les étapes d'exécution.
   - Reconnaissez l'exécution du plan.
3. Sélectionnez Démarrer.
4. Vous pouvez consulter les étapes détaillées au fur et à mesure de l'exécution du plan sur la page des détails d'exécution. Vous pouvez voir chaque étape de l'exécution du plan, y compris l'heure de début, l'heure de fin, l'ARN de la ressource et les messages du journal.

Une fois la région altérée rétablie, vous pouvez exécuter à nouveau le plan (en modifiant les paramètres que vous avez fournis) pour activer la région d'origine, afin de rétablir les opérations de votre application sur la région principale d'origine.

Tutoriel : Configuration de l'autogénération du rapport d'exécution du plan

Ce didacticiel vous explique comment configurer l'autogénération des rapports d'exécution du plan pour un plan de changement de région. Les rapports fournissent une documentation PDF complète sur l'exécution des plans à des fins de conformité.

Dans ce didacticiel, vous allez effectuer les étapes suivantes :

- Création d'un compartiment Amazon S3 pour le stockage des rapports
- Activer la génération automatique des rapports sur un plan de changement de région
- Exécutez le plan et téléchargez le rapport

Conditions préalables

Avant de commencer ce didacticiel, vérifiez que vous disposez des éléments suivants :

- Un plan de changement de région existant avec des flux de travail configurés
- Autorisations pour créer des compartiments Amazon S3
- Le rôle IAM d'exécution de votre plan est configuré avec les autorisations requises. Pour de plus amples informations, veuillez consulter Autorisations relatives aux rapports d'exécution automatique du plan.

Étape 1 : créer un compartiment Amazon S3 pour les rapports

1. Ouvrez la console Amazon S3 à l'adressehttps://console.aws.amazon.com/s3/.
2. Choisissez Créer un compartiment.
3. Fournissez les informations suivantes :
   - Nom du compartiment : entrez un nom unique, tel que `my-region-switch-reports`
   - Paramètres de blocage de l'accès public : bloquez tous les accès publics (recommandé)
   - Versionnage des compartiments : activer la gestion des versions (facultatif mais recommandé)
   - Chiffrement par défaut : sélectionnez le cryptage. Si vous utilisez SSM-KMS, le planExecutionRole kms: chiffrement et les kms: GenerateDataKey autorisations sont nécessaires sur la clé CMK par défaut du compartiment s3
4. Choisissez Créer un compartiment.
5. Notez le nom du compartiment à utiliser à l'étape suivante.

Étape 2 : Activez la génération automatique des rapports sur votre plan

1. Ouvrez la console de changement de région à l'adressehttps://console.aws.amazon.com/route53recovery/regionswitch/home.
2. Sélectionnez le plan pour lequel vous souhaitez configurer les rapports.
3. Choisissez Dans la barre de navigation, accédez à Actions, puis sélectionnez Modifier les détails du plan.
4. Dans la section Paramètres du rapport, fournissez les informations suivantes :
   - Sélectionnez Activer la génération automatique des rapports

- URI Amazon S3 : sélectionnez ou entrez l'URI du compartiment S3 que vous avez créé à l'étape 1
- ID du compte propriétaire du bucket : entrez l'ID de compte du propriétaire du bucket

5. Choisissez Enregistrer.
6. Attendez que l'évaluation du plan soit terminée. En cas de problème de configuration, des avertissements apparaîtront sur la page des détails du plan.

Étape 3 : Exécuter le plan et télécharger le rapport

1. Sur la page des détails du plan, choisissez Execute.
2. Terminez l'exécution du plan comme d'habitude, en sélectionnant la région à activer et le mode d'exécution.
3. Une fois l'exécution du plan terminée, accédez à la page des détails de l'exécution.
4. Dans la section Rapport d'exécution du plan, surveillez l'état de génération du rapport. La génération du rapport s'achève généralement dans les 30 minutes suivant la fin de l'exécution.
5. Lorsque le statut du rapport indique Terminé, choisissez Télécharger le rapport d'exécution du plan pour télécharger le PDF.
6. Vous pouvez également accéder à votre compartiment Amazon S3 pour accéder directement au rapport. Les rapports sont stockés selon le modèle de dénomination suivant : `ExecutionReport-${planVersion.ownerAccountId}-${planName}-${execution.regionTo}-${event.executionId}-${dateStr}.pdf`

Le rapport généré inclut :

- Résumé avec aperçu des services et date de création du rapport
- Détails de configuration du plan tels qu'ils existaient au moment de l'exécution
- Chronologie d'exécution détaillée avec les étapes, les ressources affectées et les statuts
- Planifier les avertissements présents au début de l'exécution
- États des CloudWatch alarmes Amazon et historique des alarmes associées
- Pour les plans pour parents, les détails de configuration et d'exécution des plans pour enfants
- Glossaire des termes et des concepts

Résolution des problèmes

Si la génération du rapport échoue, vérifiez les points suivants :

- Erreurs d'autorisation : vérifiez que le rôle d'exécution dispose des autorisations IAM correctes. Pour de plus amples informations, veuillez consulter Autorisations relatives aux rapports d'exécution automatique du plan. Consultez les avertissements relatifs à l'évaluation du plan pour détecter des problèmes d'autorisation spécifiques.
- Accès au compartiment Amazon S3 : assurez-vous que le compartiment Amazon S3 existe et qu'il est accessible depuis la région où le plan est configuré. Vérifiez que les politiques relatives aux compartiments ne bloquent pas l'accès depuis le rôle d'exécution.
- Chiffrement des compartiments : si vous utilisez des clés KMS gérées par le client pour le chiffrement des compartiments, assurez-vous que le rôle d'exécution est autorisé à utiliser la clé KMS.

Pour obtenir de l'aide supplémentaire, consultez les messages d'erreur détaillés sur la page des détails d'exécution ou contactez le AWS Support.

Tutoriel : Exécution d'un flux de travail RDS après restauration

Ce didacticiel vous explique comment exécuter un flux de travail après restauration après un basculement RDS réussi. Cette exécution après restauration rétablit la redondance en rétablissant la réplication entre régions pour la base de données RDS, garantissant ainsi que votre base de données RDS est prête pour les futurs événements régionaux.

Dans ce didacticiel, vous allez effectuer les étapes suivantes :

- Vérifiez les conditions préalables à l'exécution après la restauration
- Créez un flux de travail après la restauration avec le bloc d'exécution RDS Create Cross-Region Replica
- Exécuter le flux de travail après la restauration

Conditions préalables

Avant de commencer ce didacticiel, vérifiez que vous disposez des éléments suivants :

- Un active/passive plan de changement de région avec un flux de travail d'activation incluant un bloc d'exécution RDS Promote Read Replica

- Une exécution d'activation réussie qui a favorisé la lecture d'une réplique dans l'autre région
- Les deux régions sont saines et accessibles
- L'ID d'exécution de la dernière exécution de restauration

Étape 1 : créer un flux de travail après la restauration

1. Dans la console de changement de région, choisissez le plan, choisissez Modifier les flux de travail, sélectionnez Config, cochez la case Inclure le flux de travail post-restauration dans le plan et enregistrez.
2. Sur la page Modifier les flux de travail, sélectionnez le menu déroulant Sélectionnez un flux de travail pour ajouter des étapes et choisissez Post-restauration.
3. Choisissez Ajouter une étape.
4. Sélectionnez le bloc d'exécution Amazon RDS pour créer une réplique interrégionale.
5. Dans le panneau de droite, configurez le bloc :

   - Nom de l'étape : Entrez « Créer une réplique de lecture interrégionale »
   - Description de l'étape (facultatif)
   - ARN de l'instance de base de données RDS pour la région principale : l'ARN de la base de données de la région principale doit être identique à l'étape de promotion et de lecture de la réplique.
   - ARN de l'instance de base de données RDS pour la région secondaire : l'ARN de la base de données promue en secondaire doit être le même que celui de l'étape de promotion et de lecture de la réplique.
   - Délai d'expiration (facultatif) : entrez une valeur de délai, telle que 90 minutes

   Pour plus d'informations sur les autorisations IAM requises pour ce bloc d'exécution, consultezExemple de politique relative aux blocs d'exécution Amazon RDS.
6. Choisissez Enregistrer l'étape.
7. Choisissez Enregistrer le flux de travail.

Étape 2 : Exécuter le flux de travail après la restauration

1. Sur la page des détails du plan de changement de région, en haut à droite, choisissez Execute post-recovery.

2. Entrez les détails de l'exécution :
   - ID d'exécution de la restauration : entrez l'ID d'exécution de la dernière exécution de restauration. Ce champ est utilisé pour identifier la région actuellement active.
   - Région dans laquelle exécuter : sélectionnez la région inactive qui ne reçoit aucun trafic d'application. Il s'agit de la région dans laquelle une réplique en lecture sera créée.
3. Passez en revue les étapes d'exécution et confirmez l'exécution.
4. Choisissez Démarrer une exécution.
5. Surveillez la progression de l'exécution sur la page des détails de l'exécution. Le bloc d'exécution RDS Create Cross-Region Replica renommera votre ancienne instance principale et créera une nouvelle réplique en lecture dans la région précédemment altérée.

Une fois l'exécution post-restauration terminée avec succès, la réplication entre régions de votre application sera rétablie et vous serez prêt pour les futurs événements régionaux. Vous pouvez vérifier si la nouvelle réplique de lecture a été créée en vérifiant la console RDS dans la région cible. L'ancien serveur principal sera renommé et étiqueté avec renamedByRegionSwitch.

> **Important**
>
> Le changement de région vérifie que l'ID d'exécution de la restauration correspond à la dernière exécution connue du plan. Si l'ID d'exécution n'est pas valide ou s'il ne s'agit pas de l'ID de la dernière exécution de restauration connue, l'exécution post-restauration ne sera pas exécutée.

Opérations de l'API de changement de région

Le tableau suivant répertorie les opérations ARC que vous pouvez utiliser pour le changement de région, avec des liens vers la documentation pertinente.

Action	Utilisation de la console ARC	Utilisation de l'API ARC	API de plan de données
Approuver ou refuser une étape d'exécution du plan	Consultez Bloc d'exécution de	Consultez ApprovePlanExecutionStep	Oui

Action	Utilisation de la console ARC	Utilisation de l'API ARC	API de plan de données
	l'approbation manuelle		
Annuler l'exécution d'un plan	Consultez Création d'un plan de changement de région	Consultez CancelPlanExecution	Oui
Créez un plan	Consultez Création d'un plan de changement de région	Consultez CreatePlan	Non
Supprimer un plan	Consultez Utilisation du changement de région	Consultez DeletePlan	Non
Obtenez un plan	Consultez Utilisation du changement de région	Consultez GetPlan	Non
Obtenir le statut de l'évaluation du plan	Consultez Évaluation du plan	Consultez GetPlanEvaluationStatus	Oui
Obtenez l'exécution d'un plan	Consultez Tableaux de bord de changement de région	Consultez GetPlanExecution	Oui
Obtenez un plan dans la région	Consultez Utilisation du changement de région	Consultez GetPlanInRegion	Oui
Lister les événements d'exécution du plan	Consultez Exécuter un plan de changement de région pour récupérer une application	Consultez ListPlanExecutionEvents	Oui

Action	Utilisation de la console ARC	Utilisation de l'API ARC	API de plan de données
Lister les exécutions du plan	Consultez Exécuter un plan de changement de région pour récupérer une application	Consultez ListPlanExecutions	Oui
Lister les plans	Consultez Utilisation du changement de région	Consultez ListPlans	Non
Lister les plans de la région	Consultez Utilisation du changement de région	Consultez ListPlansInRegion	Oui
Répertorier les bilans de santé de la Route 53 pour un plan	Consultez Bloc d'exécution du contrôle de santé Amazon Route 53	Voir ListRoute53HealthChecksForPlan	Non
Répertorier les bilans de santé de la Route 53 pour un plan dans la région	Consultez Bloc d'exécution du contrôle de santé Amazon Route 53	Voir ListRoute53HealthChecksForPlanInRegion	Oui
Répertorie les balises d'une ressource.	Consultez Marquage pour le changement de région ARC ;	Consultez ListTagsForResource	Non
Commencer l'exécution d'un plan	Consultez Exécuter un plan de changement de région pour récupérer une application	Consultez StartPlanExecution	Oui

Action	Utilisation de la console ARC	Utilisation de l'API ARC	API de plan de données
Étiqueter une ressource	Consultez Création d'un plan de changement de région	Consultez TagResource	Non
Supprimer les balises d'une ressource	Consultez Marquage pour le changement de région ARC ;	Consultez UntagResource	Non
Mettre à jour un plan	Consultez Création d'un plan de changement de région	Consultez UpdatePlan	Non
Mettre à jour l'exécution d'un plan	Consultez Création d'un plan de changement de région	Consultez UpdatePlanExecution	Oui
Mettre à jour une étape d'exécution du plan	Consultez Création d'un plan de changement de région	Consultez UpdatePlanExecutionStep	Oui

Utilisation du changement de région

Cette section fournit des step-by-step instructions pour travailler avec les plans de changement de région, que vous pouvez utiliser pour récupérer des applications multirégionales. Le changement de région vous permet de créer des plans pour les deux approches active/passive et pour les approches active/active de reprise.

Pour créer un plan de restauration pour votre application, procédez comme suit :

1. Créez un plan de changement de région. Un plan est une structure dotée de certains attributs, tels que la spécificité dans Régions AWS laquelle votre application s'exécute. Chaque plan inclut un ou plusieurs flux de travail.

   Vous pouvez éventuellement créer plusieurs plans et intégrer ces plans enfants dans un plan de reprise global.

2. Créez un flux de travail pour le plan. Vous ne pouvez pas exécuter un plan sans créer au préalable un flux de travail.
3. Dans le flux de travail, ajoutez une ou plusieurs étapes qui constituent chacune un bloc d'exécution.

   Par exemple, vous pouvez ajouter une étape pour étendre les groupes EC2 Auto Scaling dans une région de destination.
4. Une fois que vous avez ajouté des étapes à votre flux de travail, des étapes supplémentaires peuvent être nécessaires, telles que la configuration des contrôles de santé dans Amazon Route 53. Chaque section du bloc d'exécution inclut les informations de configuration dont vous avez besoin. Pour de plus amples informations, veuillez consulter Ajouter des blocs d'exécution.
5. Pour récupérer votre application lorsqu'elle s'exécute dans un environnement Région AWS défaillant, exécutez le plan.

   Vous pouvez suivre la progression de l'exécution d'un plan en consultant les informations dans le tableau de bord global ou dans un tableau de bord régional.

Les sections suivantes fournissent des informations détaillées et des étapes pour créer un plan et des flux de travail, et pour ajouter des étapes de blocage d'exécution dans vos flux de travail.

Table des matières

Les procédures décrites dans cette section montrent comment utiliser les plans, les flux de travail, les blocs d'exécution et les déclencheurs à l'aide du AWS Management Console. Pour utiliser plutôt les opérations de l'API de changement de région, voirOpérations de l'API de changement de région.

Création d'un plan de changement de région

Vous pouvez créer deux types de plans différents dans Region Switch : un active/active plan ou un active/passive plan. Lorsque vous créez un plan, spécifiez le type qui s'applique à la manière dont vous souhaitez gérer le basculement.

- Une approche active/passive déploie deux répliques d'applications dans deux régions, le trafic étant acheminé uniquement vers la région active. Vous pouvez activer la réplique dans la région passive en exécutant le plan de changement de région.
- Une approche active/active déploie deux répliques d'applications dans deux régions, et les deux répliques traitent du travail ou reçoivent du trafic.

Pour créer un plan de changement de région

1. Dans la console de changement de région, choisissez Créer un plan de changement de région avec active/passive approche.
2. Fournissez les informations suivantes :
   - Nom du plan - Entrez un nom descriptif pour votre plan.
   - Approche multirégionale : sélectionnez Actif/passif ou actif/actif. Cette approche signifie que deux répliques d'applications sont déployées dans deux régions, le trafic étant acheminé uniquement vers la région active. Vous pouvez activer la réplique dans la région passive en exécutant le plan de changement de région.
     - Choisissez actif/passif si vous avez déployé deux répliques d'applications dans deux régions, le trafic étant acheminé uniquement vers la région active. Vous pouvez ensuite activer la réplique dans la région passive en exécutant le plan de changement de région qui spécifie actif/passif.
     - Choisissez Actif/actif si vous avez déployé deux répliques d'applications dans deux régions et que les deux répliques traitent du travail ou reçoivent du trafic.
   - Régions ou régions principales et de secours : sélectionnez les régions principales et de secours pour votre application. Pour un active/active déploiement, sélectionnez les régions dans lesquelles les répliques sont déployées.
   - Objectif de temps de restauration (RTO) - Entrez le RTO souhaité. Le changement de région l'utilise pour donner un aperçu du temps nécessaire à l'exécution du plan de changement de région par rapport au RTO souhaité.

- Rôle IAM - Fournissez un rôle IAM que le commutateur régional utilisera pour exécuter le plan. Pour en savoir plus sur les autorisations, consultez Identity and Access Management pour le changement de région dans ARC.
- CloudWatch Alarme Amazon - Fournissez une alarme d'état de l'application que vous avez créée avec Amazon CloudWatch, pour indiquer l'état de santé de votre application dans chaque région. Le changement de région utilise ces alarmes d'état de l'application pour déterminer le temps de restauration réel une fois que vous avez changé de région pour implémenter la restauration.

  Avant d'ajouter des CloudWatch alarmes à un plan de changement de région, assurez-vous que vous avez mis en place la bonne politique IAM. Pour de plus amples informations, veuillez consulter CloudWatch alarmes pour les autorisations relatives à l'état des applications.
- Génération automatique de rapports : activez éventuellement la génération automatique de rapports pour les exécutions de plans. Lorsque cette option est activée, Region Switch génère un rapport PDF complet une fois l'exécution de chaque plan terminée et le transmet à un compartiment Amazon S3 que vous spécifiez. Fournissez l'URI Amazon S3 et l'ID de compte propriétaire du compartiment.

  Avant d'activer la génération automatique de rapports pour les plans, assurez-vous que vous avez mis en place la bonne politique IAM. Pour plus d'informations sur la génération de rapports et les autorisations requises, consultezRapports d'exécution automatique du plan.
- Tags - Vous pouvez éventuellement ajouter un ou plusieurs tags à votre plan.

Création de flux de travail liés au changement de région

Après avoir créé un plan de changement de région, vous devez définir et créer des flux de travail qui spécifient le processus de restauration de votre application. Pour chaque plan, vous définissez un ou plusieurs flux de travail qui achèvent la restauration de votre application. Dans chaque flux de travail, vous ajoutez des étapes qui incluent des blocs d'exécution qui définissent chaque action que le changement de région doit effectuer pour la restauration de votre application.

Le nombre de flux de travail que vous créez dépend du scénario de déploiement de votre application et de vos préférences en matière de gestion de la restauration. Par exemple :

- Si votre plan de changement de région concerne un active/active application deployment, you also need to create a deactivation workflow. This means that for or active/active déploiement,

vous aurez au moins deux flux de travail : un flux de travail d'activation et un flux de travail de désactivation.

- Si votre plan de changement de région concerne le déploiement d'une active/passive application, vous disposez d'une région principale et d'une région secondaire. Si vous choisissez d'avoir des flux de travail d'activation distincts pour chaque région, vous allez créer deux flux de travail : un pour chaque région.

Pour créer des flux de travail liés au plan de changement de région

1. Dans le plan de changement de région que vous avez créé, choisissez Créer des flux de travail.
2. Sélectionnez l'une des options de flux de travail suivantes :
   - Créez le même flux de travail d'activation pour toutes les régions : vous permet d'utiliser le même flux de travail d'activation dans toutes les régions.
   - Créez des flux de travail séparément pour chaque région : crée un flux de travail d'activation individuel pour chaque région.
3. Vous pouvez éventuellement fournir une description de chaque flux de travail.
4. Définissez le flux de travail requis pour récupérer votre application. Dans votre flux de travail, vous ajoutez des blocs d'exécution pour définir les étapes que le changement de région doit effectuer pour votre restauration. Chaque bloc d'exécution définit des actions, telles que le réacheminement du trafic d'applications ou la restauration de bases de données dans une région en cours d'activation, et prend en charge les ressources dans une autre Compte AWS. Vous pouvez choisir de faire exécuter les blocs d'exécution en parallèle ou de manière séquentielle. Pour obtenir des informations détaillées sur les blocs d'exécution spécifiques que vous pouvez ajouter aux flux de travail, consultezAjouter des blocs d'exécution.
5. En fonction de l'option de flux de travail que vous avez sélectionnée, procédez comme suit :
   - Si vous avez sélectionné Créer le même flux de travail d'activation pour toutes les régions, un seul flux de travail d'activation est requis.
   - Si vous avez sélectionné Créer des flux de travail séparément pour chaque région, deux flux de travail d'activation sont requis.

   Pour les active/active plans, vous devez définir à la fois un flux de travail d'activation et un flux de travail de désactivation.

Ajouter des blocs d'exécution

Vous ajoutez des étapes aux flux de travail dans votre plan de changement de région, pour effectuer les étapes individuelles nécessaires au basculement ou au basculement de votre application. Pour plus de détails sur les fonctionnalités et le comportement de chaque type de bloc d'exécution, consultez les descriptions suivantes.

Le changement de région exécute une évaluation du plan immédiatement après avoir créé un plan ou l'avoir mis à jour, puis toutes les 30 minutes en régime permanent. Le changement de région stocke les informations relatives à l'évaluation du plan dans toutes les régions où votre plan est configuré. Chaque section du bloc d'exécution inclut ici des informations sur ce qui est évalué lorsque Region Switch exécute l'évaluation du plan.

Le changement de région inclut des types de blocs d'exécution qui aident à dimensionner les ressources de calcul dans le cadre de la restauration. Si vous utilisez ces blocs d'exécution dans un plan, sachez que le changement de région ne garantit pas que la capacité de calcul souhaitée sera atteinte. Si vous avez une application critique et que vous devez garantir l'accès à la capacité, nous vous recommandons de réserver la capacité. Il existe des stratégies que vous pouvez suivre pour réserver de la capacité de calcul dans une région secondaire tout en limitant les coûts. Pour en savoir plus, voir Pilot light avec capacité réservée : comment optimiser les coûts de reprise après sinistre à l'aide des réservations de capacité à la demande.

Le commutateur de région prend en charge les blocs d'exécution suivants.

Bloc d'exécution	Fonction	Configuration peu gracieuse
Bloc d'exécution du plan de commutation de la région ARC	Orchestrez la restauration de plusieurs applications en une seule exécution en spécifiant les plans enfants à exécuter.	Lancez des forfaits pour enfants avec leurs configurations peu gracieuses.
Bloc d'exécution du groupe Amazon EC2 Auto Scaling	Faites évoluer les ressources de calcul EC2 qui se trouvent dans un groupe Auto Scaling dans le cadre de l'exécution de votre plan.	Spécifiez le pourcentage minimum de capacité de calcul qui doit être égalé dans la région que vous activez.
Bloc d'exécution du dimensionnement des	Faites évoluer les modules de cluster Amazon EKS dans le cadre de l'exécution de votre plan.	N/A

Bloc d'exécution	Fonction	Configuration peu gracieuse
ressources Amazon EKS		
Bloc d'exécution du dimensionnement du service Amazon ECS	Adaptez les tâches de service Amazon ECS dans le cadre de l'exécution de votre plan.	N/A
Bloc d'exécution du contrôle de routage ARC	Ajoutez une étape pour modifier l'état d'un ou de plusieurs contrôles de routage ARC, afin de rediriger le trafic de votre application vers une cible Région AWS.	N/A
Bloc d'exécution de la base de données globale Amazon Aurora	Exécutez un processus de restauration pour une base de données globale Aurora.	Effectuez un basculement des bases de données globales Aurora (cela peut entraîner une perte de données).
Bloc d'exécution Amazon DocumentDB Global Cluster	Exécutez un flux de restauration pour un cluster global Amazon DocumentDB.	Effectuez un basculement du cluster global Amazon DocumentDB (cela peut potentiellement entraîner une perte de données).
Bloc d'exécution Amazon RDS Promote Read Replica	Transformez une réplique de lecture Amazon RDS en instance de base de données autonome.	N/A
Amazon RDS Create Inter-Region Replica : bloc d'exécution	Créez une réplique de lecture interrégionale pour une instance de base de données Amazon RDS dans le cadre de la post-restauration.	N/A

Bloc d'exécution	Fonction	Configuration peu gracieuse
Bloc d'exécution de l'approbation manuelle	Insérez une étape d'approbation, pour demander l'approbation ou l'annulation d'une exécution avant de poursuivre.	N/A
Action personnalisée : bloc d'exécution Lambda	Ajoutez une étape personnalisée pour exécuter une fonction Lambda, afin de permettre des actions personnalisées.	Sautez l'étape.
Bloc d'exécution du contrôle de santé Amazon Route 53	Spécifie les régions vers lesquelle s le trafic de votre application sera redirigé pendant le basculement.	N/A

Bloc d'exécution du plan de commutation de la région ARC

Le bloc d'exécution du plan de changement de région vous permet d'orchestrer l'ordre dans lequel plusieurs applications basculent vers la région que vous souhaitez activer, en faisant référence à d'autres plans de changement de région enfants. Grâce à cette relation parent/enfant, vous pouvez créer des processus de restauration complexes et coordonnés qui gèrent plusieurs ressources et dépendances au sein de votre infrastructure.

Configuration

Lorsque vous utilisez le bloc d'exécution du plan de changement de région, vous sélectionnez un plan de changement de région spécifique que vous souhaitez exécuter dans le flux de travail du plan que vous créez.

> **Important**
>
> Avant de configurer le bloc d'exécution, assurez-vous que vous avez mis en place la bonne stratégie IAM. Pour de plus amples informations, veuillez consulter Exemple de politique de bloc d'exécution d'un plan de changement de région.

Pour configurer un bloc d'exécution d'un plan de changement de région, entrez les valeurs suivantes :

1. Nom de l'étape : entrez un nom.
2. Description de l'étape (facultatif) : entrez une description de l'étape.
3. Plan de changement de région : sélectionnez un plan à exécuter dans le flux de travail du plan actuel.

Choisissez ensuite Enregistrer l'étape.

Comment ça marche

Utilisez le bloc d'exécution du plan de changement de région pour créer des flux de travail parents avec parent/child des relations. Notez que ce bloc d'exécution ne prend pas en charge les niveaux supplémentaires de plans enfants et limite le nombre de plans parents-enfants. Les plans pour enfants doivent prendre en charge les mêmes régions que celles prises en charge par le plan parent et doivent suivre la même approche de rétablissement que le plan parent (c' active/active est-à-dire actif/passif).

Ce bloc prend en charge les modes d'exécution gracieux et disgracieux. Des paramètres peu élégants lanceront les plans pour enfants avec leur configuration peu élégante. Si le bloc de commutation de région a été exécuté correctement, puis est passé en mode d'exécution disgracieux, tout plan enfant passera également en mode d'exécution disgracieux.

Ce qui est évalué dans le cadre de l'évaluation du plan

Si vous partagez un plan entre plusieurs comptes et que le plan n'est plus partagé avec le compte du plan parent, l'évaluation du changement de région renvoie un avertissement indiquant que le plan n'est pas valide.

Bloc d'exécution du groupe Amazon EC2 Auto Scaling

Le bloc d'exécution du groupe EC2 Auto Scaling vous permet de dimensionner les instances EC2 dans le cadre de votre processus de restauration multirégional. Vous pouvez définir un pourcentage de capacité par rapport à la région que vous quittez (source et destination).

Configuration

Lorsque vous configurez le bloc d'exécution du groupe EC2 Auto Scaling, vous entrez les ARN EC2 Auto Scaling pour les régions spécifiques associées à votre plan. Vous devez saisir EC2 ARNs Auto Scaling dans chaque région que vous souhaitez étendre pendant l'exécution du plan.

> **Important**
>
> Avant de configurer le bloc d'exécution, assurez-vous que vous avez mis en place la bonne stratégie IAM. Pour de plus amples informations, veuillez consulter Exemple de politique d'exécution par blocs d'EC2 Auto Scaling.

Pour configurer un bloc d'exécution d'un groupe EC2 Auto Scaling, entrez les valeurs suivantes :

1. Nom de l'étape : entrez un nom.
2. Description de l'étape (facultatif) : entrez une description de l'étape.
3. ARN du groupe EC2 Auto Scaling par région : entrez l'ARN du groupe EC2 Auto Scaling dans chaque région de votre plan.
4. Pourcentage correspondant à la capacité de la région activée : entrez le pourcentage souhaité du nombre d'instances en cours d'exécution dans le groupe Auto Scaling pour correspondre à la région activée.
5. Approche de surveillance des capacités : sélectionnez l'une des approches suivantes pour surveiller la capacité de vos groupes EC2 Auto Scaling :
   - Capacité de fonctionnement maximale échantillonnée sur 24 heures : choisissez cette option pour utiliser la valeur de capacité souhaitée spécifiée dans la configuration de votre groupe EC2 Auto Scaling. Cette option ne crée pas de coûts supplémentaires, mais elle est potentiellement moins précise que l'utilisation de l'autre option, CloudWatch les métriques.

     Dans l'API de changement de région, cette option correspond à la spécification`sampledMaxInLast24Hours`.

     Pour plus d'informations, consultez la section Définir les limites de dimensionnement pour votre groupe Auto Scaling dans le guide de l'utilisateur Amazon EC2 Auto Scaling.
   - Capacité de fonctionnement maximale échantillonnée sur 24 heures avec CloudWatch : Choisissez cette option pour utiliser les métriques spécifiées dans Amazon CloudWatch pour EC2 Auto Scaling. L'utilisation de cette option peut être plus précise, mais entraîne des coûts supplémentaires liés à l'utilisation de CloudWatch métriques.

     Dans l'API de changement de région, cette option correspond à la spécification`autoscalingMaxInLast24Hours`.

Pour utiliser cette option, vous devez d'abord activer les métriques de groupe pour vos groupes Auto Scaling. Pour plus d'informations, consultez la section Enable Auto Scaling group metrics dans le guide de l'utilisateur Amazon EC2 Auto Scaling.

6. Délai d'expiration : entrez une valeur de délai d'expiration.

Choisissez ensuite Enregistrer l'étape.

Comment ça marche

Après avoir configuré un bloc d'exécution EC2 Auto Scaling, Region switch confirme qu'il n'existe qu'un seul groupe Auto Scaling source et un seul groupe Auto Scaling de destination. S'il existe plusieurs groupes Auto Scaling, le bloc d'exécution échoue lors de l'évaluation du plan. La capacité cible est définie comme le nombre d'instances dont l'état est défini sur`InService`. Pour plus d'informations, consultez la section Cycle de vie des instances EC2 Auto Scaling.

Sur la base de la valeur que vous spécifiez (lorsque vous configurez le bloc d'exécution Auto Scaling) pour un pourcentage correspondant, Region Switch calcule la nouvelle capacité souhaitée pour le groupe Auto Scaling de destination. La nouvelle capacité souhaitée est comparée à la capacité souhaitée du groupe Auto Scaling de destination. La formule utilisée par Region switch pour calculer la capacité souhaitée est la suivante :`ceil(percentToMatch * Source Auto Scaling group capacity)`, où ceil () est une fonction qui arrondit tout résultat fractionnaire. Si la capacité actuellement souhaitée du groupe Auto Scaling de destination est supérieure ou égale à la capacité souhaitée du nouveau groupe Auto Scaling calculé par Region Switch, le bloc d'exécution se poursuit. Notez que le changement de région ne réduit pas la capacité du groupe Auto Scaling.

Lorsque Region Switch exécute un bloc Auto Scaling, Region Switch tente d'augmenter la capacité du groupe Region Auto Scaling cible pour qu'elle corresponde à la capacité souhaitée. Ensuite, le changement de région attend que la capacité du groupe Auto Scaling demandée soit atteinte dans le groupe Auto Scaling de la région cible avant de passer à l'étape suivante du plan.

> **Note**
>
> L'exécution de ce bloc modifie les paramètres de capacité minimale et souhaitée de vos groupes Auto Scaling, ce qui peut entraîner une dérive de configuration si vous gérez ces valeurs par le biais d' infrastructure-as-codeoutils ou d'autres automatismes. Assurez-vous que vos processus de gestion de configuration tiennent compte de ces modifications afin d'éviter les annulations involontaires.

Si vous utilisez une active/active approche, le commutateur de région utilise l'autre région configurée comme source. En d'autres termes, si une région est désactivée, le changement de région utilise l'autre région active comme source pour déterminer le pourcentage d'échelle.

Ce bloc prend en charge les modes d'exécution gracieux et disgracieux. Vous pouvez configurer une exécution irrégulière en spécifiant le pourcentage minimum de capacité de calcul à égaler dans la région cible avant que le changement de région ne passe à l'étape suivante du plan.

Ce qui est évalué dans le cadre de l'évaluation du plan

Lorsque Region Switch évalue votre plan, Region Switch effectue plusieurs vérifications critiques sur la configuration et les autorisations des blocs d'exécution de votre groupe EC2 Auto Scaling. L'évaluation du changement de région vérifie que les groupes Auto Scaling sont présents dans les deux régions, garantit qu'ils sont correctement configurés et accessibles, et note le nombre d'instances en cours d'exécution dans chaque région. Cela confirme également que la capacité maximale du groupe Auto Scaling de la région cible est suffisante pour gérer le pourcentage de correspondance d'échelle spécifié pour la capacité requise.

Le changement de région confirme également que le rôle IAM du plan dispose des autorisations appropriées pour Auto Scaling. Pour plus d'informations sur les autorisations requises pour les blocs d'exécution de commutateurs régionaux, consultezExemples de politiques basées sur l'identité pour le changement de région dans ARC. Si l'une des vérifications échoue, le changement de région renvoie des messages d'avertissement, que vous pouvez consulter dans la console. Vous pouvez également recevoir les avertissements de validation via EventBridge ou en utilisant des opérations d'API.

Bloc d'exécution du dimensionnement des ressources Amazon EKS

Le bloc d'exécution du dimensionnement des ressources EKS vous permet de dimensionner les ressources EKS dans le cadre de votre processus de restauration multirégional. Lorsque vous configurez le bloc d'exécution, vous définissez un pourcentage de capacité à adapter, par rapport à la capacité de la région en cours de désactivation.

Configuration des autorisations d'accès à EKS

Avant de pouvoir ajouter une étape pour le dimensionnement des ressources EKS, vous devez fournir à Region Switch les autorisations nécessaires pour effectuer des actions avec les ressources Kubernetes de vos clusters EKS. Pour fournir un accès au commutateur de région, vous devez créer une entrée d'accès EKS pour le rôle IAM que le commutateur de région utilise

pour l'exécution du plan, en utilisant la politique d'accès au commutateur de région suivante : `arn:aws:eks::aws:cluster-access-policy/AmazonARCRegionSwitchScalingPolicy`

Politique d'accès EKS pour les commutateurs régionaux

Les informations suivantes fournissent des informations détaillées sur la politique d'accès EKS.

Nom: `AmazonARCRegionSwitchScalingPolicy`

ARN de la politique : `arn:aws:eks::aws:cluster-access-policy/AmazonARCRegionSwitchScalingPolicy`

Groupes d'API Kubernetes	Ressources Kubernetes	Verbes (autorisations) Kubernetes
*	*/échelle	obtenir, mettre à jour
*	*/statut	get
autoscaling	autodétartreurs horizontaux à pod	obtenir, patcher

Création d'une entrée d'accès EKS pour le changement de région

L'exemple suivant décrit comment créer les associations d'entrée et de politique d'accès requises afin que Region Switch puisse effectuer des actions spécifiques pour vos ressources Kubernetes. Dans cet exemple, les autorisations s'appliquent à l'espace de noms *`my-namespace1`* du cluster EKS *`my-cluster`* pour le rôle IAM. `arn:aws:iam::555555555555:role/`*`my-role`*

Lorsque vous configurez ces autorisations, assurez-vous de suivre ces étapes pour les deux clusters EKS de votre bloc d'exécution.

Prérequis

> Avant de commencer, remplacez le mode d'authentification du cluster par `API_AND_CONFIG_MAP` ou`API`. La modification du mode d'autorisation ajoute l'API pour les entrées d'accès. Pour plus d'informations, consultez Modifier le mode d'authentification pour utiliser les entrées d'accès dans le guide de l'utilisateur Amazon EKS.

Créez l'entrée d'accès

La première étape consiste à créer l'entrée d'accès à l'aide d'une AWS CLI commande similaire à la suivante :

```
aws eks create-access-entry --cluster-name my-cluster --principal-arn
        arn:aws:iam::555555555555:user/my-user --type STANDARD
```

Pour plus d'informations, consultez la section Créer des entrées d'accès dans le guide de l'utilisateur Amazon EKS.

Création de l'association d'entrée d'accès

Créez ensuite l'association à la politique d'accès du commutateur régional à l'aide d'une AWS CLI commande similaire à la suivante :

```
aws eks associate-access-policy --cluster-name my-cluster --principal-arn
 arn:aws:iam::555555555555:role/my-role \
         --access-scope type=namespace,namespaces=my-namespace1 --policy-arn
         arn:aws:eks::aws:cluster-access-policy/AmazonARCRegionSwitchScalingPolicy
```

Pour plus d'informations, consultez Associer les politiques d'accès aux entrées d'accès dans le guide de l'utilisateur Amazon EKS.

Assurez-vous de répéter ces étapes avec le deuxième cluster EKS de votre bloc d'exécution, dans l'autre région, afin de vous assurer que les deux clusters sont accessibles par le biais du commutateur de région.

Configuration

> **Important**
>
> Avant d'ajouter une étape de dimensionnement des ressources EKS, assurez-vous d'abord que vous avez configuré les autorisations appropriées. Pour de plus amples informations, veuillez consulter Configuration des autorisations d'accès à EKS. Assurez-vous également que vous avez mis en place la bonne politique IAM. Pour de plus amples informations, veuillez consulter Exemple de politique d'exécution du dimensionnement des ressources Amazon EKS.

Notez que le changement de région prend actuellement en charge les ReplicaSet ressources suivantes : apps/v1, Deployment, and apps/v 1.

Pour la configuration du bloc d'exécution, entrez les valeurs suivantes.

1. Nom de l'étape : entrez un nom.
2. Description de l'étape (facultatif) : entrez une description de l'étape.
3. Nom de l'application : entrez le nom de votre application EKS, par exemple, MyApplication.
4. Type de ressource Kubernetes : entrez le type de ressource pour l'application, par exemple, Déploiement.
5. Ressource par région : pour chaque région, entrez les informations relatives au cluster EKS, notamment l'ARN du cluster EKS, l'espace de noms des ressources, etc.
6. Pourcentage correspondant à la capacité de la région activée : entrez le pourcentage souhaité de pods actifs dans la région source pour qu'il corresponde à celui de la région activée.
7. Approche de surveillance de la capacité : la seule option de surveillance de la capacité est déjà sélectionnée, capacité de fonctionnement maximale échantillonnée sur 24 heures.

   Cette approche de surveillance des capacités utilise la `ReplicaCount` valeur des demandes de service EKS. Pour plus d'informations, consultez la section En savoir plus sur le changement de zone ARC dans Amazon EKS dans le guide de l'utilisateur d'Amazon Elastic Kubernetes Service.
8. Délai d'expiration : entrez une valeur de délai d'expiration.

Choisissez ensuite Enregistrer l'étape.

Comment ça marche

Au cours de l'exécution d'un plan, Region Switch récupère le nombre maximum de répliques échantillonné au cours des 24 dernières heures pour la ressource cible dans la région que vous activez. Il calcule ensuite le nombre de répliques souhaité pour la ressource de destination à l'aide de la formule suivante : `ceil(percentToMatch * Source replica count)`

Si le nombre de répliques prêtes pour la destination est inférieur à la valeur souhaitée, Region Switch adapte la valeur de réplication de la ressource de destination à la capacité souhaitée. Il attend que les répliques soient prêtes et utilise le scaler automatique de votre nœud pour augmenter la capacité du nœud si nécessaire.

Si le `hpaName` champ facultatif n'est pas vide, Region switch HorizontalPodAutoscaler applique le correctif suivant pour empêcher toute réduction automatique pendant ou après l'exécution : `{"spec":{"behavior":{"scaleDown":{"selectPolicy":"Disabled"}}}}`

Assurez-vous de configurer tout outil de correction de dérive, tel que l' GitOps outillage, de manière à ignorer le champ de réplication pour les ressources du correctif, ainsi que le champ. HorizontalPodAutoscaler

Ce qui est évalué dans le cadre de l'évaluation du plan

Lorsque Region Switch évalue votre plan, Region Switch effectue plusieurs vérifications sur le bloc d'exécution et les autorisations que vous avez configurés pour EKS. Le changement de région vérifie que le rôle IAM du plan dispose des autorisations appropriées pour décrire les clusters EKS et répertorier les politiques d'entrée d'accès associées. Le changement de région valide également que le rôle IAM est associé à la bonne politique d'entrée d'accès, de sorte que le commutateur de région dispose des autorisations requises pour agir sur les ressources Kubernetes. Enfin, Region Switch confirme que les clusters EKS et les ressources Kubernetes configurés existent.

En outre, Region Switch vérifie qu'il a correctement collecté et stocké les données de surveillance nécessaires (nombre de répliques Kubernetes) et capture le nombre de pods en cours d'exécution nécessaires pour exécuter le plan de changement de région.

Bloc d'exécution du dimensionnement du service Amazon ECS

Le bloc d'exécution du dimensionnement du service ECS vous permet de dimensionner votre service ECS dans une région de destination dans le cadre de votre processus de restauration multirégional. Vous pouvez définir un pourcentage de capacité par rapport à la région à partir de laquelle le changement de région bascule ou se désactive.

Configuration

Pour configurer le bloc d'exécution du service ECS Scaling, entrez les valeurs suivantes.

> **Important**
>
> Avant de configurer le bloc d'exécution, assurez-vous que vous avez mis en place la bonne stratégie IAM. Pour de plus amples informations, veuillez consulter Exemple de politique de mise à l'échelle des blocs d'exécution du service Amazon ECS.

1. Nom de l'étape : entrez un nom.

2. Description de l'étape (facultatif) : entrez une description de l'étape.
3. Ressource pour la région : pour chaque région, entrez l'ARN du cluster ECS et l'ARN du service ECS.
4. Pourcentage correspondant au nombre de tâches de la région source : entrez le pourcentage souhaité de tâches en cours d'exécution dans la région source pour qu'il corresponde à celui de la région activée.
5. Approche de surveillance de la capacité : sélectionnez l'une des approches suivantes pour surveiller la capacité d'Amazon ECS :
   - Capacité de fonctionnement maximale échantillonnée sur 24 heures : choisissez cette option pour utiliser la valeur du nombre de tâches en cours dans votre service Amazon ECS. Cette option ne crée pas de coûts supplémentaires, mais elle est potentiellement moins précise que l'utilisation de l'autre option, CloudWatch les métriques.

     Dans l'API de changement de région, cette option correspond à la spécification`sampledMaxInLast24Hours`.

     Pour plus d'informations, consultez la section Mise à l'échelle automatique de votre service Amazon ECS dans le guide du développeur Amazon Elastic Container Service.
   - Capacité de fonctionnement maximale échantillonnée sur 24 heures via Container Insights : choisissez cette option pour utiliser les métriques Amazon ECS Container Insights. L'utilisation de cette option peut être plus précise, mais entraîne des coûts supplémentaires liés à l'utilisation de Container Insights.

     Dans l'API de changement de région, cette option correspond à la spécification`autoscalingMaxInLast24Hours`.

     Pour utiliser cette option, vous devez d'abord activer Container Insights. Pour plus d'informations, consultez la section Configurer Container Insights dans le guide de CloudWatch l'utilisateur Amazon.
6. Délai d'expiration : entrez une valeur de délai d'expiration.

Choisissez ensuite Enregistrer l'étape.

Comment ça marche

Après avoir configuré le bloc d'exécution dans votre plan, Region Switch confirme qu'il n'existe qu'un seul service ECS source et un seul service de destination. S'il existe plusieurs services, Region

Switch renvoie un avertissement pour le bloc d'exécution. Le changement de région stocke ces données dans toutes les régions pour lesquelles votre plan est configuré. La capacité cible est définie comme le nombre souhaité défini sur votre service ECS.

Pour une active/passive approche, le commutateur de région calcule la nouvelle capacité souhaitée pour le service ECS dans la région de destination (d'activation). La nouvelle capacité souhaitée est comparée à la capacité souhaitée du service ECS de destination. La formule utilisée par Region switch pour calculer la capacité souhaitée est la suivante :`ceil(percentToMatch * Source Auto Scaling group capacity)`, où ceil () est une fonction qui arrondit tout résultat fractionnaire. Si le nombre actuellement souhaité pour le service ECS de destination est supérieur à la nouvelle capacité souhaitée calculée pour le service ECS, l'exécution du plan se poursuit. Notez que le changement de région ne réduit pas la capacité du service ECS.

Si le service ECS a activé le dimensionnement automatique des applications, Region Switch met à jour la capacité minimale dans Application Autoscaling et met également à jour le nombre souhaité dans le service ECS.

Lorsque le commutateur régional exécute un bloc de service ECS, le commutateur régional tente d'augmenter la capacité ECS de la région cible pour qu'elle corresponde à la capacité souhaitée. Ensuite, le changement de région attend que la capacité de service ECS demandée soit atteinte dans le service ECS de la région cible avant de passer à l'étape suivante du plan. Si vous le souhaitez, vous pouvez configurer l'étape pour qu'elle soit terminée avant que le traitement ne soit terminé en définissant un délai d'attente pour le changement de région avant que la capacité ne soit atteinte.

Si vous utilisez une active/active approche, le commutateur de région utilise l'autre région configurée comme source. En d'autres termes, si une région est désactivée, le changement de région utilise l'autre région active comme source pour déterminer le pourcentage d'échelle.

Ce qui est évalué dans le cadre de l'évaluation du plan

Lorsque Region Switch évalue votre plan, Region Switch effectue plusieurs vérifications sur la configuration et les autorisations des blocs d'exécution de votre service ECS. Le changement de région vérifie que les services ECS sont présents à la fois dans les régions source et cible, et vérifie que la capacité maximale définie pour le service ECS de la région cible est suffisante pour gérer le pourcentage de correspondance spécifié par rapport à la capacité de la région cible. Le changement de région valide également que le rôle IAM du plan dispose des autorisations appropriées pour le service ECS. Pour plus d'informations sur les autorisations requises pour les blocs d'exécution de commutateurs régionaux, consultezExemples de politiques basées sur l'identité pour le changement de région dans ARC.

En outre, Region Switch vérifie que les données de surveillance nécessaires pour les services ECS ont `ResourceMonitor` été collectées et stockées avec succès, et enregistre le nombre de tâches en cours d'exécution.

Si l'une des vérifications échoue, le changement de région renvoie des messages d'avertissement, que vous pouvez consulter dans la console. Vous pouvez également recevoir les avertissements de validation via EventBridge ou en utilisant des opérations d'API.

Bloc d'exécution du contrôle de routage ARC

Si vous avez configuré le contrôle de routage d'Amazon Application Recovery Controller (ARC) pour votre application, vous pouvez ajouter une étape de contrôle de routage ARC pour rediriger le trafic de l'application. Cette étape vous permet de modifier l'état d'un ou de plusieurs contrôles de routage ARC afin de rediriger le trafic de votre application vers une destination Région AWS. Le contrôle de routage ARC redirige le trafic en utilisant des contrôles de santé dans Amazon Route 53 qui sont configurés avec les enregistrements DNS associés aux contrôles de routage.

> **Important**
>
> Le contrôle de routage d'Amazon Application Recovery Controller (ARC) n'est disponible que dans la partition AWS commerciale.

Configuration

Pour configurer un bloc d'exécution du contrôle de routage, entrez les valeurs suivantes.

> **Important**
>
> Avant de configurer le bloc d'exécution, assurez-vous que vous avez mis en place la bonne stratégie IAM. Pour de plus amples informations, veuillez consulter Exemple de politique de bloc d'exécution des contrôles de routage ARC.

1. Nom de l'étape : entrez un nom.
2. Description de l'étape (facultatif) : entrez une description de l'étape.
3. Contrôles de routage souhaités : pour chaque région que vous souhaitez activer ou désactiver, entrez l'ARN du contrôle de routage et l'état initial du contrôle de routage, Activé ou Désactivé.

4. Délai d'expiration : entrez une valeur de délai d'expiration.

Choisissez ensuite Enregistrer l'étape.

Le modèle attendu pour ce bloc d'exécution est de spécifier des contrôles de routage et des états initiaux correspondant à la manière dont vous avez configuré votre application en particulier Régions AWS. Par exemple, si vous avez un plan qui vous permet d'activer les régions A et B pour votre application, vous pouvez avoir un contrôle de routage pour la région A où vous définissez l'état sur Activé et un contrôle de routage pour la région B où vous définissez l'état sur Activé.

Ensuite, lorsque vous exécutez le plan et que vous spécifiez que vous souhaitez activer la région A, le flux de travail qui inclut ce bloc d'exécution met le contrôle de routage spécifié à Activé, ce qui dirige le trafic vers la région A.

Comment ça marche

En configurant un bloc d'exécution du contrôle de routage ARC, vous pouvez rediriger le trafic de l'application vers une destination ou Région AWS, dans le cas d'une active/active approche, empêcher le trafic d'être acheminé vers une région que vous désactivez. Si votre plan inclut plusieurs flux de travail, assurez-vous de fournir les mêmes entrées pour les enregistrements DNS pour tous les blocs d'exécution du contrôle de routage que vous utilisez.

Ce bloc ne prend pas en charge le mode d'exécution peu scrupuleux.

Ce qui est évalué dans le cadre de l'évaluation du plan

Lorsque Region Switch évalue votre plan, Region switch effectue plusieurs vérifications sur le routage, les contrôles, la configuration des blocs d'exécution et les autorisations. Le commutateur de région vérifie que les commandes de routage spécifiées sont correctement configurées et accessibles.

Le changement de région confirme également que le rôle IAM du plan dispose des autorisations requises pour accéder aux états de contrôle de routage et les mettre à jour. Pour plus d'informations sur les autorisations requises pour les blocs d'exécution de commutateurs régionaux, consultezExemples de politiques basées sur l'identité pour le changement de région dans ARC.

Les autorisations IAM correctes sont essentielles au bon fonctionnement du bloc d'exécution du contrôle de routage. Si l'une de ces validations échoue, Region Switch renvoie des avertissements indiquant la présence de problèmes et fournit des messages d'erreur spécifiques pour vous aider à résoudre les problèmes d'autorisation ou de configuration. Cela garantit que votre plan dispose

de l'accès nécessaire pour gérer et interagir avec les contrôles de routage ARC lorsque cette étape s'exécute pendant l'exécution d'un plan.

Comparaison des contrôles de routage ARC et des blocs d'exécution des contrôles de santé Route 53

Le bloc d'exécution du contrôle de santé Amazon Route 53 dans Region Switch constitue une alternative moins coûteuse pour la gestion du trafic basée sur le DNS. Toutefois, ce bloc d'exécution dépend de la région Région AWS que vous activez, de sorte que cette région doit être disponible. Cela répond aux besoins de la plupart des clients, car ils activent une région saine.

Les contrôles de routage ARC fournissent une gestion du trafic hautement fiable basée sur le DNS avec un SLA de disponibilité à 100 %. Grâce aux contrôles de routage, vos équipes opérationnelles peuvent transférer le trafic entre les régions à l'aide de glissières de sécurité. Les contrôles de routage fournissent une solution à locataire unique avec un SLA de 100 %. Un cluster de contrôle de routage est réparti sur cinq régions et peut tolérer que deux régions soient hors ligne. Si vous avez des applications très critiques, pensez à utiliser des contrôles de routage.

Les contrôles de routage ne sont pas nécessaires pour utiliser le changement de région. Vous pouvez utiliser le commutateur de région pour gérer la redirection du trafic en utilisant les blocs d'exécution des contrôles de santé de Route 53 sans contrôles de routage.

Les contrôles de routage ajoutent de la valeur avec le changement de région dans les situations suivantes :

- Vous avez besoin du SLA de disponibilité à 100 % pour le mécanisme de contrôle du trafic lui-même.
- Votre entreprise a besoin de contrôles opérationnels manuels assortis de règles de sécurité pour les applications critiques.
- Vous voulez defense-in-depth que les équipes opérationnelles puissent annuler manuellement le routage automatique du trafic si nécessaire.

Les blocs d'exécution du bilan de santé de Route 53 ne dépendent pas du plan de contrôle. Les modifications apportées aux dossiers de contrôle de santé utilisent le plan de données, de sorte qu'elles ne nécessitent pas la région d'activation pour traiter les mises à jour de configuration. Les blocs d'exécution du bilan de santé Route 53 sont suffisants dans les situations suivantes :

- Votre application peut dépendre de Région AWS celle que vous activez.

- La redirection automatique du trafic dans le cadre du processus de restauration répond à vos exigences.
- L'optimisation des coûts est une priorité. Les blocs d'exécution des contrôles de santé Route 53 sont moins coûteux que les contrôles de routage.

La plupart des clients commencent par utiliser les blocs d'exécution des contrôles d'état de Route 53 comme mécanisme de routage du trafic par défaut et ajoutent des contrôles de routage uniquement pour leurs applications les plus critiques qui nécessitent le plus haut niveau de fiabilité pour le mécanisme de gestion du trafic.

Bloc d'exécution de la base de données globale Amazon Aurora

Le bloc d'exécution de la base de données globale Amazon Aurora vous permet d'exécuter un flux de travail de restauration en cas de basculement ou de basculement pour une base de données globale.

- Basculement : utilisez cette approche pour récupérer après une panne imprévue. Avec cette approche, vous effectuez un basculement entre régions vers l'un des clusters de bases de données secondaires de vos bases de données globales Aurora. L'objectif du point de récupération (RPO) pour cette approche est généralement une valeur différente de zéro mesurée en secondes. L'ampleur de la perte de données dépend du délai de réplication des bases de données globales Aurora Régions AWS au moment de la panne. Pour plus d'informations, consultez la section Restauration d'une base de données globale Amazon Aurora suite à une panne imprévue dans le guide de l'utilisateur Amazon Aurora.
- Basculement : cette opération était auparavant appelée basculement planifié géré. Adoptez cette approche pour les scénarios contrôlés, tels que la maintenance opérationnelle et d'autres procédures opérationnelles planifiées, où tous les clusters Aurora et les autres services avec lesquels ils interagissent sont en bon état. Étant donné que cette fonction synchronise les clusters de bases de données secondaires avec le cluster principal avant toute modification, le RPO est égal à 0 (aucune donnée perdue). Pour plus d'informations, consultez la section Effectuer des commutations pour les bases de données mondiales Amazon Aurora dans le guide de l'utilisateur Amazon Aurora.

Configuration

Pour configurer un bloc d'exécution de la base de données globale Aurora, entrez les valeurs suivantes.

> **Important**
>
> Avant de configurer le bloc d'exécution, assurez-vous que vous avez mis en place la bonne stratégie IAM. Pour de plus amples informations, veuillez consulter Exemple de politique d'exécution de la base de données globale Aurora.

1. Nom de l'étape : entrez un nom.
2. Description de l'étape (facultatif) : entrez une description de l'étape.
3. Nom du cluster de base de données globale Aurora : entrez l'identifiant de la base de données globale.
4. ARN du cluster pour la région : entrez l'ARN du cluster à utiliser dans chaque région du plan.
5. Spécifiez l'option pour la base de données Aurora : choisissez Switchover ou Failover (perte de données), selon la méthode que vous souhaitez
6. Nom du cluster de base de données globale Aurora :
7. Délai d'expiration : entrez une valeur de délai d'expiration.

Choisissez ensuite Enregistrer l'étape.

Comment ça marche

En configurant un bloc d'exécution des bases de données globales Aurora, vous pouvez basculer ou basculer des bases de données globales dans le cadre de la restauration de votre application. Si vous utilisez une active/active approche, le commutateur de région utilise l'autre région configurée comme source. En d'autres termes, si une région est désactivée, le changement de région utilise l'autre région active comme source pour déterminer le pourcentage d'échelle.

Ce bloc prend en charge les modes d'exécution gracieux et disgracieux. Des paramètres incorrects provoquent un basculement de la base de données globale Aurora, ce qui peut entraîner une perte de données.

Pour plus d'informations sur la reprise après sinistre d'Aurora Global Database, y compris le basculement et le basculement, consultez la section Utilisation du basculement ou du basculement dans les bases de données mondiales Amazon Aurora dans le guide de l'utilisateur Amazon Aurora.

Ce qui est évalué dans le cadre de l'évaluation du plan

Lorsque Region Switch évalue votre plan, Region Switch effectue plusieurs vérifications sur la configuration et les autorisations de votre bloc d'exécution Aurora. Le changement de région vérifie que les informations suivantes sont correctes :

- Le cluster global Aurora spécifié dans la configuration existe.
- Il existe des clusters de base de données Aurora dans les régions source et de destination.
- Les clusters de base de données source et de destination sont dans un état qui permet le passage d'une base de données globale à un autre.
- Il existe des instances de base de données dans les clusters source et de destination
- Les versions du moteur de cluster global pour l'action de commutation sont compatibles. Cela inclut de vérifier que les clusters utilisent les mêmes versions majeure, mineure et correctif, à quelques exceptions près répertoriées dans la documentation Aurora.

Le changement de région confirme également que le rôle IAM du plan dispose des autorisations requises pour le basculement et le basculement d'Aurora. Pour plus d'informations sur les autorisations requises pour les blocs d'exécution de commutateurs régionaux, consultezExemples de politiques basées sur l'identité pour le changement de région dans ARC.

Les autorisations IAM correctes sont essentielles au bon fonctionnement du bloc d'exécution Aurora. Si l'une de ces validations échoue, Region Switch renvoie des avertissements indiquant la présence de problèmes et fournit des messages d'erreur spécifiques pour vous aider à résoudre les problèmes d'autorisation ou de configuration. Cela garantit que votre plan dispose de l'accès nécessaire pour gérer et interagir avec l'Aurora lorsque cette étape s'exécute pendant l'exécution d'un plan.

Bloc d'exécution Amazon DocumentDB Global Cluster

Le bloc d'exécution Amazon DocumentDB Global Cluster vous permet d'exécuter un flux de travail de restauration en cas de basculement ou de basculement pour un cluster global.

- Basculement : utilisez cette approche pour récupérer après une panne imprévue. Avec cette approche, vous effectuez un basculement entre régions vers l'un des clusters secondaires de votre cluster global Amazon DocumentDB. L'objectif du point de récupération (RPO) pour cette approche est généralement une valeur différente de zéro mesurée en secondes. L'ampleur de la perte de données dépend du délai global de réplication du cluster Amazon DocumentDB Régions AWS au moment de l'échec.

- Basculement : utilisez cette approche pour des scénarios contrôlés, tels que la maintenance opérationnelle et d'autres procédures opérationnelles planifiées dans lesquels tous les clusters Amazon DocumentDB sont sains. Comme cette fonctionnalité synchronise les clusters secondaires avec les clusters principaux avant d'apporter d'autres modifications, le RPO est égal à 0 (aucune perte de données).

Configuration

Pour configurer un bloc d'exécution Amazon DocumentDB Global Cluster, entrez les valeurs suivantes.

> **Important**
>
> Avant de configurer le bloc d'exécution, assurez-vous que vous avez mis en place la bonne stratégie IAM. Pour de plus amples informations, veuillez consulter Exemple de politique d'exécution par blocs d'Amazon DocumentDB Global Cluster.

1. Nom de l'étape : entrez un nom.
2. Description de l'étape (facultatif) : entrez une description de l'étape.
3. Identifiant du cluster global Amazon DocumentDB : entrez l'identifiant du cluster global.
4. ARN du cluster pour la région : entrez l'ARN du cluster à utiliser dans chaque région du plan.
5. Spécifiez l'option pour le cluster Amazon DocumentDB : choisissez Switchover ou Failover (perte de données).
6. Délai d'expiration : entrez une valeur de délai d'expiration.

Choisissez ensuite Enregistrer l'étape.

Comment ça marche

En configurant un bloc d'exécution Amazon DocumentDB Global Cluster, vous pouvez basculer ou basculer sur des clusters globaux dans le cadre de la restauration de votre application. Si vous utilisez une active/active approche, le commutateur de région utilise l'autre région configurée comme source. En d'autres termes, si une région est désactivée, le changement de région utilise l'autre région active comme source pour déterminer le pourcentage d'échelle.

Ce bloc prend en charge les modes d'exécution gracieux et disgracieux. Des paramètres incorrects provoquent un basculement d'Amazon DocumentDB Global Cluster, ce qui peut entraîner une perte de données.

Pendant les opérations de basculement ou de basculement, le point de terminaison DNS utilisé par les clients pour écrire sera modifié. Les clients sont tenus de s'assurer qu'ils utilisent le bon point de terminaison une fois l'opération terminée.

Ce qui est évalué dans le cadre de l'évaluation du plan

Lorsque Region Switch évalue votre plan, Region Switch effectue plusieurs vérifications sur la configuration et les autorisations de votre bloc d'exécution Amazon DocumentDB. Le changement de région vérifie que les informations suivantes sont correctes :

- Le cluster global Amazon DocumentDB spécifié dans la configuration existe.
- Il existe des clusters Amazon DocumentDB dans les régions source et de destination.
- Les clusters source et de destination sont disponibles.
- Il existe des instances dans les clusters source et de destination.
- Les versions du moteur de cluster global sont compatibles.

Le changement de région confirme également que le rôle IAM du plan dispose des autorisations requises pour le basculement et le basculement d'Amazon DocumentDB. Pour plus d'informations sur les autorisations requises pour les blocs d'exécution de commutateurs régionaux, consultezExemples de politiques basées sur l'identité pour le changement de région dans ARC.

Les autorisations IAM correctes sont essentielles au bon fonctionnement du bloc d'exécution Amazon DocumentDB. Si l'une de ces validations échoue, Region Switch renvoie des avertissements indiquant la présence de problèmes et fournit des messages d'erreur spécifiques pour vous aider à résoudre les problèmes d'autorisation ou de configuration. Cela garantit que votre plan dispose de l'accès nécessaire pour gérer et interagir avec Amazon DocumentDB lorsque cette étape s'exécute pendant l'exécution d'un plan.

Bloc d'exécution Amazon RDS Promote Read Replica

Le bloc d'exécution Amazon RDS Promote Read Replica vous permet de promouvoir une réplique de lecture Amazon RDS vers une instance de base de données autonome dans le cadre de votre processus de restauration multirégional. Cela vous permet de basculer vers une région saine en faisant de la réplique lue de cette région la nouvelle base de données principale.

Configuration

Pour configurer un bloc d'exécution Amazon RDS Promote Read Replica, entrez les valeurs suivantes.

> **Important**
>
> Avant de configurer le bloc d'exécution, assurez-vous que vous avez mis en place la bonne stratégie IAM. Pour de plus amples informations, veuillez consulter Exemple de politique relative aux blocs d'exécution Amazon RDS.

1. Nom de l'étape : entrez un nom.
2. Description de l'étape (facultatif) : entrez une description de l'étape.
3. ARN de l'instance de base de données RDS pour la région : entrez l'ARN de l'instance de base de données pour la réplique lue dans chaque région du plan.
4. Délai d'expiration : entrez une valeur de délai d'expiration.

Choisissez ensuite Enregistrer l'étape.

Comment ça marche

En configurant un bloc d'exécution Amazon RDS Promote Read Replica, vous pouvez transformer une réplique en lecture en instance de base de données autonome dans le cadre de la restauration de votre application. Lorsque vous exécutez le plan, Region Switch fait en sorte que la réplique en lecture de la région que vous activez devienne une instance de base de données indépendante.

> **Note**
>
> Ce bloc ne prend en charge que les active/passive plans

Pendant la promotion, le point de terminaison DNS que vous utilisez pour vous connecter à la base de données restera le même. Toutefois, l'instance promue ne sera plus répliquée à partir de la base de données principale d'origine. Il vous incombe de vous assurer que leur application est configurée pour utiliser le point de terminaison approprié une fois l'opération terminée.

Après la promotion, l'instance promue hérite des paramètres de sauvegarde suivants de l'instance principale d'origine :

- Période de rétention des sauvegardes
- Fenêtre de sauvegarde préférée

Ce qui est évalué dans le cadre de l'évaluation du plan

Lorsque Region Switch évalue votre plan, Region Switch effectue plusieurs vérifications sur la configuration et les autorisations de votre bloc d'exécution Amazon RDS. Le changement de région vérifie que les informations suivantes sont correctes :

- Les instances de base de données Amazon RDS spécifiées dans la configuration existent.
- Les instances de base de données dans les régions non principales sont des répliques de lecture.
- Les répliques de lecture sont dans un état disponible.
- Les instances de base de données sont correctement configurées pour la réplication entre régions.

Le changement de région confirme également que le rôle IAM du plan dispose des autorisations requises pour la promotion des répliques de lecture sur Amazon RDS. Pour plus d'informations sur les autorisations requises pour les blocs d'exécution de commutateurs régionaux, consultezExemples de politiques basées sur l'identité pour le changement de région dans ARC.

Les autorisations IAM correctes sont essentielles au bon fonctionnement du bloc d'exécution Amazon RDS. Si l'une de ces validations échoue, Region Switch renvoie des avertissements indiquant la présence de problèmes et fournit des messages d'erreur spécifiques pour vous aider à résoudre les problèmes d'autorisation ou de configuration. Cela garantit que votre plan dispose de l'accès nécessaire pour gérer et interagir avec Amazon RDS lorsque cette étape s'exécute pendant l'exécution d'un plan.

Amazon RDS Create Inter-Region Replica : bloc d'exécution

Le bloc d'exécution Amazon RDS Create Cross-Replica vous permet de créer une réplique de lecture interrégionale pour une instance de base de données Amazon RDS dans le cadre de votre processus de post-restauration. Ce bloc d'exécution est généralement utilisé après la promotion d'une réplique en lecture pour rétablir la réplication entre régions, garantissant ainsi que votre application est prête pour les futurs événements régionaux.

Configuration

Pour configurer un bloc d'exécution Amazon RDS Create Cross-Region Replica, entrez les valeurs suivantes.

> **Important**
>
> Avant de configurer le bloc d'exécution, assurez-vous que vous avez mis en place la bonne stratégie IAM. Pour de plus amples informations, veuillez consulter Exemple de politique relative aux blocs d'exécution Amazon RDS.

1. Nom de l'étape : entrez un nom.
2. Description de l'étape (facultatif) : entrez une description de l'étape.
3. ARN de l'instance de base de données source pour la région : entrez l'ARN de l'instance de base de données pour la base de données source dans chaque région du plan. Le bloc d'exécution utilise l'identifiant de la région activée comme base de données source pour créer la réplique de lecture entre régions.
4. ARN de l'instance de base de données de réplique : entrez l'ARN de l'instance à utiliser pour la nouvelle réplique de lecture.
5. Délai d'expiration : entrez une valeur de délai d'expiration.

Choisissez ensuite Enregistrer l'étape.

Comment ça marche

En configurant un bloc d'exécution Amazon RDS Create Cross-Region Replica, vous pouvez créer une réplique en lecture dans l'autre région dans le cadre de votre processus de post-restauration. Ce bloc d'exécution est conçu pour s'exécuter après un basculement réussi afin de rétablir la réplication entre régions.

Ce bloc ne peut être ajouté qu'aux active/passive plans.

Au cours de l'exécution, l'ancienne instance principale sera renommée et étiquetée avec renamedByRegionSwitch. Ensuite, une nouvelle instance de réplique en lecture sera créée avec les paramètres suivants copiés à partir de l'ancien serveur principal :

- Identifiant de l'instance
- Groupes de paramètres DB
- Groupes de sous-réseaux DB
- Clé KMS

- Groupes de sécurité VPC
- Groupes d’options
- Configuration multi-AZ
- Secret d'authentification de domaine (ARN)

> **Important**
>
> L'instance principale renommée reste active et continue d'être facturée. Region Switch l'associe à renamedByRegionSwitch à des fins d'identification, mais ne le modifie ni ne le supprime autrement. Vous êtes chargé de gérer l'instance renommée, notamment de décider de la maintenir en activité, de l'arrêter ou de la supprimer en fonction de vos exigences opérationnelles et financières.

> **Note**
>
> Ce bloc d'exécution est conçu pour les flux de travail après restauration et nécessite que la région source soit saine et accessible. Il doit être utilisé après un basculement réussi pour rétablir la réplication entre régions.

Ce qui est évalué dans le cadre de l'évaluation du plan

Lorsque Region Switch évalue votre plan, Region Switch effectue plusieurs vérifications sur la configuration et les autorisations de votre bloc d'exécution Amazon RDS. Le changement de région vérifie que les informations suivantes sont correctes :

- Les instances de base ARNs de données de la configuration sont valides et correctement formatées.
- Les instances de base de données source existent dans leurs régions respectives.
- Les instances de base de données source sont disponibles.

Le changement de région confirme également que le rôle IAM du plan dispose des autorisations requises pour créer des répliques de lecture Amazon RDS. Pour plus d'informations sur les autorisations requises pour les blocs d'exécution de commutateurs régionaux, consultezExemples de politiques basées sur l'identité pour le changement de région dans ARC.

Les autorisations IAM correctes sont essentielles au bon fonctionnement du bloc d'exécution Amazon RDS. Si l'une de ces validations échoue, Region Switch renvoie des avertissements indiquant la présence de problèmes et fournit des messages d'erreur spécifiques pour vous aider à résoudre les problèmes d'autorisation ou de configuration. Cela garantit que votre plan dispose de l'accès nécessaire pour gérer et interagir avec Amazon RDS lorsque cette étape s'exécute pendant l'exécution d'un plan.

Bloc d'exécution de l'approbation manuelle

Le bloc d'exécution manuelle de l'approbation vous permet d'insérer une étape d'approbation que vous associez à un rôle IAM. Les utilisateurs ayant accès au rôle peuvent approuver ou refuser l'exécution d'une étape, suspendre l'étape jusqu'à ce que l'approbation soit accordée ou, éventuellement, empêcher le plan de progresser.

Pour garantir que l'approbation manuelle est requise lors de l'exécution du plan, vous saisissez une étape d'approbation manuelle à un emplacement spécifique du flux de travail, puis vous configurez le rôle IAM pour spécifier qui peut approuver l'étape.

Configuration

Pour configurer un bloc d'exécution d'approbation manuelle, entrez les valeurs suivantes.

> **Important**
>
> Avant de configurer le bloc d'exécution, assurez-vous que vous avez mis en place la bonne stratégie IAM. Pour de plus amples informations, veuillez consulter Exemple de politique d'exécution des approbations manuelles.

1. Nom de l'étape : entrez un nom.
2. Description de l'étape (facultatif) : entrez une description de l'étape.
3. Rôle d'approbation IAM : entrez l'ARN d'un rôle IAM autorisé à approuver manuellement la poursuite de l'exécution pour le plan de changement de région. Le rôle IAM doit figurer dans le compte propriétaire du plan.
4. Délai d'expiration : entrez une valeur de délai d'expiration.

Choisissez ensuite Enregistrer l'étape.

Comment ça marche

En configurant un bloc d'exécution d'approbation manuelle, vous pouvez demander une approbation dans le cadre de la restauration de votre application. Pour un bloc d'exécution manuelle, Region Switch effectue les opérations suivantes :

- Lorsque Region Switch exécute un bloc d'exécution manuelle, il suspend l'exécution et définit le statut d'exécution du plan sur En attente d'approbation.
- Toute personne ayant accès au rôle défini dans le bloc d'exécution peut approuver ou refuser l'exécution de l'étape.
- S'ils approuvent l'exécution de l'étape, Region Switch procède à l'exécution du plan. S'ils refusent, le changement de région annule l'exécution du plan.

Ce bloc ne prend pas en charge le mode d'exécution peu scrupuleux.

Ce qui est évalué dans le cadre de l'évaluation du plan

Le changement de région n'effectue aucune évaluation pour les blocs d'exécution d'approbation manuelle.

Action personnalisée : bloc d'exécution Lambda

Le bloc d'exécution Lambda d'actions personnalisées vous permet d'ajouter une étape personnalisée à un plan à l'aide d'une fonction Lambda.

Configuration

Pour configurer un bloc d'exécution Lambda, entrez les valeurs suivantes.

> **⚠ Important**
>
> Avant de configurer le bloc d'exécution, assurez-vous que vous avez mis en place la bonne stratégie IAM. Pour de plus amples informations, veuillez consulter Exemple de politique de bloc d'exécution Lambda pour les actions personnalisées.

1. Nom de l'étape : entrez un nom.
2. Description de l'étape (facultatif) : entrez une description de l'étape.
3. ARN de la fonction Lambda à invoquer lors de l'activation ou de la désactivation de Region : Spécifiez l'ARN de la fonction Lambda à exécuter pour cette étape.

4. Région dans laquelle exécuter la fonction Lambda : dans le menu déroulant, choisissez la région dans laquelle vous souhaitez exécuter les fonctions Lambda.
5. Délai d'expiration : entrez une valeur de délai d'expiration.
6. Intervalle entre les tentatives : entrez un intervalle entre les tentatives, pour réexécuter la fonction Lambda si elle échoue dans cet intervalle.

Choisissez ensuite Enregistrer l'étape.

Comment ça marche

- Lorsque vous créez un bloc d'exécution Lambda d'action personnalisé, vous devez spécifier deux fonctions Lambda pour l'étape à exécuter, une dans chacune des régions du plan.
- Vous pouvez configurer la région dans laquelle vous souhaitez que le Lambda s'exécute, par exemple, dans la région d'activation ou dans la région de désactivation. Toutefois, si vous exécutez dans la région de désactivation, vous devenez dépendant de cette région. Nous vous déconseillons de devenir dépendant de la région de désactivation.

Ce bloc prend en charge les modes d'exécution gracieux et disgracieux. En mode d'exécution peu élégant, Region Switch ignore l'étape du bloc d'exécution Lambda.

Ce qui est évalué dans le cadre de l'évaluation du plan

Lorsque Region Switch évalue votre plan, Region Switch effectue plusieurs vérifications sur la configuration et les autorisations de votre bloc d'exécution Lambda. Le changement de région vérifie que les informations suivantes sont correctes :

- Les fonctions Lambda spécifiées dans la configuration existent.
- Les paramètres de simultanéité des fonctions Lambda ne sont pas limités, notamment en vérifiant les points suivants :
  - La simultanéité n'est pas définie sur 0.
  - Au moins une exécution simultanée est disponible, ou cette simultanéité non réservée existe.

Le commutateur de région exécute une exécution à sec de la fonction Lambda pour valider les paramètres et les autorisations spécifiés, sans exécuter la logique de la fonction elle-même. Les coûts Lambda standard sont encourus lorsque vous effectuez un essai à sec.

Le changement de région valide également que le rôle IAM du plan dispose des autorisations requises pour l'exécution de Lambda. Pour plus d'informations sur les autorisations requises pour les blocs d'exécution de commutateurs régionaux, consultezExemples de politiques basées sur l'identité pour le changement de région dans ARC.

Les autorisations IAM correctes sont essentielles au bon fonctionnement du bloc d'exécution Lambda. Si l'une de ces validations échoue, Region Switch renvoie des avertissements indiquant la présence de problèmes et fournit des messages d'erreur spécifiques pour vous aider à résoudre les problèmes d'autorisation ou de configuration. Cela garantit que votre plan dispose de l'accès nécessaire pour gérer et interagir avec le Lambda lorsque cette étape s'exécute pendant l'exécution d'un plan.

Bloc d'exécution du contrôle de santé Amazon Route 53

Le bloc d'exécution du bilan de santé d'Amazon Route 53 vous permet de spécifier les régions vers lesquelles le trafic de votre application sera redirigé lors du basculement. Le bloc d'exécution crée des bilans de santé Amazon Route 53, que vous associez ensuite aux enregistrements DNS Route 53 de votre compte. Lorsque vous exécutez votre plan de changement de région, l'état du bilan de santé de Route 53 est mis à jour et le trafic est redirigé en fonction de votre configuration DNS.

> **Important**
>
> La zone hébergée Route 53 doit se trouver dans la même partition que le plan de changement de région.

Configuration

Pour configurer un bloc d'exécution du contrôle de santé Route 53, entrez les valeurs suivantes.

> **Important**
>
> Avant de configurer le bloc d'exécution, assurez-vous que vous avez mis en place la bonne stratégie IAM. Pour de plus amples informations, veuillez consulter Exemple de politique de bloc d'exécution du bilan de santé Route 53.

1. Nom de l'étape : entrez un nom.
2. Description de l'étape (facultatif) : entrez une description de l'étape.

3. ID de zone hébergée : ID de zone hébergée pour votre domaine et vos enregistrements DNS dans Route 53.
4. Nom de l'enregistrement : entrez le nom de l'enregistrement (nom de domaine) pour les enregistrements que vous utilisez, avec les contrôles de santé associés, pour rediriger le trafic vers votre application. Le changement de région trouvera les ensembles d'enregistrements Route 53 pour le nom de l'enregistrement et tentera de mapper chaque ensemble d'enregistrements à une région, en fonction du nom de région figurant dans la valeur ou l'identifiant d'ensemble du jeu d'enregistrements.
5. Identifiants du jeu d'enregistrements (facultatif) : vous avez la possibilité de fournir manuellement les identifiants du jeu d'enregistrements si le changement de région ne peut pas automatiquement mapper les ensembles d'enregistrements aux régions à partir du nom d'enregistrement fourni à l'étape 4 une fois que vous avez créé le plan. Si l'évaluation du plan renvoie un avertissement indiquant que des informations supplémentaires sont requises, mettez à jour votre plan avec des identifiants records en incluant les éléments suivants pour chaque région :
   - Identifiant du jeu d'enregistrements : entrez l'identifiant du set ou la valeur/route du trafic pour le set d'enregistrements.
   - Région : entrez la région associée au jeu d'enregistrements contenant les informations d'identification du jeu d'enregistrements.
6. Choisissez Enregistrer l'étape.
7. Configurez les contrôles de santé dans Route 53.

   Le commutateur de région fournit un identifiant de contrôle de santé, pour chaque région, pour chaque nom d'enregistrement au sein d'une zone hébergée définie dans le bloc d'exécution. Assurez-vous de configurer les contrôles de santé pour les ensembles d'enregistrements correspondants de votre compte dans Route 53 afin que le changement de région puisse rediriger correctement le trafic vers votre application pendant l'exécution du plan. Dans l'onglet Health checks de la page des détails du plan, vous pouvez consulter les bilans de santé de tous les blocs d'exécution et de toutes les régions.

Comment ça marche

Vous ajoutez une étape de vérification de l'état à votre flux de travail de changement de région afin de pouvoir rediriger le trafic vers une région secondaire, pour les active/passive configurations, ou hors d'une région désactivée, pour les active/active configurations. Si vous ajoutez plusieurs flux de travail à votre plan, fournissez les mêmes valeurs de configuration pour tous les blocs d'exécution des contrôles de santé qui utilisent les mêmes enregistrements DNS.

Sur la base des informations que vous fournissez lorsque vous configurez le bloc d'exécution, Region Switch tente de déterminer le jeu d'enregistrements correct pour chaque région de votre plan. Généralement, l'ID de zone hébergée et le nom de l'enregistrement sont des informations suffisantes pour déterminer les ensembles d'enregistrements et les régions associées. Dans le cas contraire, lorsque Region Switch exécute son évaluation automatique du plan après avoir créé le plan, un avertissement est renvoyé pour vous informer que des informations supplémentaires sont nécessaires.

Le commutateur de région envoie des bilans de santé pour chaque bloc d'exécution du bilan de santé Route 53. Pour les plans qui utilisent une approche de active/passive reprise, le bilan de santé de la région principale commence comme étant sain, et le bilan de santé de la région de secours est initialement défini comme non sain. Pour les plans qui utilisent l'approche du active/active rétablissement, les bilans de santé pour toutes les régions commencent par un état de santé sain.

Pour permettre à Region Switch d'exécuter correctement ce bloc d'exécution pour votre plan, vous devez ajouter les contrôles de santé à vos enregistrements DNS.

Pour un active/active plan, l'étape d'exécution fonctionne de la manière suivante :

- Lorsqu'un flux de travail de désactivation s'exécute pour une région, le bilan de santé est défini sur « non fonctionnel » et le trafic n'est plus dirigé vers la région.
- Lorsqu'un flux de travail d'activation est exécuté pour une région, le bilan de santé est réglé sur sain et le trafic est acheminé vers la région.

Pour un active/passive plan, l'étape d'exécution fonctionne de la manière suivante :

- Lorsqu'un flux de travail d'activation s'exécute pour une région, le bilan de santé de cette région est défini sur sain et le trafic est acheminé vers la région. Dans le même temps, le bilan de santé de l'autre région du plan est défini comme étant insalubre et les arrêts de circulation sont dirigés vers cette région.

Ce qui est évalué dans le cadre de l'évaluation du plan

Lorsque Region Switch évalue votre plan, Region Switch effectue plusieurs vérifications sur la configuration et les autorisations du bloc d'exécution du bilan de santé Route 53. Le changement de région vérifie que les contrôles de santé sont attachés aux enregistrements DNS spécifiés dans la configuration du bloc d'exécution. En d'autres termes, le changement de région vérifie que les

enregistrements DNS d'une région spécifique Région AWS sont configurés pour utiliser des contrôles de santé pour cette région.

Comparaison des contrôles de routage ARC et des blocs d'exécution des contrôles de santé Route 53

Le bloc d'exécution du contrôle de santé Amazon Route 53 dans Region Switch constitue une alternative moins coûteuse pour la gestion du trafic basée sur le DNS. Toutefois, ce bloc d'exécution dépend de la région Région AWS que vous activez, de sorte que cette région doit être disponible. Cela répond aux besoins de la plupart des clients, car ils activent une région saine.

Les contrôles de routage ARC fournissent une gestion du trafic hautement fiable basée sur le DNS avec un SLA de disponibilité à 100 %. Grâce aux contrôles de routage, vos équipes opérationnelles peuvent transférer le trafic entre les régions à l'aide de glissières de sécurité. Les contrôles de routage fournissent une solution à locataire unique avec un SLA de 100 %. Un cluster de contrôle de routage est réparti sur cinq régions et peut tolérer que deux régions soient hors ligne. Si vous avez des applications très critiques, pensez à utiliser des contrôles de routage.

Les contrôles de routage ne sont pas nécessaires pour utiliser le changement de région. Vous pouvez utiliser le commutateur de région pour gérer la redirection du trafic en utilisant les blocs d'exécution des contrôles de santé de Route 53 sans contrôles de routage.

Les contrôles de routage ajoutent de la valeur avec le changement de région dans les situations suivantes :

- Vous avez besoin du SLA de disponibilité à 100 % pour le mécanisme de contrôle du trafic lui-même.
- Votre entreprise a besoin de contrôles opérationnels manuels assortis de règles de sécurité pour les applications critiques.
- Vous voulez defense-in-depth que les équipes opérationnelles puissent annuler manuellement le routage automatique du trafic si nécessaire.

Les blocs d'exécution du bilan de santé de Route 53 ne dépendent pas du plan de contrôle. Les modifications apportées aux dossiers de contrôle de santé utilisent le plan de données, de sorte qu'elles ne nécessitent pas la région d'activation pour traiter les mises à jour de configuration. Les blocs d'exécution du bilan de santé Route 53 sont suffisants dans les situations suivantes :

- Votre application peut dépendre de Région AWS celle que vous activez.

- La redirection automatique du trafic dans le cadre du processus de restauration répond à vos exigences.
- L'optimisation des coûts est une priorité. Les blocs d'exécution des contrôles de santé Route 53 sont moins coûteux que les contrôles de routage.

La plupart des clients commencent par utiliser les blocs d'exécution des contrôles d'état de Route 53 comme mécanisme de routage du trafic par défaut et ajoutent des contrôles de routage uniquement pour leurs applications les plus critiques qui nécessitent le plus haut niveau de fiabilité pour le mécanisme de gestion du trafic.

Créez des plans pour enfants

Pour prendre en charge des scénarios de reprise plus complexes, vous pouvez créer des plans enfants en les ajoutant à l'aide de blocs d'exécution du plan de changement de région. La hiérarchie est limitée à deux niveaux, mais un plan parental peut inclure plusieurs forfaits pour enfants.

> **Important**
>
> Avant de créer un forfait enfant, assurez-vous d'avoir mis en place la bonne politique IAM. Pour de plus amples informations, veuillez consulter Exemple de politique de bloc d'exécution d'un plan de changement de région.

Pour des raisons de compatibilité, les forfaits pour enfants doivent prendre en charge toutes les régions prises en charge par le plan parent. De plus, l'approche de rétablissement, active active/active ou passive, doit être la même pour les plans parents-enfants.

Gardez à l'esprit les manières suivantes selon lesquelles un forfait enfant répond aux modifications que vous apportez à un plan parental et aux scénarios du plan parental.

- Un bloc d'exécution parent est marqué comme terminé lorsque tous les plans enfants et les autres blocs d'exécution qu'il contient sont terminés.
- Si une étape échoue dans un plan enfant, le bloc d'exécution du plan de changement de région échoue dans le plan parent.
- Les actions de contrôle initiées dans le plan parent lors de l'étape de changement de région, telles qu'une pause, un changement progressif ou abusif ou une annulation, sont automatiquement tentées sur le plan enfant, quelle que soit l'étape actuelle du plan enfant.

- Les opérations de saut ont un comportement particulier : le plan parent est ignoré, mais le plan enfant continue de s'exécuter.
- Si un plan enfant est déjà en cours d'exécution dans un bloc de commutation régional, afin de déterminer s'il continue de fonctionner, le changement de région évalue la compatibilité du plan enfant avec le plan parent. Si la configuration du plan enfant correspond aux exigences du plan parent, Region Switch traite le plan enfant comme s'il avait été initié par le plan parent.
- L'étape du plan parent échouera si le plan enfant est exécuté avec des paramètres de configuration incompatibles, tels que les suivants :
  - Le plan pour enfants fonctionne dans une autre région
  - Le plan enfant exécute une opération de désactivation lorsque le commutateur de région s'attend à ce qu'il exécute une opération d'activation
- Si le plan enfant se termine avec succès pendant une période pendant laquelle un plan parent est suspendu, le plan parent sera couronné de succès lorsque le plan parent reprendra.

Créer un déclencheur pour un plan de changement de région

Si vous souhaitez automatiser la restauration de votre application dans Region Switch, vous pouvez créer un ou plusieurs déclencheurs pour votre plan de changement de région. Les déclencheurs commencent automatiquement à exécuter un plan de changement de région, en fonction des conditions CloudWatch d'alarme que vous choisissez.

Pour créer un déclencheur pour un plan de changement de région

1. Après avoir créé un plan, sur la page des détails du plan, sélectionnez l'onglet Déclencheurs.
2. Choisissez Gérer les déclencheurs.
3. Sélectionnez les flux de travail dont vous souhaitez automatiser l'exécution, puis choisissez Ajouter un déclencheur.
4. Fournissez une description du déclencheur.
5. Sélectionnez une CloudWatch alarme, puis sélectionnez jusqu'à 10 CloudWatch alarmes pour créer les conditions du déclenchement.

   Lorsque vous sélectionnez plusieurs conditions, toutes les conditions doivent être remplies avant que l'exécution automatique du plan ne commence.

Le déclencheur lance l'exécution du plan lorsqu'une CloudWatch alarme passe aux conditions requises pour le déclenchement. Lorsque le déclencheur est ajouté au plan, si les conditions sont déjà remplies, le plan ne s'exécute pas, ce qui empêche les événements de basculement involontaires.

Exécuter un plan de changement de région pour récupérer une application

Pour récupérer une application lorsqu'elle Région AWS est défectueuse, vous devez exécuter un plan de changement de région dans Amazon Application Recovery Controller (ARC).

- Si votre application est déployée selon une active/active approche, les flux de travail de votre plan désactivent la région affectée afin que votre autre région active soit correctement dimensionnée et commence à recevoir tout le trafic de votre application.
- Si votre application est déployée selon une active/passive approche, les flux de travail de votre plan désactivent la région affectée et activent votre région de secours, en y augmentant vos ressources, si nécessaire, et en redirigeant le trafic de votre application vers la région de secours.

Pour restaurer une application manuellement, exécutez votre plan de changement de région en procédant comme suit.

Une autre option consiste à déclencher automatiquement une exécution avec des CloudWatch alarmes Amazon spécifiques que vous spécifiez pour démarrer l'exécution d'un plan. Vous pouvez spécifier des déclencheurs pour l'exécution du plan lorsque vous créez ou mettez à jour un plan. Pour de plus amples informations, veuillez consulter Créer un déclencheur pour un plan de changement de région.

Pour exécuter un plan de changement de région

1. Dans le AWS Management Console, accédez à celui Région AWS que vous souhaitez activer pour votre application.
2. Sur la console Amazon Application Recovery Controller (ARC), choisissez Region Switch, puis sélectionnez le plan que vous souhaitez exécuter.
3. Choisissez Execute plan.
4. Si votre plan inclut des étapes d'approbation manuelles, approuvez chaque étape lorsque vous y êtes invité.

Pendant l'exécution d'un plan, vous pouvez suivre sa progression sur la page des détails de l'exécution, qui s'ouvre lorsque vous choisissez d'exécuter un plan.

Vous pouvez également consulter les informations relatives à la restauration des applications en cours sur les tableaux de bord des changements de région. Sur la console de changement de région, dans le menu de navigation de gauche, sous Changement de région, choisissez l'une des options suivantes :

- Tableau de bord mondial
- Exécutions dans le nom de la région

Sachez que, s'il y a des déficiences dans une région, le tableau de bord mondial risque de ne pas afficher toutes les données de votre plan. Pour cette raison, nous vous recommandons de vous fier uniquement au tableau de bord des exécutions régionales lors d'événements opérationnels. Le tableau de bord des exécutions régionales est plus résilient car il utilise le plan de données du commutateur régional local.

Lorsque l'exécution du plan est terminée, vous pouvez voir des informations sur l'exécution du plan, ainsi que sur les autres plans exécutés par Region Switch, sur la page Détails du plan dans l'onglet Historique de l'exécution du plan.

Tableaux de bord de changement de région

Le changement de région inclut un tableau de bord global que vous pouvez utiliser pour observer l'état des plans de changement de région au sein de votre organisation et des régions. Le changement de région dispose également d'un tableau de bord des exécutions régionales qui affiche uniquement les exécutions de plans dans la région à laquelle vous êtes actuellement connecté AWS Management Console.

Sachez que, s'il y a des déficiences dans une région, le tableau de bord mondial risque de ne pas afficher toutes les données de votre plan. Pour cette raison, nous vous recommandons de vous fier uniquement au tableau de bord des exécutions régionales lors d'événements opérationnels. Le tableau de bord des exécutions régionales est plus résilient car il utilise le plan de données du commutateur régional local.

Pour ouvrir le tableau de bord global du changement de région

1. Ouvrez la console ARC à l'adressehttps://console.aws.amazon.com/route53recovery/home#/dashboard.

2. Sous Changer de région, choisissez Tableau de bord global.

Pour ouvrir le tableau de bord régional, changez de région

1. Ouvrez la console ARC à l'adressehttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Sous Changer de région, choisissez Tableau de bord régional.

Support multicompte lors du changement de région

Dans le changement de région, vous pouvez ajouter des ressources provenant d'autres comptes à vos plans. Vous pouvez également partager un plan de changement de région avec d'autres comptes. Pour plus d'informations, consultez les sections suivantes.

Ressources multi-comptes

Le changement de région permet d'héberger les ressources dans un compte distinct du compte contenant le plan de changement de région. Lorsque le changement de région exécute un plan, il assume le rôle ExecutionRole. Si le plan utilise des ressources provenant d'un compte différent de celui qui héberge le plan, le commutateur de région utilise le ExecutionRole pour assumer le rôle d'accès crossAccountRole à ces ressources.

Chaque ressource du plan de changement de région comporte deux champs facultatifs : crossAccountRole et ExternalId.

- crossAccountRole: Ce rôle permet d'accéder aux ressources d'un compte différent de celui qui héberge le plan de changement de région. Le rôle n'a besoin que d'autorisations pour agir sur les ressources de son compte ; il n'a pas besoin d'autorisations pour agir sur les ressources du compte qui héberge le plan de changement de région.
- ExternalId: il s'agit de l'ID externe STS issu de la politique de confiance du compte qui contient la ressource nécessitant une action. Il s'agit d'une chaîne alphanumérique qui constitue le secret partagé entre les deux comptes.

Partage de forfaits de changement de région

Le changement de région s'intègre à AWS Resource Access Manager (AWS RAM) pour vous permettre de partager des plans entre plusieurs Comptes AWS. Lorsque vous partagez un plan,

les comptes que vous spécifiez peuvent consulter les détails du plan, exécuter le plan et voir les exécutions du plan, ce qui permet un contrôle et une flexibilité accrus des capacités de restauration entre les différentes équipes.

Pour commencer à utiliser le partage entre comptes dans Region Switch, vous devez créer un partage de ressources dans AWS RAM. Le partage des ressources indique les participants autorisés à partager le plan associé à votre compte. Les participants peuvent consulter et exécuter le plan partagé via la console, la CLI ou AWS SDKs.

Important : vous Compte AWS devez être propriétaire des forfaits que vous souhaitez partager. Vous ne pouvez pas partager un plan qui a été partagé avec vous. Pour partager un plan avec votre organisation ou avec une unité organisationnelle AWS Organizations, vous devez activer le partage avec les Organizations.

Pour plus d'informations sur AWS RAM, voirSupport du partage des plans entre les comptes pour le changement de région ARC.

Support du partage des plans entre les comptes pour le changement de région ARC

Amazon Application Recovery Controller (ARC) 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 le changement de région ARC, vous pouvez partager le plan de changement de région. (Pour utiliser les ressources d'un autre compte dans votre plan, vous utilisez un rôle CrossAccount. Pour en savoir plus, consultezRessources multi-comptes.)

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 utilisant AWS Resource Access Manager pour partager des plans entre des comptes dans ARC, vous pouvez utiliser un plan avec plusieurs plans différents Comptes AWS. Lorsque vous choisissez

de partager un plan, un autre plan Comptes AWS que vous spécifiez peut exécuter le plan pour effectuer la restauration de l'application.

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 (OUs) dans AWS Organizations, en utilisant des rôles et des utilisateurs IAM. AWS RAM est un moyen centralisé et contrôlé de partager un plan.

Lorsque vous partagez un plan, vous pouvez réduire le nombre total de plans dont votre organisation a besoin. Avec un plan partagé, vous pouvez répartir le coût total de l'exécution du plan entre différentes équipes, afin de maximiser les avantages de l'ARC à moindre coût. Le partage de plans entre comptes peut également faciliter le processus d'intégration de plusieurs applications dans 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 ARC, vous devez créer un partage de ressources dans n. AWS RAM Le partage des ressources indique les participants autorisés à partager le plan associé à votre compte.

Cette rubrique explique comment partager les ressources que vous possédez et comment utiliser les ressources qui sont partagées avec vous.

Table des matières

Conditions préalables au partage de plans

- Pour partager un plan, vous devez le posséder dans votre Compte AWS. Cela signifie que la ressource doit être allouée ou provisionnée dans votre compte. Vous ne pouvez pas partager un plan qui a été partagé avec vous.

- Pour partager un plan avec votre organisation ou une unité organisationnelle dans 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 plan

Lorsque vous partagez un plan, les participants que vous désignez pour le partager peuvent consulter et, si vous accordez des autorisations supplémentaires, exécuter le plan.

Pour partager un plan, vous devez l'ajouter à un partage de ressources. Un partage de ressources est une ressource AWS RAM qui vous permet de partager vos ressources entre des Comptes AWS. Un partage de ressources indique les ressources à partager et les participants avec lesquels elles sont partagées. Pour partager un plan, 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 les opérations AWS RAM d'API avec le AWS Command Line Interface ou AWS SDKs.

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 plan partagé. Dans le cas contraire, les participants reçoivent une invitation à rejoindre le partage des ressources et ont accès au plan partagé après avoir accepté l'invitation.

Vous pouvez partager un plan dont vous êtes propriétaire en utilisant la AWS RAM console ou en utilisant des opérations d' AWS RAM API avec le AWS CLI ou SDKs.

Pour partager un forfait 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 forfait dont vous êtes propriétaire à l'aide du AWS CLI

Utilisez la commande create-resource-share.

Octroi d'autorisations pour partager des forfaits

Le partage de plans entre comptes nécessite les autorisations supplémentaires suivantes pour que le principal IAM partage le plan en utilisant AWS RAM :

```
# read and execute plan permissions
```

```
"arc-region-switch:GetPlan",
"arc-region-switch:GetPlanInRegion",
"arc-region-switch:GetPlanExecution",
"arc-region-switch:ListPlanExecutionEvents",
"arc-region-switch:ListPlanExecutions",
"arc-region-switch:ListRoute53HealthChecks",
"arc-region-switch:GetPlanEvaluationStatus",
"arc-region-switch:StartPlanExecution",
"arc-region-switch:CancelPlanExecution",
"arc-region-switch:UpdatePlanExecution",
"arc-region-switch:UpdatePlanExecutionStep"
```

Le propriétaire qui partage le plan doit disposer des autorisations suivantes. Si vous tentez de partager un plan AWS RAM sans disposer de ces autorisations, une erreur est renvoyée.

```
"arc-region-switch:PutResourcePolicy" # Permission only apis
"arc-region-switch:DeleteResourcePolicy" # Permission only apis
"arc-region-switch:GetResourcePolicy" # Permission only apis
```

Pour plus d'informations sur le mode d' AWS Resource Access Manager utilisation de l'IAM, voir Comment AWS Resource Access Manager utilise l'IAM dans le guide de l'AWS RAM utilisateur.

Annulation du partage d'un forfait partagé

Lorsque vous annulez le partage d'un plan, les règles suivantes s'appliquent aux participants et aux propriétaires :

- Les participants ne peuvent plus consulter ni exécuter le plan non partagé.

Pour annuler le partage d'un plan partagé dont vous êtes 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 le AWS CLI ou SDKs.

Pour annuler le partage d'un forfait 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 forfait partagé dont vous êtes propriétaire à l'aide du AWS CLI

Utilisez la commande disassociate-resource-share.

Identification d'un plan partagé

Les propriétaires et les participants peuvent identifier les plans partagés en consultant les informations dans AWS RAM. Ils peuvent également obtenir des informations sur les ressources partagées à l'aide de la console 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 plan en consultant les informations dans AWS Management Console ou en utilisant les opérations AWS Command Line Interface de l'API ARC.

Pour déterminer si un plan dont vous êtes propriétaire est partagé à l'aide de la console

Sur la AWS Management Console page de détails d'un plan, consultez l'état du partage du plan.

En tant que participant, lorsqu'un plan est partagé avec vous, vous devez généralement accepter le partage afin de pouvoir accéder au plan.

Responsabilités et autorisations pour les forfaits partagés

Autorisations accordées aux propriétaires

Les participants peuvent consulter ou exécuter le plan (s'ils disposent des autorisations appropriées).

Autorisations pour les participants

Lorsque vous partagez un plan que vous possédez avec d'autres personnes Comptes AWS, les participants peuvent consulter ou exécuter le plan (s'ils disposent des autorisations appropriées).

Lorsque vous partagez un plan en utilisant AWS RAM, un participant dispose, par défaut, d'autorisations en lecture seule. Pour consulter la liste des autorisations en lecture seule pour le changement de région, voir. Autorisations en lecture seule Les participants ont besoin d'autorisations

supplémentaires pour exécuter un plan de changement de région. Les participants qui doivent exécuter des plans ont besoin d'autorisations supplémentaires. Sachez que vous ne pouvez pas autoriser un AWS RAM participant pour les opérations suivantes :

- `ApprovePlanExecutionStep`
- `UpdatePlan`

Frais de facturation

Le propriétaire d'un plan dans ARC est facturé pour les coûts associés au plan. La création de ressources hébergées dans un plan n'entraîne aucun coût supplémentaire, pour les propriétaires de plans ou pour les participants.

Pour obtenir des informations détaillées sur les tarifs et des exemples, consultez la section Tarification d'Amazon Application Recovery Controller (ARC).

Quotas

Toutes les ressources créées dans un plan partagé sont prises en compte dans les quotas du propriétaire du plan.

Pour obtenir la liste des quotas des plans de changement de région, voirQuotas pour le changement de région.

Identity and Access Management pour le changement de région dans ARC

Gestion des identités et des accès AWS (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. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Table des matières

Comment fonctionne le changement de région dans ARC avec IAM

Avant d'utiliser IAM pour gérer l'accès à ARC, découvrez quelles fonctionnalités IAM peuvent être utilisées avec ARC.

Avant d'utiliser IAM pour gérer l'accès au changement de région dans Amazon Application Recovery Controller (ARC), découvrez quelles fonctionnalités IAM peuvent être utilisées avec le changement de région.

Fonctionnalités IAM que vous pouvez utiliser avec le changement de région dans Amazon Application Recovery Controller (ARC)

Fonctionnalité IAM	Support de changement de région
Politiques basées sur l’identité	Oui
Politiques basées sur les ressources	Oui
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition de politique	Oui
ACLs	Oui
ABAC (étiquettes dans les politiques)	Oui
Informations d’identification temporaires	Oui
Autorisations de principal	Oui
Rôles 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 le changement de région

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 Définition d'autorisations IAM personnalisées avec des politiques gérées par le client 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. 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 ARC, consultez. Exemples de politiques basées sur l'identité dans Amazon Application Recovery Controller (ARC)

Politiques basées sur les ressources dans le cadre du changement de région

Prend en charge les politiques basées sur les ressources : oui

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Par exemple, les politiques de confiance de rôle IAM et les politiques de compartiment Amazon S3 sont des politiques basées sur les ressources. 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 région

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

Les actions politiques dans ARC pour le changement de région utilisent les préfixes suivants avant l'action :

```
arc-region-switch
```

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

```
"Action": [
      "arc-region-switch:action1",
      "arc-region-switch: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-region-switch:Describe*"
```

Pour voir des exemples de politiques basées sur l'identité ARC pour le changement de région, voir. Exemples de politiques basées sur l'identité pour le changement de région dans ARC

Ressources politiques pour le changement de région

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. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

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

Pour voir des exemples de politiques basées sur l'identité ARC pour le changement de région, voir. Exemples de politiques basées sur l'identité pour le changement de région dans ARC

Clés de conditions de politique pour le changement de région

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` indique à quel moment les instructions s'exécutent en fonction de critères définis. 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. 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 voir des exemples de politiques basées sur l'identité ARC pour le changement de région, voir. Exemples de politiques basées sur l'identité pour le changement de région dans ARC

Listes de contrôle d'accès (ACLs) dans le commutateur de région

Supports ACLs : Oui

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLs 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 commutateur de région

Prise en charge d'ABAC (balises dans les politiques) : Oui

Le contrôle d'accès par attributs (ABAC) est une stratégie d'autorisation qui définit les autorisations en fonction des attributs appelés balises. Vous pouvez associer des balises aux entités et aux AWS ressources IAM, puis concevoir des politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de la ressource.

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 ABAC, consultez Définition d'autorisations avec l'autorisation 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.

Utilisation d'informations d'identification temporaires avec le changement de région

Prend en charge les informations d'identification temporaires : oui

Les informations d'identification temporaires fournissent un accès à court terme aux AWS ressources et sont automatiquement créées lorsque vous utilisez la fédération ou que vous changez de rôle. 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 et Services AWS compatibles avec IAM dans le Guide de l'utilisateur IAM.

Autorisations principales interservices pour le changement de région

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 des autorisations nécessaires pour effectuer les deux actions.

Rôles de service pour le changement de région

Prend en charge les rôles de service : Non

Un rôle de service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer un rôle de service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.

Rôles liés au service pour le changement de région

Prend en charge les rôles liés à un service : non

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 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 de région dans ARC

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier des ressources ARC. 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.

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 IAM (console) dans le Guide de l’utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par ARC, y compris le ARNs format de chaque type de ressource, consultez la section Actions, ressources et clés de condition pour Amazon Application Recovery Controller (ARC) 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 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.

- Accordez 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 d'IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utilisez 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 CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez l'Analyseur d'accès IAM pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : l'Analyseur d'accès IAM 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 politiques avec 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 la MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Sécurisation de l'accès aux API avec 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.

Politique de confiance relative aux rôles d'exécution du plan

Il s'agit de la politique de confiance requise pour le rôle d'exécution du plan, afin que l'ARC puisse exécuter un plan de changement de région.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "arc-region-switch.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Autorisations d'accès complètes

La politique IAM suivante accorde un accès complet à tous les changements de région : APIs

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "arc-region-switch.amazonaws.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "arc-region-switch:CreatePlan",
        "arc-region-switch:UpdatePlan",
        "arc-region-switch:GetPlan",
        "arc-region-switch:ListPlans",
```

```
        "arc-region-switch:DeletePlan",
        "arc-region-switch:GetPlanInRegion",
        "arc-region-switch:ListPlansInRegion",
        "arc-region-switch:ApprovePlanExecutionStep",
        "arc-region-switch:GetPlanEvaluationStatus",
        "arc-region-switch:GetPlanExecution",
        "arc-region-switch:StartPlanExecution",
        "arc-region-switch:CancelPlanExecution",
        "arc-region-switch:ListRoute53HealthChecks",
        "arc-region-switch:ListRoute53HealthChecksInRegion",
        "arc-region-switch:ListPlanExecutions",
        "arc-region-switch:ListPlanExecutionEvents",
        "arc-region-switch:ListTagsForResource",
        "arc-region-switch:TagResource",
        "arc-region-switch:UntagResource",
        "arc-region-switch:UpdatePlanExecution",
        "arc-region-switch:UpdatePlanExecutionStep"
      ],
      "Resource": "*"
    }
  ]
}
```

Autorisations en lecture seule

La politique IAM suivante accorde des autorisations d'accès en lecture seule pour le changement de région :

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "arc-region-switch:GetPlan",
        "arc-region-switch:ListPlans",
        "arc-region-switch:GetPlanInRegion",
        "arc-region-switch:ListPlansInRegion",
        "arc-region-switch:GetPlanEvaluationStatus",
        "arc-region-switch:GetPlanExecution",
```

```
        "arc-region-switch:ListRoute53HealthChecks",
        "arc-region-switch:ListRoute53HealthChecksInRegion",
        "arc-region-switch:ListPlanExecutions",
        "arc-region-switch:ListPlanExecutionEvents",
        "arc-region-switch:ListTagsForResource"
      ],
      "Resource": "*"
    }
  ]
}
```

Autorisations de blocage d'exécution

Les sections suivantes fournissent des exemples de politiques IAM qui fournissent les autorisations requises pour des blocs d'exécution spécifiques que vous ajoutez à un plan de changement de région.

Table des matières

Exemple de politique d'exécution par blocs d'EC2 Auto Scaling

Voici un exemple de politique à appliquer si vous ajoutez des blocs d'exécution à un plan de changement de région pour les groupes EC2 Auto Scaling.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "autoscaling:DescribeAutoScalingGroups"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "autoscaling:UpdateAutoScalingGroup"
      ],
      "Resource": [
        "arn:aws:autoscaling:us-
east-1:123456789012:autoScalingGroup:123d456e-123e-1111-abcd-
EXAMPLE22222:autoScalingGroupName/app-asg-primary",
        "arn:aws:autoscaling:us-
west-2:123456789012:autoScalingGroup:1234a321-123e-1234-aabb-
EXAMPLE33333:autoScalingGroupName/app-asg-secondary"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource": "*"
    }
  ]
}
```

Exemple de politique d'exécution du dimensionnement des ressources Amazon EKS

Voici un exemple de politique à appliquer si vous ajoutez des blocs d'exécution à un plan de changement de région pour le dimensionnement des ressources Amazon EKS.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "eks:DescribeCluster"
      ],
      "Resource": [
        "arn:aws:eks:us-east-1:123456789012:cluster/app-eks-primary",
        "arn:aws:eks:us-west-2:123456789012:cluster/app-eks-secondary"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "eks:ListAssociatedAccessPolicies"
      ],
      "Resource": [
        "arn:aws:eks:us-east-1:123456789012:access-entry/app-eks-primary/*",
        "arn:aws:eks:us-west-2:123456789012:access-entry/app-eks-secondary/*"
      ]
    }
  ]
}
```

Remarque : Outre cette politique IAM, le rôle d'exécution du plan doit être ajouté aux entrées d'accès du cluster Amazon EKS avec la politique `AmazonArcRegionSwitchScalingPolicy` d'accès. Pour de plus amples informations, veuillez consulter Configuration des autorisations d'accès à EKS.

Exemple de politique de mise à l'échelle des blocs d'exécution du service Amazon ECS

Voici un exemple de politique à appliquer si vous ajoutez des blocs d'exécution à un plan de changement de région pour le dimensionnement du service Amazon ECS.

JSON

```
{
```

```
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ecs:DescribeServices",
        "ecs:UpdateService"
      ],
      "Resource": [
        "arn:aws:ecs:us-east-1:123456789012:service/app-cluster-primary/app-
service",
        "arn:aws:ecs:us-west-2:123456789012:service/app-cluster-secondary/app-
service"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ecs:DescribeClusters"
      ],
      "Resource": [
        "arn:aws:ecs:us-east-1:123456789012:cluster/app-cluster-primary",
        "arn:aws:ecs:us-west-2:123456789012:cluster/app-cluster-secondary"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ecs:ListServices"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:RegisterScalableTarget"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "cloudwatch:GetMetricStatistics"
```

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

Exemple de politique de bloc d'exécution des contrôles de routage ARC

Remarque : Le bloc d'exécution des contrôles de routage Amazon ARC exige que toutes les politiques de contrôle des services (SCPs) appliquées au rôle d'exécution du plan autorisent l'accès aux régions suivantes pour ces services :

- `route53-recovery-control-config: us-west-2`
- `route53-recovery-cluster: us-west-2, us-east-1, eu-west-1, ap-southeast-2, ap-northeast-1`

Voici un exemple de politique à appliquer si vous ajoutez des blocs d'exécution à un plan de changement de région pour les contrôles de routage ARC.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "route53-recovery-control-config:DescribeControlPanel",
        "route53-recovery-control-config:DescribeCluster"
      ],
      "Resource": [
        "arn:aws:route53-recovery-control::123456789012:controlpanel/
abcd1234abcd1234abcd1234abcd1234",
        "arn:aws:route53-recovery-
control::123456789012:cluster/4b325d3b-0e28-4dcf-ba4a-EXAMPLE11111"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
```

```
        "route53-recovery-cluster:GetRoutingControlState",
        "route53-recovery-cluster:UpdateRoutingControlStates"
      ],
      "Resource": [
        "arn:aws:route53-recovery-
control::123456789012:controlpanel/1234567890abcdef1234567890abcdef/
routingcontrol/abcdef1234567890",
        "arn:aws:route53-recovery-
control::123456789012:controlpanel/1234567890abcdef1234567890abcdef/
routingcontrol/1234567890abcdef"
      ]
    }
  ]
}
```

Vous pouvez récupérer l'ID du panneau de commande de routage et l'ID du cluster à l'aide de la CLI. Pour de plus amples informations, veuillez consulter Configuration des composants de contrôle de routage.

Exemple de politique d'exécution de la base de données globale Aurora

Voici un exemple de politique à appliquer si vous ajoutez des blocs d'exécution à un plan de changement de région pour les bases de données Aurora.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "rds:DescribeGlobalClusters",
        "rds:DescribeDBClusters"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "rds:FailoverGlobalCluster",
```

```
        "rds:SwitchoverGlobalCluster"
      ],
      "Resource": [
        "arn:aws:rds::123456789012:global-cluster:app-global-db",
       "arn:aws:rds:us-east-1:123456789012:cluster:app-db-primary",
        "arn:aws:rds:us-west-2:123456789012:cluster:app-db-secondary"
      ]
    }
  ]
}
```

Exemple de politique d'exécution par blocs d'Amazon DocumentDB Global Cluster

Voici un exemple de politique à appliquer si vous ajoutez des blocs d'exécution à un plan de changement de région pour les clusters globaux Amazon DocumentDB.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "rds:DescribeGlobalClusters",
        "rds:DescribeDBClusters",
        "rds:FailoverGlobalCluster",
        "rds:SwitchoverGlobalCluster"
      ],
      "Resource": "*"
    }
  ]
}
```

Exemple de politique relative aux blocs d'exécution Amazon RDS

Voici un exemple de politique à joindre si vous ajoutez des blocs d'exécution à un plan de changement de région dans le cadre de la promotion de répliques de lecture Amazon RDS ou de la création de répliques entre régions.

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```
    {
      "Effect": "Allow",
      "Action": [
        "rds:DescribeDBInstances",
        "rds:PromoteReadReplica",
        "rds:CreateDBInstanceReadReplica",
        "rds:ModifyDBInstance"
      ],
      "Resource": "*"
    }
  ]
}
```

Exemple de politique d'exécution des approbations manuelles

Voici un exemple de politique à appliquer si vous ajoutez des blocs d'exécution à un plan de changement de région pour des approbations manuelles.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "arc-region-switch:ApprovePlanExecutionStep"
      ],
      "Resource": "arn:aws:arc-region-switch::123456789012:plan/sample-
plan:0123abc"
    }
  ]
}
```

Exemple de politique de bloc d'exécution Lambda pour les actions personnalisées

Voici un exemple de politique à appliquer si vous ajoutez des blocs d'exécution à un plan de changement de région pour les fonctions Lambda.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "lambda:GetFunction",
        "lambda:InvokeFunction"
      ],
      "Resource": [
        "arn:aws:lambda:us-east-1:123456789012:function:app-recovery-primary",
        "arn:aws:lambda:us-west-2:123456789012:function:app-recovery-secondary"
      ]
    }
  ]
}
```

Exemple de politique de bloc d'exécution du bilan de santé Route 53

Voici un exemple de politique à associer si vous ajoutez des blocs d'exécution à un plan de changement de région pour les bilans de santé de Route 53.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "route53:ListResourceRecordSets"
      ],
      "Resource": [
        "arn:aws:route53:::hostedzone/Z1234567890ABCDEFGHIJ"
      ]
    }
  ]
}
```

Exemple de politique de bloc d'exécution d'un plan de changement de région

Voici un exemple de politique à appliquer si vous ajoutez des blocs d'exécution à un plan de changement de région pour exécuter des plans enfants.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "arc-region-switch:StartPlanExecution",
        "arc-region-switch:GetPlanExecution",
        "arc-region-switch:CancelPlanExecution",
        "arc-region-switch:UpdatePlanExecution",
        "arc-region-switch:ListPlanExecutions"
      ],
      "Resource": [
        "arn:aws:arc-region-switch::123456789012:plan/child-plan-1/abcde1",
        "arn:aws:arc-region-switch::123456789012:plan/child-plan-2/fghij2"
      ]
    }
  ]
}
```

CloudWatch alarmes pour les autorisations relatives à l'état des applications

Voici un exemple de politique à associer aux CloudWatch alarmes d'accès relatives à l'état de santé des applications, qui sont utilisées pour déterminer le temps de restauration réel.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
```

```
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource": [
        "arn:aws:cloudwatch:us-east-1:123456789012:alarm:app-health-primary",
        "arn:aws:cloudwatch:us-west-2:123456789012:alarm:app-health-secondary"
      ]
    }
  ]
}
```

Autorisations relatives aux rapports d'exécution automatique du plan

Voici un exemple de politique à joindre si vous configurez la génération automatique de rapports pour un plan de changement de région. Cette politique inclut les autorisations permettant de rédiger des rapports sur Amazon S3, CloudWatch d'accéder aux données d'alarme et de récupérer les informations des forfaits enfants pour les forfaits parents.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::your-bucket-name/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmHistory"
      ],
      "Resource": [
        "arn:aws:cloudwatch:us-east-1:123456789012:alarm:app-health-primary"
        "arn:aws:cloudwatch:us-west-2:123456789012:alarm:app-health-secondary"
      ],
    },
    {
      "Effect": "Allow",
      "Action": [
        "arc-region-switch:GetPlanExecution",
        "arc-region-switch:ListPlanExecutionEvents"
```

```
      ],
      "Resource": [
        "arn:aws:arc-region-switch:us-east-1:123456789012:plan/child-plan-1/abcde1",
        "arn:aws:arc-region-switch:us-west-2:123456789012:plan/child-plan-2/fghij2"
      ],
    }
  ]
}
```

Remarque : Si vous configurez une AWS KMS clé gérée par le client pour le chiffrement du compartiment Amazon S3, vous devez également ajouter `kms:GenerateDataKey` des `kms:Encrypt` autorisations pour la clé.

Autorisations relatives aux ressources entre comptes

Si les ressources se trouvent dans des comptes différents, vous aurez besoin d'un rôle multicompte. Voici un exemple de politique de confiance pour un rôle multicompte.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:role/RegionSwitchExecutionRole"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "sts:ExternalId": "UniqueExternalId123"
        }
      }
    }
  ]
}
```

Et voici l'autorisation pour le rôle d'exécution du plan d'assumer ce rôle entre comptes :

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::987654321098:role/RegionSwitchCrossAccountRole",
      "Condition": {
        "StringEquals": {
          "sts:ExternalId": "UniqueExternalId123"
        }
      }
    }
  ]
}
```

Autorisations complètes des rôles d'exécution du plan

La création d'une politique complète incluant des autorisations pour tous les blocs d'exécution nécessiterait une politique assez large. En pratique, vous ne devez inclure des autorisations que pour les blocs d'exécution que vous utilisez dans vos plans spécifiques.

Voici un exemple de politique que vous pouvez utiliser comme point de départ pour une politique de rôle d'exécution de plan. Assurez-vous d'ajouter des politiques supplémentaires requises pour les blocs d'exécution spécifiques que vous incluez dans votre plan. N'incluez que les autorisations requises pour les blocs d'exécution spécifiques que vous utilisez dans votre plan, conformément au principe du moindre privilège

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iam:SimulatePrincipalPolicy",
```

```
            "Resource": "arn:aws:iam::123456789012:role/
RegionSwitchExecutionRole"
        },
        {
            "Effect": "Allow",
            "Action": [
                "arc-region-switch:GetPlan",
                "arc-region-switch:GetPlanExecution",
                "arc-region-switch:ListPlanExecutions"
            ],
            "Resource": "*"
        }
    ]
}
```

Journalisation et surveillance pour le changement de région dans ARC

Vous pouvez utiliser Amazon CloudWatch et Amazon EventBridge pour surveiller le changement de région dans Amazon Application Recovery Controller (ARC), afin de recevoir des alertes, d'analyser des modèles et de résoudre les problèmes. AWS CloudTrail

Rubriques

- Enregistrement des appels d'API de changement de région à l'aide AWS CloudTrail
- Utilisation du changement de région dans ARC avec Amazon EventBridge

Enregistrement des appels d'API de changement de région à l'aide AWS CloudTrail

Le commutateur de région Amazon Application Recovery Controller (ARC) est intégré à un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans ARC. AWS CloudTrail CloudTrail capture tous les appels d'API pour ARC sous forme d'événements. Les appels capturés incluent des appels provenant de la console ARC et des appels de code vers les opérations de l'API 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 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 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 ARC dans CloudTrail

CloudTrail est activé sur votre compte Compte AWS lorsque vous créez le compte. Lorsqu'une activité se produit dans 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 l'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 ARC sont enregistrées CloudTrail et documentées dans le lien de référence de l'API TBD. Par exemple, les appels au `TBD` `TBD` et les `TBD` 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 Gestion des identités et des accès AWS (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 de plus amples informations, veuillez consulter l'élément userIdentity CloudTrail .

Affichage des événements liés au changement de région dans l'historique des événements

CloudTrail vous permet de consulter les événements récents dans l'historique des événements. La plupart des événements liés aux demandes d'API de changement de région se produisent dans la région dans laquelle vous travaillez avec un plan de changement de région, par exemple, lorsque vous créez un plan ou que vous exécutez un plan. Toutefois, certaines actions de changement de région que vous exécutez dans la console ARC sont effectuées à l'aide des opérations de l'API du plan de contrôle, plutôt que des opérations du plan de données. Pour les opérations du plan de contrôle, vous pouvez consulter les événements dans l'est des États-Unis (Virginie du Nord). Pour savoir quels appels d'API sont des opérations du plan de contrôle, consultezOpérations de l'API de changement de région.

Comprendre les entrées du fichier journal ARC

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'`StartPlanExecution`action du changement de région.

```
{
    "eventVersion": "1.11",
    "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"
            },
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2025-07-06T17:38:05Z"
            }
        }
    },
    "eventTime": "2025-07-06T18:08:03Z",
    "eventSource": "arc-region-switch.amazonaws.com",
    "eventName": "StartPlanExecution",
    "awsRegion": "us-east-1",
    "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": {
        "planArn": "arn:aws:arc-region-switch::555555555555:plan/
CloudTrailIntegTestPlan:bbbbb",
        "targetRegion": "us-east-1",
        "action": "activate"    }
    "responseElements": {
        "executionId": "us-east-1/ddddddd EXAMPLE",
        "plan": "arn:aws:arc-region-switch::555555555555:plan/
CloudTrailIntegTestPlan:bbbbb",
        "planVersion": "1",
        "activateRegion": "us-east-1"    },
    "requestID": "fd42dcf7-6446-41e9-b408-d096example",
    "eventID": "4b5c42df-1174-46c8-be99-d67aexample",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management",
      "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "us-east-1.arc.amazon.aws"
}
```

Utilisation du changement de région dans ARC avec Amazon EventBridge

À l'aide d'Amazon EventBridge, vous pouvez configurer des règles basées sur les événements qui surveillent les ressources de votre changement de région dans Amazon Application Recovery Controller (ARC), 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 chaque fois qu'un plan de changement de région est terminé.

Vous pouvez créer des règles dans Amazon EventBridge pour agir sur les événements de changement de région ARC suivants :

- Exécution du plan de changement de région. L'événement indique qu'un plan de changement de région a été exécuté (exécuté).
- Évaluation du plan de changement de région. L'événement indique qu'une évaluation du plan de changement de région est terminée.

Pour capturer des événements ARC 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 transmis d'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 changement de région avec EventBridge

Avec EventBridge, vous pouvez créer des règles qui définissent les actions à entreprendre lorsque l'ARC émet des événements pour les ressources de changement de région.

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 de changement de région.

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. Région AWS Pour créer la règle, choisissez la région dans laquelle vous avez créé le plan pour lequel vous souhaitez surveiller les 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. Pour des exemples, reportez-vous à la section suivante.

Exemples de modèles de changement de région

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 l'ARC.

Les modèles d'événements suivants fournissent des exemples que vous pouvez utiliser EventBridge pour la fonctionnalité de changement de région dans ARC.

- Sélectionnez tous les événements dans Region Switch for PlanExecution.

```
{
    "source": [ "aws.arc-region-switch" ],
    "detail-type": [ "ARC Region switch Plan Execution" ]
}
```

- Sélectionnez tous les événements dans Region Switch for PlanEvaluation.

```
    {
    "source": [ "aws.arc-region-switch" ],
```

```
    "detail-type": [ "ARC Region Switch Plan Evaluation" ]
    }
```

Voici un exemple d'événement ARC pour l'exécution d'un plan de changement de région :

```
{
   "version": "0",
   "id": "1111111-bbbb-aaaa-cccc-dddddEXAMPLE", # Random uuid
   "detail-type": "ARC Region Switch Plan Execution",
   "source": "aws.arc-region-switch",
   "account": "111122223333",
   "time": "2023-11-16T23:38:14Z",
   "region": "us-east-1",
   "resources": ["arn:aws:arc-region-switch::111122223333:plan/aaaaaExample"], #
 planArn
   "detail": {
    "version": "0.0.1",
    "eventType": "ExecutionStarted",
    "executionId": "bbbbbbEXAMPLE",
    "executionAction": "activating/deactivating {region}",
    "idempotencyKey": "1111111-2222-3333-4444-5555555555", # As there is a possibility
 of dual logging
   }
}
```

Voici un exemple d'événement ARC pour l'exécution par étapes d'un plan de changement de région :

```
{
   "version": "0",
   "id": "1111111-bbbb-aaaa-cccc-dddddEXAMPLE", # Random uuid
   "detail-type": "ARC Region Switch Plan Execution",
   "source": "aws.arc-region-switch",
   "account": "111122223333",
   "time": "2023-11-16T23:38:14Z",
   "region": "us-east-1",
   "resources": ["arn:aws:arc-region-switch::111122223333:plan/aaaaaExample"], #
 planArn
   "detail": {
    "version": "0.0.1",
    "eventType": "StepStarted",
    "executionId": "bbbbbbEXAMPLE",
    "executionAction": "activating/deactivating {region}",
```

```
    "idempotencyKey": "1111111-2222-3333-4444-5555555555", # As there is a possibility
 of dual logging
    "stepDetails" : {
     "stepName": "Routing control step",
     "resource": ["arn:aws:route53-recovery-control::111122223333:controlpanel/
abcdefghiEXAMPLE/routingcontrol/jklmnopqrsEXAMPLE"]
    }
   }
}
```

Voici un exemple d'événement ARC pour un avertissement d'évaluation d'un plan de changement de région.

Pour l'évaluation d'un plan de changement de région, un événement est émis lorsqu'un avertissement est renvoyé. Si l'avertissement n'est pas effacé, un événement n'est émis pour l'avertissement qu'une fois toutes les 24 heures. Lorsque l'événement est effacé, aucun autre événement n'est émis pour cet avertissement.

```
{
   "version": "0",
   "id": "05d4d2d5-9c76-bfea-72d2-d4614802adb4", # Random uuid
   "detail-type": "ARC Region Switch Plan Execution",
   "source": "aws.arc-region-switch",
   "account": "111122223333",
   "time": "2023-11-16T23:38:14Z",
   "region": "us-east-1",
   "resources": ["arn:aws:arc-region-switch::111122223333:plan/a2b89be4821bfd1d"],
   "detail": {
     "version": "0.0.1",
     "idempotencyKey": "1111111-2222-3333-4444-5555555555",
     "metadata": {
        "evaluationTime" : "timestamp",
        "warning" : "There is a plan evaluation warning for arn:aws:arc-region-
switch::111122223333:plan/a2b89be4821bfd1d. Navigate to the Region switch console to
 resolve."
     }
   }
}
```

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 :

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
```

```
      "Action": [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "events.amazonaws.com",
          "delivery.logs.amazonaws.com"
        ]
      },
      "Resource": "arn:aws:logs:us-east-1:222222222222:log-group:/aws/events/
*:*",
      "Sid": "TrustEventsToStoreLogEvent"
    }
  ]
}
```

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 de préparation, voir Surveiller une ressource de vérification de l'état 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.

Quotas pour le changement de région

Le changement de région dans Amazon Application Recovery Controller (ARC) est soumis aux quotas suivants.

Entité	Quota
Nombre de plans par compte	10 Vous pouvez demander une augmentation de quota.
Nombre de blocs d'exécution par plan	100
Nombre de blocs d'exécution du plan de changement de région par plan	25
Nombre de blocs d'exécution en parallèle par étape	20
Nombre d' CloudWatch alarmes par condition de déclenchement	10

Exemples de code pour Application Recovery Controller utilisant AWS SDKs

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.

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

- Exemples de base pour l'utilisation d'Application Recovery Controller AWS SDKs
  - Actions pour Application Recovery Controller utilisant AWS SDKs
    - Utilisation GetRoutingControlState avec un AWS SDK
    - Utilisation UpdateRoutingControlState avec un AWS SDK

Exemples de base pour l'utilisation d'Application Recovery Controller AWS SDKs

Les exemples de code suivants montrent comment utiliser les bases d'Amazon Route 53 Application Recovery Controller avec AWS SDKs.

Exemples

- Actions pour Application Recovery Controller utilisant AWS SDKs
  - Utilisation GetRoutingControlState avec un AWS SDK
  - Utilisation UpdateRoutingControlState avec un AWS SDK

Actions pour Application Recovery Controller utilisant AWS SDKs

Les exemples de code suivants montrent comment effectuer des actions individuelles d'Application Recovery Controller avec AWS SDKs. Chaque exemple inclut un lien vers GitHub, où vous pouvez trouver des instructions pour configurer et exécuter le code.

Les exemples suivants incluent uniquement les actions les plus couramment utilisées. Pour obtenir la liste complète, consultez la Référence des API du contrôleur de récupération d'application Amazon Route 53.

Exemples

- Utilisation GetRoutingControlState avec un AWS SDK
- Utilisation UpdateRoutingControlState avec un AWS SDK

Utilisation **`GetRoutingControlState`** avec un AWS SDK

Les exemples de code suivants illustrent 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

Kit SDK for 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).

SAP ABAP

Kit SDK pour SAP ABAP

> **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.

```
    CONSTANTS cv_pfl TYPE /aws1/rt_profile_id VALUE 'ZCODE_DEMO'.
    DATA lo_exception TYPE REF TO /aws1/cx_rt_generic.
    DATA lo_session TYPE REF TO /aws1/cl_rt_session_base.
    DATA lo_client TYPE REF TO /aws1/if_r5v.
    DATA lt_endpoints TYPE TABLE OF string.
    DATA lv_endpoint TYPE string.
    DATA lv_region TYPE /aws1/rt_region_id.

    " Parse the comma-separated cluster endpoints
    " Expected format: "https://endpoint1.com|us-west-2,https://endpoint2.com|us-
east-1"
    SPLIT iv_cluster_endpoints AT ',' INTO TABLE lt_endpoints.

    " As a best practice, shuffle cluster endpoints to distribute load
    " For more information, see https://docs.aws.amazon.com/r53recovery/latest/
dg/route53-arc-best-practices.html#route53-arc-best-practices.regional
    " For simplicity, we'll try them in order (shuffling can be added if needed)

    " Try each endpoint in order
    LOOP AT lt_endpoints INTO lv_endpoint.
      TRY.
          " Parse endpoint and region from the format "url|region"
          DATA(lv_pos) = find( val = lv_endpoint sub = '|' ).
          IF lv_pos > 0.
            DATA(lv_url) = substring( val = lv_endpoint len = lv_pos ).
            lv_region = substring( val = lv_endpoint off = lv_pos + 1 ).
          ELSE.
            " If no region specified, use default
            lv_url = lv_endpoint.
            lv_region = 'us-east-1'.
          ENDIF.
```

```
        " Create session for this region
        lo_session = /aws1/cl_rt_session_aws=>create( cv_pfl ).

        " Create client with the specific endpoint
        lo_client = create_recovery_client(
          iv_endpoint = lv_url
          iv_region   = lv_region
          io_session  = lo_session ).

        " Try to get the routing control state
        oo_result = lo_client->getroutingcontrolstate(
          iv_routingcontrolarn = iv_routing_control_arn ).

        " If successful, return the result
        RETURN.

      CATCH /aws1/cx_r5vendpttmpyunavailex INTO DATA(lo_endpoint_ex).
        " This endpoint is temporarily unavailable, try the next one
        lo_exception = lo_endpoint_ex.
        CONTINUE.

      CATCH /aws1/cx_r5vaccessdeniedex
            /aws1/cx_r5vinternalserverex
            /aws1/cx_r5vresourcenotfoundex
            /aws1/cx_r5vthrottlingex
            /aws1/cx_r5vvalidationex
            /aws1/cx_rt_generic INTO lo_exception.
        " For other errors, re-raise immediately
        RAISE EXCEPTION lo_exception.
    ENDTRY.
  ENDLOOP.

  " If we get here, all endpoints failed - re-raise the last exception
  IF lo_exception IS BOUND.
    RAISE EXCEPTION lo_exception.
  ENDIF.
```

- Pour plus de détails sur l'API, reportez-vous GetRoutingControlStateà la section de référence du AWS SDK pour l'API SAP ABAP.

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 SDK.

Utilisation **`UpdateRoutingControlState`** avec un AWS SDK

Les exemples de code suivants illustrent 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

Kit SDK for 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).

SAP ABAP

Kit SDK pour SAP ABAP

> **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.

```
    CONSTANTS cv_pfl TYPE /aws1/rt_profile_id VALUE 'ZCODE_DEMO'.
    DATA lo_exception TYPE REF TO /aws1/cx_rt_generic.
    DATA lo_session TYPE REF TO /aws1/cl_rt_session_base.
    DATA lo_client TYPE REF TO /aws1/if_r5v.
    DATA lt_endpoints TYPE TABLE OF string.
    DATA lv_endpoint TYPE string.
    DATA lv_region TYPE /aws1/rt_region_id.

    " Parse the comma-separated cluster endpoints
    " Expected format: "https://endpoint1.com|us-west-2,https://endpoint2.com|us-
east-1"
    SPLIT iv_cluster_endpoints AT ',' INTO TABLE lt_endpoints.

    " As a best practice, shuffle cluster endpoints to distribute load
    " For more information, see https://docs.aws.amazon.com/r53recovery/latest/
dg/route53-arc-best-practices.html#route53-arc-best-practices.regional
    " For simplicity, we'll try them in order (shuffling can be added if needed)

    " Try each endpoint in order
    LOOP AT lt_endpoints INTO lv_endpoint.
      TRY.
          " Parse endpoint and region from the format "url|region"
          DATA(lv_pos) = find( val = lv_endpoint sub = '|' ).
          IF lv_pos > 0.
            DATA(lv_url) = substring( val = lv_endpoint len = lv_pos ).
            lv_region = substring( val = lv_endpoint off = lv_pos + 1 ).
          ELSE.
            " If no region specified, use default
            lv_url = lv_endpoint.
            lv_region = 'us-east-1'.
          ENDIF.
```

```
        " Create session for this region
        lo_session = /aws1/cl_rt_session_aws=>create( cv_pfl ).

        " Create client with the specific endpoint
        lo_client = create_recovery_client(
          iv_endpoint = lv_url
          iv_region   = lv_region
          io_session  = lo_session ).

        " Try to update the routing control state
        oo_result = lo_client->updateroutingcontrolstate(
          iv_routingcontrolarn     = iv_routing_control_arn
          iv_routingcontrolstate   = iv_routing_control_state
          it_safetyrulestooverride = it_safety_rules_override ).

        " If successful, return the result
        RETURN.

      CATCH /aws1/cx_r5vendpttmpyunavailex INTO DATA(lo_endpoint_ex).
        " This endpoint is temporarily unavailable, try the next one
        lo_exception = lo_endpoint_ex.
        CONTINUE.

      CATCH /aws1/cx_r5vaccessdeniedex
            /aws1/cx_r5vconflictexception
            /aws1/cx_r5vinternalserverex
            /aws1/cx_r5vresourcenotfoundex
            /aws1/cx_r5vthrottlingex
            /aws1/cx_r5vvalidationex
            /aws1/cx_rt_generic INTO lo_exception.
        " For other errors, re-raise immediately
        RAISE EXCEPTION lo_exception.
    ENDTRY.
  ENDLOOP.

  " If we get here, all endpoints failed - re-raise the last exception
  IF lo_exception IS BOUND.
    RAISE EXCEPTION lo_exception.
  ENDIF.
```

- Pour plus de détails sur l'API, reportez-vous UpdateRoutingControlStateà la section de référence du AWS SDK pour l'API SAP ABAP.

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 SDK.

Sécurité dans Amazon Application Recovery Controller

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 ceci 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 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 d'ARC. Les rubriques suivantes expliquent comment configurer 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.

Rubriques

Protection des données dans Amazon Application Recovery Controller

Le modèle de responsabilité AWS partagée s'applique à la protection des données dans Amazon 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 d'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 Gestion des identités et des accès AWS (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- SSL/TLS À utiliser pour communiquer avec AWS les ressources. Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail. Pour plus d'informations sur l'utilisation des CloudTrail sentiers pour capturer AWS des activités, consultez la section Utilisation des CloudTrail sentiers dans le guide de AWS CloudTrail l'utilisateur.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-3 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d'informations sur les points de terminaison FIPS disponibles, consultez Norme FIPS (Federal Information Processing Standard) 140-3.

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Nom. Cela inclut lorsque vous travaillez avec ARC ou autre à Services AWS l'aide de la console, de l'API ou AWS SDKs. AWS CLI Toutes les données que vous entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

Chiffrement au repos

Les informations de configuration client stockées par Amazon Application Recovery Controller sont chiffrées au repos.

Chiffrement en transit

Les demandes et réponses des clients concernant Amazon Application Recovery Controller sont chiffrées pendant le transport dans l'ensemble du service à l'aide du protocole TLS.

Identity and Access Management pour Amazon Application Recovery Controller (ARC)

Gestion des identités et des accès AWS (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. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Public ciblé

La façon dont vous utilisez Gestion des identités et des accès AWS (IAM) varie en fonction de votre rôle :

- Utilisateur du service : demandez des autorisations à votre administrateur si vous ne pouvez pas accéder aux fonctionnalités (voir Résolution des problèmes d'identité et d'accès à Amazon Application Recovery Controller (ARC))
- Administrateur du service : déterminez l'accès des utilisateurs et soumettez les demandes d'autorisation (voir Comment les fonctionnalités d'Amazon Application Recovery Controller (ARC) fonctionnent avec IAM)

- Administrateur IAM : rédigez des politiques pour gérer l'accès (voir Exemples de politiques basées sur l'identité dans Amazon Application Recovery Controller (ARC))

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 en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

Vous pouvez vous connecter en tant qu'identité fédérée à l'aide d'informations d'identification provenant d'une source d'identité telle que AWS IAM Identity Center (IAM Identity Center), d'une authentification unique ou d'informations d'identification. Google/Facebook Pour plus d'informations sur la connexion, consultez Connexion à votre Compte AWS dans le Guide de l'utilisateur Connexion à AWS .

Pour l'accès par programmation, AWS fournit un SDK et une CLI pour signer les demandes de manière cryptographique. Pour plus d'informations, consultez Signature AWS Version 4 pour les demandes d'API dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une seule identité de connexion appelée utilisateur Compte AWS root qui dispose d'un accès complet à toutes Services AWS les ressources. Il est vivement déconseillé d'utiliser l'utilisateur racine pour vos tâches quotidiennes. Pour les tâches qui requièrent des informations d'identification de l'utilisateur racine, consultez Tâches qui requièrent les informations d'identification de l'utilisateur racine dans le Guide de l'utilisateur IAM.

Identité fédérée

Il est recommandé d'obliger les utilisateurs humains à utiliser la fédération avec un fournisseur d'identité pour accéder à Services AWS l'aide d'informations d'identification temporaires.

Une identité fédérée est un utilisateur provenant de l'annuaire de votre entreprise, de votre fournisseur d'identité Web ou Directory Service qui y accède à Services AWS l'aide d'informations d'identification provenant d'une source d'identité. Les identités fédérées 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. Pour plus d'informations, 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 qui dispose d'autorisations spécifiques pour une seule personne ou application. Nous vous recommandons d'utiliser ces informations d'identification temporaires au lieu des utilisateurs IAM avec des informations d'identification à long terme. Pour plus d'informations, voir Exiger des utilisateurs humains qu'ils utilisent la fédération avec un fournisseur d'identité pour accéder à AWS l'aide d'informations d'identification temporaires dans le guide de l'utilisateur IAM.

Les groupes IAM spécifient une collection d'utilisateurs IAM et permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Pour plus d'informations, consultez Cas d'utilisation pour les utilisateurs IAM dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une identité dotée d'autorisations spécifiques qui fournit des informations d'identification temporaires. Vous pouvez assumer un rôle en passant d'un rôle utilisateur à un rôle IAM (console) ou en appelant une opération AWS CLI ou AWS API. Pour plus d'informations, consultez Méthodes pour endosser un rôle dans le Guide de l'utilisateur IAM.

Les rôles IAM sont utiles pour l'accès des utilisateurs fédérés, les autorisations temporaires des utilisateurs IAM, les accès intercompte, les accès entre services et les applications exécutées sur Amazon EC2. Pour plus d'informations, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Gestion de l'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 définit les autorisations lorsqu'elles sont associées à une identité ou à une ressource. AWS évalue ces politiques lorsqu'un directeur fait une demande. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations les documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

À l'aide de politiques, les administrateurs précisent qui a accès à quoi en définissant 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. Un administrateur IAM crée des politiques IAM et les ajoute aux rôles, que les utilisateurs peuvent ensuite assumer. Les politiques IAM définissent les autorisations quelle que soit la méthode que vous utilisez pour exécuter l'opération.

Politiques basées sur l'identité

Les stratégies basées sur l'identité sont des documents de stratégie d'autorisations JSON que vous attachez à une identité (utilisateur, groupe ou rôle). Ces politiques contrôlent les actions que peuvent exécuter ces identités, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Définition d'autorisations IAM personnalisées avec des politiques gérées par le client dans le Guide de l'utilisateur IAM.

Les politiques basées sur l'identité peuvent être des politiques intégrées (intégrées directement dans une seule identité) ou des politiques gérées (politiques autonomes associées à plusieurs identités). Pour découvrir comment choisir entre des politiques gérées et 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. Les exemples incluent les politiques de confiance de rôle IAM et les stratégies de compartiment Amazon S3. 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. Vous devez spécifier un principal dans une politique basée sur les ressources.

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.

Autres types de politique

AWS prend en charge des types de politiques supplémentaires qui peuvent définir les autorisations maximales accordées par les types de politiques les plus courants :

- Limites d'autorisations : une limite des autorisations définit le nombre maximum d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM. Pour plus d'informations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.
- Politiques de contrôle des services (SCPs) — Spécifiez les autorisations maximales pour une organisation ou une unité organisationnelle dans AWS Organizations. Pour plus d'informations, consultez Politiques de contrôle de service dans le Guide de l'utilisateur AWS Organizations .
- Politiques de contrôle des ressources (RCPs) : définissez le maximum d'autorisations disponibles pour les ressources de vos comptes. Pour plus d'informations, voir Politiques de contrôle des ressources (RCPs) dans le guide de AWS Organizations l'utilisateur.

- Politiques de session : politiques avancées que vous passez en tant que paramètre lorsque vous créez par programmation une session temporaire pour un rôle ou un utilisateur fédéré. Pour plus d'informations, consultez Politiques de session 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 Application Recovery Controller (ARC) fonctionnent avec IAM

Pour plus d'informations sur le fonctionnement de chaque fonctionnalité d'Amazon Application Recovery Controller (ARC) 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
- IAM pour changement de région

Exemples de politiques basées sur l'identité dans Amazon Application Recovery Controller (ARC)

Pour consulter des exemples de politiques basées sur l'identité pour chaque fonctionnalité d'Amazon Application Recovery Controller (ARC), consultez les rubriques suivantes dans les Gestion des identités et des accès AWS chapitres consacrés à chaque fonctionnalité :

- Exemples de politiques basées sur l'identité pour le changement automatique de zone dans ARC
- Exemples de politiques basées sur l'identité pour le changement de zone dans l'ARC
- Exemples de politiques basées sur l'identité pour le contrôle du routage dans ARC
- Exemples de politiques basées sur l'identité pour le contrôle de l'état de préparation dans ARC

AWS politiques gérées pour Amazon Application Recovery Controller (ARC)

Pour plus d'informations sur les politiques AWS gérées pour les fonctionnalités ARC associées à 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 Application Recovery Controller (ARC)

Consultez les détails des mises à jour des politiques AWS gérées relatives aux fonctionnalités d'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 flux RSS sur la page d'historique du document ARC.

Modifier	Description	Date
AmazonApplicationRecoveryControllerRegionSwitchPlanExecutionPolicy : nouvelle politique	Amazon Application Recovery Controller (ARC) a publié une nouvelle politique gérée qui accorde des autorisations pour l'exécution et l'évaluation du plan de changement de région. Cette politique fournit un accès en lecture seule aux informations du plan de changement de région, à l'état d'exécution et aux données de CloudWatch surveillance d'Amazon. Il inclut également l'autorisation de simuler les	3 novembre 2025

Modifier	Description	Date
	principales politiques IAM pour l'évaluation du plan.	
AWSZonalAutoshiftPracticeRunSLRPolicy stratégie gérée — Politique mise à jour	Ajoute la déclaration de politique `Autoshift PracticeCheckPermissions` avec les autorisations `autoscaling:DescribeAutoScalingGroups` , `ec2:DescribeInstances` `elasticloadbalancing:DescribeTargetHealth` , et `elasticloadbalancing:DescribeTargetHealth` pour prendre en charge les contrôles de capacité équilibrés. Pour en savoir plus, veuillez consulter la section Comment fonctionnent l'autoshift zonal et les courses d'entraînement.	30 juin 2025

Modifier	Description	Date
AWSServiceRoleForPercPracticePolicy— Nouvelle politique	L'ARC a ajouté un nouveau rôle lié au service pour le passage automatique et les essais d'entraînement. ARC utilise les autorisations activées par le rôle lié au service pour surveiller les alarmes CloudWatch Amazon fournies par le Tableau de bord Health client et les événements client 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 AWSService RoleForZonalAutoshiftPracticeRun	30 novembre 2023
AmazonRoute53 RecoveryControlConfigReadOnlyAccess — 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

Modifier	Description	Date

Route53 RecoveryReadinessServiceRolePolicy — Politique mise à jour	ARC a ajouté de nouvelles autorisations pour demander des informations sur les instances Amazon EC2.
	
	ARC utilise les autorisations suivantes pour interroger les instances Amazon EC2, effectuer des contrôles de disponibilité et déterminer l'état de préparation des instances.
	
	`ec2:DescribeVpnGateways`
	
	`ec2:DescribeCustomerGateways`
		17 février 2023

Route53 RecoveryReadinessServiceRolePolicy — Politique mise à jour	ARC a ajouté une nouvelle autorisation permettant de demander des informations sur les fonctions Lambda. 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

Modifier	Description	Date
AmazonRoute53 RecoveryControlConfigFullAccess — 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
AmazonRoute53 RecoveryControlConfigFullAccess — Politique mise à jour	Ajout d'autorisations Amazon Route 53 manquantes à la politique.	15 avril 2022
AmazonRoute53 RecoveryClusterReadOnlyAccess — Politique mise à jour	ARC a ajouté une nouvelle autorisation`route53-recovery-cluster:ListRoutingControls` , pour permettre le contrôle du routage des listes ARNs avec une haute disponibilité.	15 mars 2022
AmazonRoute53 RecoveryControlConfigReadOnlyAccess — Politique mise à jour	ARC a ajouté une nouvelle autorisation`route53-recovery-control-config:ListTagsForResources` , pour permettre de répertorier les balises d'une ressource.	20 décembre 2021

Modifier	Description	Date
Route53 RecoveryReadinessServiceRolePolicy — Politique mise à jour	ARC a ajouté une nouvelle autorisation pour demander des informations sur Amazon API Gateway. 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
AmazonRoute53 RecoveryReadinessReadOnlyAccess — Ajout de nouvelles autorisations	ARC a ajouté deux nouvelles autorisations à AmazonRoute53 RecoveryReadinessReadOnlyAccess : ARC utilise `route53-recovery-readiness:GetArchitectureRecommendations` et autorise `route53-recovery-readiness:GetCellReadinessSummary` un accès en lecture seule à ces actions pour travailler sur la préparation à la restauration.	15 octobre 2021

Modifier	Description	Date

Route53 RecoveryReadinessServiceRolePolicy — Politique mise à jour	ARC a ajouté de nouvelles autorisations pour demander des informations sur les fonctions Lambda.
	
	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

Modifier	Description	Date
Route53 RecoveryReadinessServiceRolePolicy — Ajout de nouvelles politiques gérées	ARC a ajouté les nouvelles politiques gérées suivantes : AmazonRoute53 RecoveryReadinessFullAccess AmazonRoute53 RecoveryReadinessReadOnlyAccess AmazonRoute53 RecoveryClusterFullAccess AmazonRoute53 RecoveryClusterReadOnlyAccess AmazonRoute53 RecoveryControlConfigFullAccess AmazonRoute53 RecoveryControlConfigReadOnlyAccess	18 août 2021
ARC a commencé à suivre les modifications	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 Application Recovery Controller (ARC)

Utilisez les informations suivantes pour diagnostiquer et résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec Amazon Application Recovery Controller (ARC) et IAM.

Rubriques

- Je ne suis pas autorisé à effectuer une action dans ARC
- Je ne suis pas autorisé à effectuer iam : PassRole

- Je souhaite autoriser des personnes extérieures Compte AWS à moi à accéder à mes ressources ARC

Je ne suis pas autorisé à effectuer une action dans 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 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, vous devez 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 ARC. Toutefois, l'action nécessite que le service ait des autorisations accordées par un rôle de service. Mary n'est pas autorisée à transmettre 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 autoriser des personnes extérieures Compte AWS à moi à accéder à mes ressources ARC

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 (ACLs), vous pouvez utiliser ces politiques pour autoriser les utilisateurs à accéder à vos ressources.

Pour plus d'informations, consultez les éléments suivants :

- Pour savoir si ARC prend en charge ces fonctionnalités, consultezComment les fonctionnalités d'Amazon Application Recovery Controller (ARC) 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 en savoir plus sur la différence entre l'utilisation des rôles et des politiques basées sur les ressources pour l'accès intercompte, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Accédez au changement de zone d'Amazon Application Recovery Controller (ARC) à l'aide d'un point de terminaison d'interface ()AWS PrivateLink

Vous pouvez l'utiliser AWS PrivateLink pour créer une connexion privée entre votre VPC et le changement de zone d'Amazon Application Recovery Controller (ARC). Vous pouvez accéder au décalage de zone ARC comme s'il se trouvait dans votre VPC, sans utiliser de passerelle Internet, de périphérique NAT, de connexion VPN ou de connexion. Direct Connect Les instances de votre VPC n'ont pas besoin d'adresses IP publiques pour accéder à ARC Zonal Shift.

Vous établissez cette connexion privée en créant un point de terminaison d'interface optimisé par AWS PrivateLink. Nous créons une interface réseau de point de terminaison dans chaque sous-réseau que vous activez pour le point de terminaison d'interface. Il s'agit d'interfaces réseau gérées par les demandeurs qui servent de point d'entrée pour le trafic destiné au changement de zone ARC.

Pour plus d'informations, consultez la section Accès Services AWS par AWS PrivateLink le biais du AWS PrivateLink guide.

Considérations relatives au décalage de zone ARC

Avant de configurer un point de terminaison d'interface pour le décalage de zone ARC, consultez les considérations du AWS PrivateLink guide.

ARC Zonal Shift permet d'appeler toutes ses actions d'API via le point de terminaison de l'interface.

Création d'un point de terminaison d'interface pour le décalage zonal ARC

Vous pouvez créer un point de terminaison d'interface pour le changement de zone ARC à l'aide de la console Amazon VPC ou AWS Command Line Interface du AWS CLI(). Pour plus d'informations, consultez Création d'un point de terminaison d'interface dans le Guide AWS PrivateLink .

Créez un point de terminaison d'interface pour le décalage zonal ARC en utilisant le nom de service suivant :

```
com.amazonaws.region.arc-zonal-shift
```

Si vous activez le DNS privé pour le point de terminaison de l'interface, vous pouvez envoyer des demandes d'API à ARC Zonal Shift en utilisant son nom DNS régional par défaut. Par exemple, `arc-zonal-shift.us-east-1.amazonaws.com`.

Création d’une politique de point de terminaison pour votre point de terminaison d’interface

Une politique de point de terminaison est une ressource IAM que vous pouvez attacher à votre point de terminaison d’interface. La politique de point de terminaison par défaut permet un accès complet au décalage de zone ARC via le point de terminaison de l'interface. Pour contrôler l'accès autorisé au changement de zone ARC depuis votre VPC, associez une politique de point de terminaison personnalisée au point de terminaison de l'interface.

Une politique de point de terminaison spécifie les informations suivantes :

- Les principaux qui peuvent effectuer des actions (Comptes AWS, utilisateurs IAM et rôles IAM).
- Les actions qui peuvent être effectuées.
- La ressource sur laquelle les actions peuvent être effectuées.

Pour plus d’informations, consultez Contrôle de l’accès aux services à l’aide de politiques de point de terminaison dans le Guide AWS PrivateLink .

Exemple : politique de point de terminaison VPC pour les actions de changement de zone ARC

Voici un exemple de politique de point de terminaison personnalisée. Lorsque vous attachez cette politique au point de terminaison de votre interface, elle donne accès aux actions de changement de zone ARC répertoriées pour tous les principaux sur toutes les ressources.

```
{
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [
            "arc-zonal-shift:ListManagedResources",
            "arc-zonal-shift:StartZonalShift",
            "arc-zonal-shift:CancelZonalShift"
         ],
         "Resource":"*"
      }
   ]
}
```

Ils `Resource` peuvent également être répertoriés comme`arn:aws:elasticloadbalancing:us-east-1:111122223333:loadbalancer/app/Testing/1111111ecd42dc05`.

Journalisation et surveillance dans ARC

La surveillance joue un rôle important dans le maintien de la disponibilité et des performances d'ARC 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 vos ressources et votre activité ARC, et répondre aux incidents potentiels, par exemple, AWS CloudTrail et Amazon CloudWatch.

Pour plus d'informations sur la surveillance de chaque fonctionnalité dans 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
- Journalisation et surveillance pour le changement de région
- Enregistrement et surveillance pour vérifier l'état de préparation

Validation de conformité pour Amazon Application Recovery Controller

Des auditeurs tiers évaluent la sécurité et la conformité d'Amazon 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. Pour plus d'informations sur votre responsabilité en matière de conformité lors de l'utilisation Services AWS, consultez AWS la documentation de sécurité.

Résilience dans Amazon Application Recovery Controller

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, ARC propose plusieurs fonctionnalités pour répondre à vos besoins en matière de résilience et de sauvegarde des données.

Sécurité de l'infrastructure dans Amazon Application Recovery Controller

En tant que service géré, il 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 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.

Historique du document relatif au guide du développeur Amazon Application Recovery Controller (ARC)

Les entrées suivantes décrivent les modifications importantes apportées à la documentation d'Amazon Application Recovery Controller (ARC).

- Version : dernière
- Dernière mise à jour de la documentation : 31 mars 2026

Modifier	Description	Date
Modification de la disponibilité du contrôle de préparation	La fonctionnalité de vérification du niveau de préparation d'Amazon Application Recovery Controller (ARC) ne sera plus ouverte aux nouveaux clients à compter du 30 avril 2026. Les clients existants peuvent continuer à utiliser le service normalement. Pour plus d'informations, consultez la section Modification de la disponibilité du test de disponibilité d'Amazon Application Recovery Controller (ARC).	31 mars 2026
Nouvelle politique gérée pour l'exécution du plan de changement de région	Amazon Application Recovery Controller (ARC) a publié une nouvelle politique gérée qui accorde des autorisations pour l'exécution et l'évaluation du plan de changemen	3 novembre 2025

Modifier	Description	Date
	t de région. `AmazonApplicationRecoveryControllerRegionSwitchPlanExecutionPolicy` Pour plus d'informations, consultez les mises à jour des politiques AWS gérées par Amazon Application Recovery Controller (ARC).	
Vous pouvez désormais utiliser le décalage de zone AWS PrivateLink entre votre VPC et Amazon Application Recovery Controller (ARC).	Vous pouvez utiliser an AWS PrivateLink pour créer une connexion privée entre votre VPC et le changement de zone d'Amazon Application Recovery Controller (ARC). Pour plus d'informations, consultez Access Amazon Application Recovery Controller (ARC) zonal shift à l'aide d'un point de terminaison d'interface (AWS PrivateLink).	11 août 2025

Modifier	Description	Date
Nouveau service de changement de région	Le changement de région permet aux clients d'orchest rer les étapes spécifiques, en prenant en charge les comptes multiples, nécessair es pour exploiter leur applicati on multirégionale à partir d'une autre. Région AWS Pour plus d'informations, voir Changement de région dans ARC.	1er août 2025
Améliorations apportées aux courses d'entraînement	Vous pouvez désormais démarrer des séances d'entraînement à la demande dans ARC. En outre, les courses d'entraînement incluent désormais la vérificat ion de la capacité suffisante AZs dans d'autres régions de la Région. Pour plus d'informations, consultez la section Fonctionn ement.	30 juin 2025

Modifier	Description	Date
Met à jour une politique gérée	Met à jour la politique `AWSZonalAutoshiftPracticeRunSLRPolicy` gérée en ajoutant la déclaration de politique `AutoshiftPracticeCheckPermissions` avec les autorisations`autoscaling:DescribeAutoScalingGroups` , `ec2:DescribeInstances` `elasticloadbalancing:DescribeTargetHealth` , et `elasticloadbalancing:DescribeTargetHealth` pour prendre en charge les contrôles de capacité équilibrés. Pour plus d'informations, consultez la section Stratégie AWSZonal AutoshiftPracticeRun SLRPolicy gérée.	30 juin 2025
Mises à jour des types d'exception pour l'autoshift zonal	Vous pouvez désormais interagir avec le changement automatique de zone par ressource. Pour plus d'informations, consultez la section Fonctionnement.	21 avril 2025

Modifier	Description	Date
Testez l'autoshift zonal ARC avec AWS FIS	Vous pouvez l'utiliser AWS FIS pour tester la façon dont ARC Zonal AutoShift rétablit automatiquement votre application lors d'une coupure de courant AZ Pour plus d'informations, voir Tester l'autoshift zonal avec. AWS FIS	26 mars 2025
ARC prend désormais en charge les IPv6 points de terminaison pour les contrôles de routage et le décalage de zone.	ARC prend désormais en charge les IPv6 points de terminaison pour les contrôles de routage et le décalage de zone. Pour plus d'informations, voir Configuration des composants de contrôle de routage.	21 novembre 2024
Capacité de changement de zone pour les groupes Amazon EC2 Auto Scaling	ARC prend désormais en charge le décalage de zone pour les groupes Amazon EC2 Auto Scaling. Pour plus d'informations, consultez Support for Amazon EC2 Auto Scaling groups.	18 novembre 2024

Modifier	Description	Date
Capacité de changement de zone pour Amazon EKS	Vous pouvez démarrer un changement de zone pour un cluster Amazon EKS, ou vous pouvez autoriser le changement de zone à le AWS faire pour vous en activant le changemen t automatique de zone. Ce changement met à jour le flux de trafic east-to-west réseau dans votre cluster afin de ne considérer que les points de terminaison réseau des pods exécutés sur des nœuds de travail comme sains AZs. Pour plus d'informations, consultez Support for Amazon Elastic Kubernetes Service.	22 octobre 2024
Capacité de changement de zone pour les équilibreurs de charge réseau	ARC prend désormais en charge le décalage de zone pour les équilibreurs de charge réseau avec des configurations activées ou désactivées entre zones. Pour plus d'informations, consultez Support pour les équilibreurs de charge réseau.	11 octobre 2024

Modifier	Description	Date
Notifications des observateurs Autoshift	Grâce aux notifications d'observation Autoshift, vous pouvez configurer l'autoshift zonal pour vous avertir, via Amazon EventBridge, chaque fois qu'un changement automatique AWS démarre afin de déplacer le trafic hors d'une zone de disponibilité potentiellement altérée. Il n'est pas nécessaire de configurer des ressources spécifiques avec le changement automatique par zone pour activer ces notifications distinctes. Pour plus d'informations, consultez Utilisation de l'autoshift zonal avec Amazon EventBridge.	12 juillet 2024

Modifier	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 d'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 Application Recovery Controller (ARC) ?	30 avril 2024

Modifier	Description	Date
Ajoute une capacité de changement automatique zonal	Ajoute une nouvelle fonctionn alité dans 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 Application Recovery Controlle r (ARC).	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 Autorisations des rôles liés à un service pour AWSServiceRoleForZ onalAutoshiftPracticeRun.	30 novembre 2023

Modifier	Description	Date
Ajoute le support multi-comptes pour les clusters	Ajoute la prise en charge multicompte pour les clusters dans 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, voir Support des comptes croisés pour les clusters dans 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

Modifier	Description	Date
Rôle lié à un service mis à jour	Ajout de nouvelles autorisations `ec2:DescribeVpnGateways` et `ec2:DescribeCustomerGateways`, au rôle lié au service pour ARC, de 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 ARC.	17 février 2023
Déclenchement GA pour changement de zone	Prend en charge la version GA de Zonal Shift pour ARC, qui inclut le contrôle d'accès basé sur les attributs (ABAC) pour les ressources gérées enregistrées dans ARC pour le changement de zone. Pour plus d'informations, voir Contrôle d'accès basé sur les attributs (ABAC) avec ARC.	10 janvier 2023

Modifier	Description	Date
Ajout d'un nouveau changement de zone multi-AZ	Ajout de contenu décrivant un nouveau service dans ARC, Zonal Shift, 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 zonal dans ARC.	28 novembre 2022
Rôle lié à un service mis à jour	Ajout d'une nouvelle autorisation au rôle lié au service permettant à 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 ARC.	31 août 2022

Modifier	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 Application Recovery Controller (ARC).	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 Application Recovery Controller (ARC).	15 avril 2022

Modifier	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 des listes inclus dans l'API extrêmement fiable du plan de données 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

Modifier	Description	Date
Ajout d'un support de balisage supplémentaire	Ajout de la prise en charge du balisage de ressources supplémentaires dans 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 Application Recovery Controller (ARC).	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 Application Recovery Controller (ARC)	20 décembre 2021

Modifier	Description	Date
Ajout de la prise en charge des alertes en temps réel avec EventBridge	Support ajouté EventBridge, ce qui signifie que vous pouvez désormais ajouter des règles pour recevoir des alertes et agir en cas de changement de statut du contrôle de préparation de l'ARC, par exemple lorsqu'un statut passe de PRÊT à PAS PRÊT. Pour plus d'informations, consultez la section Utilisation d'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 Application Recovery Controller (ARC).	16 novembre 2021

Modifier	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 Application Recovery Controller (ARC).	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 ARC afin qu'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 ARC.	28 octobre 2021

Modifier	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 ARC afin qu'ARC puisse auditer les fonctions Lambda à l'aide de contrôles de 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 ARC.	8 octobre 2021
Liens CloudFormation et modèles Terraform ajoutés	Ajout de liens vers des modèles téléchargeables CloudFormation et des modèles Hashicorp Terraform pour vous aider à démarrer rapidement avec Arc. Pour plus d'informations, voir Préparation à la restauration avec une nouvelle application.	13 septembre 2021

Modifier	Description	Date
Ajout de nouvelles politiques gérées	Les politiques AWS gérées suivantes ont été ajoutées pour ARC : `AmazonRoute53RecoveryReadinessFullAccess` `AmazonRoute53RecoveryReadinessReadOnlyAccess` ,`AmazonRoute53RecoveryClusterFullAccess` ,`AmazonRoute53RecoveryClusterReadOnlyAccess` ,`AmazonRoute53RecoveryControlConfigFullAccess` , et`AmazonRoute53RecoveryControlConfigReadOnlyAccess` . Pour plus d'informations, consultez les politiques AWS gérées pour Amazon Application Recovery Controller (ARC).	18 août 2021
A commencé à suivre les politiques AWS gérées pour Amazon Application Recovery Controller (ARC)	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 Application Recovery Controller (ARC).	27 Juillet 2021

Modifier	Description	Date
Version initiale d'Amazon Application Recovery Controller (ARC)	ARC améliore la disponibilité des applications en coordonnant de manière centralisée les basculements au sein d'une AWS région ou entre plusieurs régions. 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, voir Qu'est-ce que l'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.