Guide de l'utilisateur

AWS Centre de résilience

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

AWS Centre de résilience: Guide de l’utilisateur

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

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

Table of Contents

Qu'est-ce que c'est AWS Resilience Hub ? ... 1
AWS Resilience Hub — Gestion de la résilience ... 2
Comment AWS Resilience Hub fonctionne ... 2
AWS Resilience Hub — Tests de résilience ... 5
AWS Resilience Hub concepts ... 6
Résilience ... 6
Objectif de point de récupération (RPO) ... 6
Objectif de temps de rétablissement (RTO) ... 6
Objectif de temps de rétablissement estimé de la charge de travail ... 6
Objectif estimé du point de rétablissement de la charge de travail ... 7
Application ... 7
Composant de l'application ... 7
État de conformité de l'application ... 7
Détection des écarts ... 8
Évaluation de la résilience ... 8
Score de résilience ... 8
Type de perturbation ... 9
AWS FIS expériences ... 9
ARRÊT ... 10
AWS Resilience Hub personas ... 10
AWS Resilience Hub Ressources prises en charge ... 11
AWS Resilience Hub et MyApplications ... 15
En savoir plus ... 17
Mise en route ... 18
Prérequis ... 18
Ajout d'une application ... 19
Commencez par ajouter une application ... 20
Gérez les ressources de votre application ... 21
Ajoutez des ressources à votre AWS Resilience Hub application ... 22
Définissez le RTO et le RPO ... 26
Configuration de l'évaluation planifiée et de la notification de dérive ... 28
Autorisations de configuration ... 29
Configuration des paramètres de configuration de l'application ... 30
Ajoutez des tags à votre application ... 31

Réviser et publier ... 31
Exécuter une évaluation ... 32
En utilisant AWS Resilience Hub ... 34
AWS Resilience Hub résumé ... 34
État de la demande ... 35
Principales recommandations en matière d'infrastructure par type de ressource ... 36
Recommandations en matière d'infrastructure ... 36
Recommandations opérationnelles non mises en œuvre ... 36
Recommandations relatives aux alarmes ... 37
Recommandations SOP ... 37
AWS FIS recommandations d'expériences ... 37
Applications présentant des dérives ... 38
Score de résilience ... 38
Les 10 meilleures applications en termes de score de résilience ... 38
État de l'application par stratégie ... 39
AWS Resilience Hub tableau de bord ... 39
État de la demande ... 40
Score de résilience des applications au fil du temps ... 40
Alarmes mises en œuvre ... 41
Expériences mises en œuvre ... 41
Gestion d'applications ... 41
Afficher le résumé de l'application ... 44
Modification des ressources de l'application ... 47
Gestion des composants de l'application ... 55
Publier une nouvelle version de l'application ... 64
Affichage des versions de l'application ... 65
Afficher les ressources de votre application ... 66
Suppression d'une application ... 67
Paramètres de configuration de l'application ... 68
Gestion des politiques de résilience ... 69
Création de politiques de résilience ... 70
Accès aux détails de la politique de résilience ... 74
Gestion des évaluations de résilience dans AWS Resilience Hub ... 75
Exécution d'évaluations de résilience dans AWS Resilience Hub ... 76
Révision des rapports d'évaluation ... 77
Supprimer les évaluations de résilience ... 86

Gestion des évaluations de résilience à partir du widget Resiliency 87
Exécution d'évaluations de résilience à partir du widget Resiliency 88
Consulter le résumé de l'évaluation dans le widget Resiliency 90
Gérer les alarmes 91
Création d'alarmes à partir des recommandations opérationnelles 91
Affichage des alarmes 95
Gestion des procédures opérationnelles standard 98
Élaboration d'une SOP basée sur les recommandations AWS Resilience Hub 100
Création d'un document SSM personnalisé 101
Utiliser un document SSM personnalisé au lieu du document par défaut 101
Tests SOPs 102
Affichage des procédures opérationnelles standard 102
Gestion des AWS Fault Injection Service expériences 104
Lancer, créer et exécuter AWS FIS des expériences 105
Visualisation AWS FIS des expériences 108
AWS Fault Injection Service échecs d'expérience/vérification de l'état 111
Comprendre les scores de résilience 114
Accès au score de résilience de vos applications 114
Calcul des scores de résilience 117
Intégration des recommandations dans les applications 131
Modifier le AWS CloudFormation modèle 133
Utilisation AWS Resilience Hub APIs pour décrire et gérer une application 137
Préparation de la demande 137
Création d'une application 137
Création d'une politique de résilience 138
Importer les ressources de l'application et surveiller l'état de l'importation 139
Publiez votre application et attribuez une politique de résilience 142
Exécution et analyse de l'application 143
Exécuter et surveiller une évaluation de la résilience 144
Création d'une politique de résilience 147
Modifiez votre candidature 162
Ajouter des ressources manuellement 162
Regroupement des ressources dans un seul composant d'application 163
Exclure une ressource d'un AppComponent 165
Sécurité 167
Protection des données 167

Chiffrement au repos ... 169
Chiffrement en transit ... 169
Gestion de l'identité et des accès ... 169
Public ciblé ... 170
Authentification par des identités ... 170
Gestion des accès à l'aide de politiques ... 174
Comment AWS Resilience Hub fonctionne avec IAM ... 178
Configuration des rôles et autorisations IAM ... 191
Résolution des problèmes ... 192
AWS Resilience Hub référence des autorisations d'accès ... 195
AWS politiques gérées ... 209
AWS Resilience Hub référence aux personas et aux autorisations IAM ... 220
Importation du fichier d'état Terraform dans AWS Resilience Hub ... 223
Activation de AWS Resilience Hub l'accès à votre cluster Amazon EKS ... 228
Activation AWS Resilience Hub de la publication sur vos rubriques Amazon SNS ... 240
Limiter les autorisations pour inclure ou exclure AWS Resilience Hub des recommandations ... 241
Sécurité de l'infrastructure ... 242
Contrôles de résilience pour les AWS services ... 243
Amazon Elastic File System ... 244
Type de système de fichiers ... 244
Backup du système de fichiers ... 244
Réplication des données ... 244
Amazon Relational Database Service et Amazon Aurora ... 244
Déploiement mono-AZ ... 245
déploiement multi-AZ ... 245
Sauvegarde ... 245
Basculement entre régions ... 245
Basculement régional plus rapide ... 246
Amazon Simple Storage Service ... 246
Gestion des versions ... 246
Sauvegarde planifiée ... 246
Réplication des données ... 247
Amazon DynamoDB ... 247
Sauvegarde planifiée ... 247
Tableau global ... 248

Amazon Elastic Compute Cloud 248
Instance dynamique 248
Groupes Auto Scaling 248
EC2 Flotte Amazon 249
Amazon EBS 249
Sauvegarde planifiée 249
Sauvegarde et réplication des données 249
AWS Lambda 250
Client : Amazon VPC Access 250
File d'attente de lettres mortes 250
Amazon Elastic Kubernetes Service 250
déploiement multi-AZ 250
Déploiement vs. ReplicaSet 251
Maintenance du déploiement 251
Amazon Simple Notification Service 251
Abonnements thématiques 252
Amazon Simple Queue Service 252
File d'attente de lettres mortes 252
Amazon Elastic Container Service 252
déploiement multi-AZ 252
Elastic Load Balancing 252
déploiement multi-AZ 252
Amazon API Gateway 253
Déploiement entre régions 253
Déploiement multi-AZ d'API privées 253
Amazon DocumentDB 253
déploiement multi-AZ 253
Déploiement en cluster élastique et multi-AZ 254
Cluster élastique et instantanés manuels 254
Passerelle NAT 254
déploiement multi-AZ 254
Amazon Route 53 254
déploiement multi-AZ 254
Contrôleur Amazon Application Recovery (ARC) 255
déploiement multi-AZ 255
Serveur FSx de fichiers Amazon pour Windows 255

Type de système de fichiers 255
Backup du système de fichiers 255
Réplication des données 255
AWS Step Functions 256
Gestion des versions et alias 256
Déploiement entre régions 256
Amazon ElastiCache (Redis OSS) 256
Déploiement mono-AZ 256
Déploiement mono-AZ 256
Basculement entre régions 257
Sauvegarde 257
Basculement régional plus rapide 257
Utilisation d'autres services 258
AWS CloudFormation 258
AWS Resilience Hub et AWS CloudFormation modèles 258
En savoir plus sur AWS CloudFormation 259
AWS CloudTrail 259
AWS Systems Manager 259
AWS Trusted Advisor 260
Historique de la documentation 264
AWS Glossaire 300
..... ccci

Qu'est-ce que c'est AWS Resilience Hub ?

AWS Resilience Hub est un emplacement central sur lequel vous pouvez gérer et améliorer la résilience de vos applications AWS. AWS Resilience Hub vous permet de définir vos objectifs de résilience, d'évaluer votre posture de résilience par rapport à ces objectifs et de mettre en œuvre des recommandations d'amélioration basées sur le AWS Well-Architected Framework. Vous pouvez également y créer et exécuter des AWS Fault Injection Service expériences qui imitent les perturbations réelles de votre application pour vous aider à mieux comprendre les dépendances et à découvrir les faiblesses potentielles. AWS Resilience Hub AWS Resilience Hub fournit un emplacement central avec tous les AWS services et outils dont vous avez besoin pour renforcer en permanence votre posture de résilience. AWS Resilience Hub collabore avec d'autres services pour fournir des recommandations et vous aider à gérer les ressources de votre application. Pour de plus amples informations, veuillez consulter Utilisation d'autres services .

Le tableau suivant fournit les liens de documentation de tous les services de résilience associés.

Services de AWS résilience et références connexes

AWS service de résilience	Lien vers la documentation
AWS Elastic Disaster Recovery	Qu'est-ce qu'Elastic Disaster Recovery
AWS Backup	Qu'est-ce que AWS Backup
Contrôleur Amazon Application Recovery (ARC) (ARC)	Qu'est-ce qu'Amazon Application Recovery Controller (ARC)

Rubriques

- AWS Resilience Hub — Gestion de la résilience
- AWS Resilience Hub — Tests de résilience
- AWS Resilience Hub concepts
- AWS Resilience Hub personas
- AWS Resilience Hub ressources prises en charge
- AWS Resilience Hub et MyApplications

AWS Resilience Hub — Gestion de la résilience

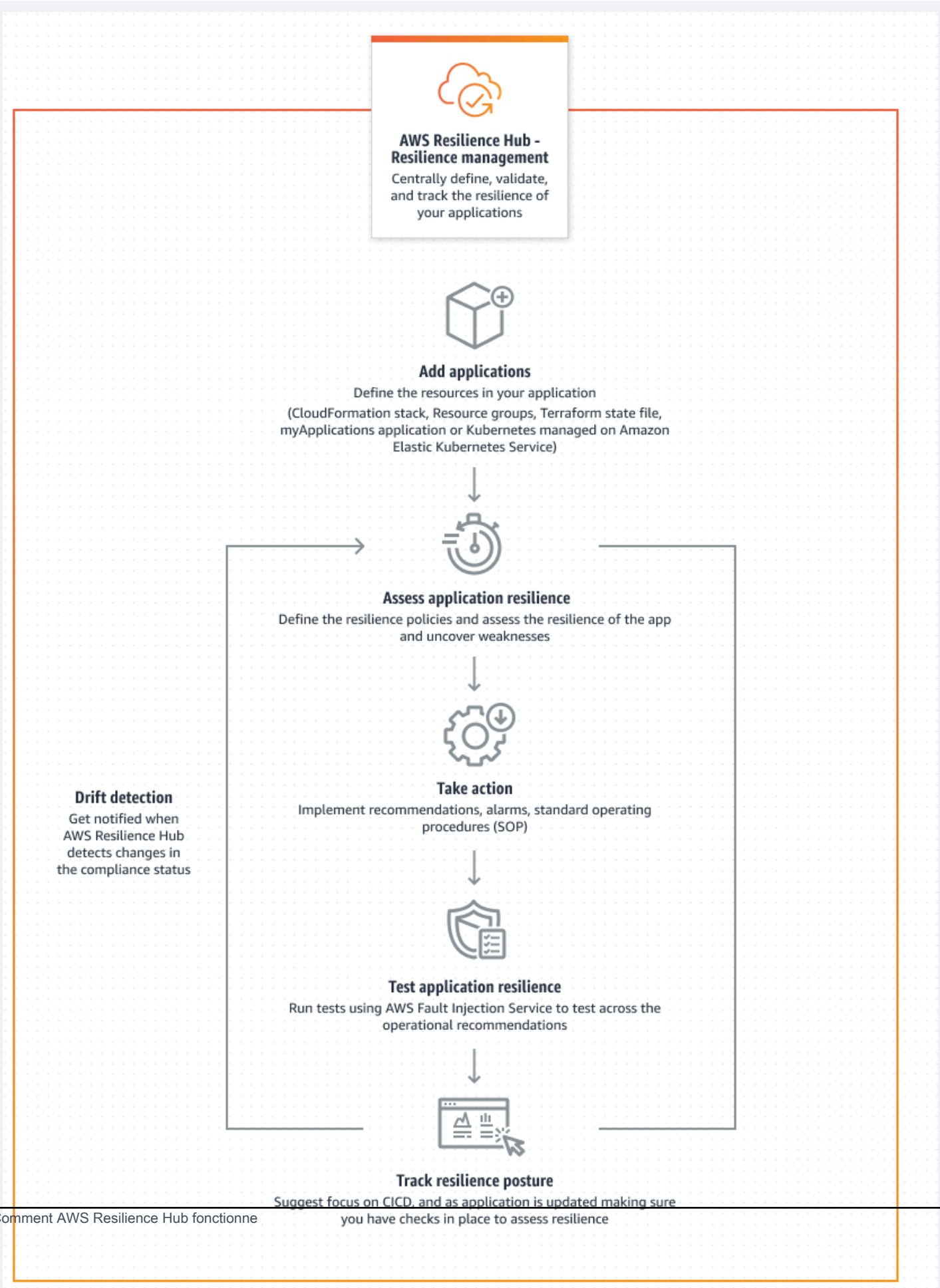
AWS Resilience Hub vous offre un emplacement central pour définir, valider et suivre la résilience de votre AWS application. AWS Resilience Hub vous aide à protéger vos applications contre les perturbations et à réduire les coûts de restauration afin d'optimiser la continuité des activités et de répondre aux exigences réglementaires et de conformité. Vous pouvez utiliser AWS Resilience Hub pour effectuer les opérations suivantes :

- Analysez votre infrastructure et obtenez des recommandations pour améliorer la résilience de vos applications. Outre des conseils architecturaux pour améliorer la résilience de votre application, les recommandations fournissent du code pour respecter votre politique de résilience, en mettant en œuvre des tests, des alarmes et des procédures opérationnelles standard (SOPs) que vous pouvez déployer et exécuter avec votre application dans votre pipeline d'intégration et de livraison (CI/CD).
- Évaluez les objectifs de temps de restauration (RTO) et d'objectif de point de reprise (RPO) dans différentes conditions.
- Optimisez la continuité des activités tout en réduisant les coûts de reprise.
- Identifiez et résolvez les problèmes avant qu'ils ne surviennent en production.

Après avoir déployé une application en production, vous pouvez l'ajouter AWS Resilience Hub à votre pipeline CI/CD pour valider chaque version avant sa mise en production.

Comment AWS Resilience Hub fonctionne

Le schéma suivant fournit un aperçu général du AWS Resilience Hub fonctionnement.


AWS Resilience Hub - Resilience management
Centrally define, validate, and track the resilience of your applications
Add applications
Define the resources in your application
(CloudFormation stack, Resource groups, Terraform state file, myApplications application or Kubernetes managed on Amazon Elastic Kubernetes Service)
Assess application resilience
Define the resilience policies and assess the resilience of the app and uncover weaknesses
Take action
Implement recommendations, alarms, standard operating procedures (SOP)
Test application resilience
Run tests using AWS Fault Injection Service to test across the operational recommendations
Track resilience posture
Suggest focus on CICD, and as application is updated making sure you have checks in place to assess resilience
Drift detection
Get notified when AWS Resilience Hub detects changes in the compliance status

Describe

Décrivez votre application en important des ressources à partir de AWS CloudFormation piles, de fichiers d'état Terraform ou de clusters Amazon Elastic Kubernetes Service, ou vous pouvez choisir parmi des applications déjà définies dans MyApplications. AWS Resource Groups

Définir

Définissez les politiques de résilience pour vos applications. Ces politiques incluent des objectifs RTO et RPO pour les interruptions liées aux applications, à l'infrastructure, aux zones de disponibilité et aux régions. Ces cibles sont utilisées pour estimer si l'application répond à la politique de résilience.

Évaluation

Après avoir décrit votre application et y avoir associé une politique de résilience, exécutez une évaluation de la résilience. L' AWS Resilience Hub évaluation utilise les meilleures pratiques du AWS Well-Architected Framework pour analyser les composants d'une application et découvrir les faiblesses potentielles en matière de résilience. Ces faiblesses peuvent être dues à une configuration incomplète de l'infrastructure, à une mauvaise configuration ou à des situations nécessitant des améliorations de configuration supplémentaires. Pour améliorer la résilience, mettez à jour votre application et votre politique de résilience conformément aux recommandations du rapport d'évaluation. Les recommandations incluent la configuration des composants, les alarmes, les tests et la restauration SOPs. Vous pouvez ensuite exécuter une autre évaluation et comparer les résultats avec le rapport précédent pour voir dans quelle mesure la résilience s'améliore. Répétez ce processus jusqu'à ce que votre RTO de charge de travail estimé et votre RPO de charge de travail estimé atteignent vos objectifs de RTO et de RPO.

Valider

Exécutez des tests pour mesurer la résilience de vos AWS ressources et le temps nécessaire à la restauration après une application, une infrastructure, une zone de disponibilité et des Région AWS incidents. Pour mesurer la résilience, ces tests simulent les pannes de vos AWS ressources. Parmi les pannes, citons les erreurs d'indisponibilité du réseau, les basculements, les processus interrompus, la restauration du démarrage d'Amazon RDS et les problèmes liés à votre zone de disponibilité.

Afficher et suivre

Après avoir déployé une AWS application en production, vous pouvez l'utiliser AWS Resilience Hub pour continuer à suivre la posture de résilience de l'application. En cas de panne, l'opérateur peut visualiser la panne AWS Resilience Hub et lancer le processus de restauration associé.

AWS Resilience Hub — Tests de résilience

AWS Resilience Hub prend en charge une meilleure intégration avec le AWS FIS. Cette intégration permet AWS Resilience Hub de proposer des recommandations personnalisées à l'aide d' AWS FIS actions et de scénarios basés sur le contexte spécifique de l'application évaluée. L'exécution des expériences recommandées ou la réalisation de vos propres tests à l'aide du AWS FIS service contribueront directement à améliorer le score de résilience de votre application.

Ces AWS FIS actions et scénarios testent la posture de résilience d'une application en créant des événements perturbateurs afin que vous puissiez observer la réaction de votre application. AWS FIS propose plusieurs scénarios prédéfinis et un large choix d'actions qui génèrent des perturbations. En outre, il inclut également les commandes et les glissières de sécurité dont vous avez besoin pour effectuer les expériences en production. Les commandes et les glissières de sécurité incluent des options permettant de revenir en arrière automatiquement ou d'arrêter l'expérience si des conditions spécifiques sont remplies. Pour commencer à utiliser la console AWS FIS pour exécuter des expériences depuis la AWS Resilience Hub console, remplissez les conditions requises définies dans the section called "Prérequis" la section.

Le tableau suivant répertorie toutes les AWS FIS options disponibles dans le volet de navigation et les liens vers la AWS FIS documentation associée qui contient les procédures pour commencer à utiliser les AWS FIS tests depuis AWS Resilience Hub la console.

AWS FIS options et références du menu de navigation

AWS FIS option de menu de navigation	AWS FIS documentation
Tests de résilience	Création d'un modèle d'expérience
Bibliothèque de scénarios	AWS FIS bibliothèque
Modèles d'expériences	Modèles d'expériences pour AWS FIS

Le tableau suivant répertorie toutes les AWS FIS options disponibles dans le menu déroulant de la section Tests de résilience et les liens vers la AWS FIS documentation associée qui contient les procédures pour commencer à utiliser les AWS FIS tests depuis la AWS Resilience Hub console.

AWS FIS options et références du menu déroulant

AWS FIS option de menu déroulant	AWS FIS documentation
Création d'un modèle d'expérience	Création d'un modèle d'expérience
Création d'une expérience à partir d'un scénario	Utilisation d'un scénario

AWS Resilience Hub concepts

Ces concepts peuvent vous aider à mieux comprendre AWS Resilience Hub l'approche adoptée pour améliorer la résilience des applications et prévenir les pannes d'applications.

Résilience

La capacité de maintenir la disponibilité et de récupérer après une interruption logicielle ou opérationnelle dans un délai défini.

Objectif de point de récupération (RPO)

Durée maximale acceptable depuis le dernier point de récupération des données. Il détermine ce qui est considéré comme étant une perte de données acceptable entre le dernier point de reprise et l'interruption du service.

Objectif de temps de rétablissement (RTO)

Le délai maximum acceptable entre l'interruption du service et le rétablissement du service. Elle détermine ce qui est considéré comme étant un créneau de temps acceptable d'indisponibilité du service.

Objectif de temps de rétablissement estimé de la charge de travail

L'objectif de temps de rétablissement de la charge de travail estimé (RTO de charge de travail estimé) est le RTO que votre application est censée atteindre sur la base de la définition de l'application importée, puis exécuter une évaluation.

Objectif estimé du point de rétablissement de la charge de travail

L'objectif du point de reprise de charge de travail estimé (RPO de charge de travail estimé) est le RPO que votre application est censée atteindre en fonction de la définition de l'application importée, puis d'une évaluation.

Application

Une AWS Resilience Hub application est un ensemble de ressources AWS prises en charge qui sont surveillées et évaluées en permanence pour gérer sa posture de résilience.

Composant de l'application

Groupe de AWS ressources connexes qui fonctionnent et échouent en tant qu'unité unique. Par exemple, si vous avez une base de données principale et une base de données répliquée, les deux bases de données appartiennent au même composant d'application (AppComponent).

AWS Resilience Hub détermine quelles AWS ressources peuvent appartenir à quel type de AppComponent. Par exemple, un `DBInstance` peut appartenir à `AWS::ResilienceHub::DatabaseAppComponent` mais pas à`AWS::ResilienceHub::ComputeAppComponent`.

État de conformité de l'application

AWS Resilience Hub indique les types d'état de conformité suivants pour vos applications.

Politique respectée

On estime que l'application atteindra ses objectifs de RTO et de RPO définis dans la politique. Tous ses composants répondent aux objectifs politiques définis. Par exemple, vous avez sélectionné un objectif de RTO et de RPO de 24 heures pour les perturbations dans toutes les régions AWS . AWS Resilience Hub peut voir que vos sauvegardes sont copiées dans votre région de secours. Vous êtes toujours tenu de maintenir une restauration à partir d'une procédure d'exploitation standard (SOP) de sauvegarde, de la tester et de la chronométrer. Cela figure dans les recommandations opérationnelles et fait partie de votre score de résilience global.

Politique violée

Il n'a pas été possible d'estimer que l'application atteindra les objectifs de RTO et de RPO définis dans la politique. Un ou plusieurs d'entre eux AppComponents ne répondent pas aux objectifs de la politique. Par exemple, vous avez sélectionné un objectif RTO et RPO de 24 heures pour les

interruptions entre les AWS régions, mais la configuration de votre base de données n'inclut aucune méthode de restauration entre régions, telle qu'une réplication globale et des copies de sauvegarde.

Non évalué

La demande nécessite une évaluation. Il n'est actuellement ni évalué ni suivi.

Changements détectés

Une nouvelle version publiée de l'application n'a pas encore été évaluée.

Détection des écarts

AWS Resilience Hub exécute une notification de dérive lors de l'exécution d'une évaluation de votre application afin de vérifier si les modifications apportées aux AppComponent configurations ont affecté le statut de conformité de votre application. En outre, il vérifie et détecte les modifications telles que l'ajout ou la suppression de ressources dans les sources d'entrée de l'application et en informe. À des fins de comparaison, AWS Resilience Hub utilise l'évaluation précédente dans laquelle le composant de l'application respectait la politique. AWS Resilience Hub détecte les types de dérives suivants :

- Déviation de la politique d'application — Ce type de dérive identifie tous AppComponents ceux qui étaient conformes à la politique lors de l'évaluation précédente mais qui ne l'ont pas été lors de l'évaluation actuelle.
- Dérive des ressources de l'application : ce type de dérive identifie toutes les ressources dérivées dans la version actuelle de l'application.

Évaluation de la résilience

AWS Resilience Hub utilise une liste de lacunes et de solutions potentielles pour mesurer l'efficacité d'une politique sélectionnée en matière de reprise et de poursuite après un sinistre. Il évalue le statut de conformité de chaque composant d'application ou de chaque application à la politique. Ce rapport inclut des recommandations d'optimisation des coûts et des références aux problèmes potentiels.

Score de résilience

AWS Resilience Hub génère un score qui indique dans quelle mesure votre application suit nos recommandations pour respecter la politique de résilience, les alarmes, les procédures opérationnelles standard (SOPs) et les tests de l'application.

Type de perturbation

AWS Resilience Hub vous aide à évaluer la résilience face aux types de pannes suivants :

Application

L'infrastructure est saine, mais l'application ou la pile logicielle ne fonctionne pas comme il se doit. Cela peut se produire après le déploiement d'un nouveau code, des modifications de configuration, une corruption de données ou un dysfonctionnement des dépendances en aval.

Infrastructure cloud

L'infrastructure cloud ne fonctionne pas comme prévu en raison d'une panne. Une panne peut survenir en raison d'une erreur locale dans un ou plusieurs composants. Dans la plupart des cas, ce type de panne est résolu en redémarrant, en recyclant ou en rechargeant les composants défectueux.

Interruption de l'infrastructure cloud AZ

Une ou plusieurs zones de disponibilité ne sont pas disponibles. Ce type de panne peut être résolu en passant à une autre zone de disponibilité.

Incident dans la région d'infrastructure cloud

Une ou plusieurs régions ne sont pas disponibles. Ce type d'incident peut être résolu en passant à un autre Région AWS.

AWS FIS expériences

AWS Resilience Hub recommande des expériences utilisant AWS FIS des actions pour vérifier la résilience des applications face à différents types de pannes. Ces pannes incluent les applications, l'infrastructure, les zones de disponibilité (AZ) ou les Région AWS incidents liés aux composants de l'application.

Ces expériences vous permettent d'effectuer les opérations suivantes :

- Injectez un échec.
- Vérifiez que les alarmes peuvent détecter une panne.
- Vérifiez que les procédures de restauration, ou procédures opérationnelles standard (SOPs), fonctionnent correctement pour récupérer l'application après une panne.

Tests pour SOPs mesurer le RTO de charge de travail estimé et le RPO de charge de travail estimé. Vous pouvez tester différentes configurations d'applications et mesurer si le RTO et le RPO de sortie répondent aux objectifs définis dans votre politique.

ARRÊT

Une procédure opérationnelle standard (SOP) est un ensemble d'étapes prescriptives conçues pour restaurer efficacement votre application en cas de panne ou d'alarme. Sur la base de l'évaluation de l'application, AWS Resilience Hub recommande un ensemble de mesures SOPs et il est recommandé de les préparer, de les tester et de SOPs les mesurer avant une interruption afin de garantir une reprise rapide.

AWS Resilience Hub personas

La création d'une application d'entreprise nécessite un effort de collaboration entre différentes équipes interfonctionnelles telles que l'infrastructure, la continuité des activités, le propriétaire de l'application et les autres parties prenantes responsables de la surveillance des applications. Les différentes personnalités issues des différentes équipes contribuent à la création et à la gestion des applications AWS Resilience Hub, chacune ayant un rôle et des responsabilités différents. Pour en savoir plus sur l'octroi d'autorisations à différentes personnes, consultezthe section called "AWS Resilience Hub référence aux personas et aux autorisations IAM".

Pour commencer à créer des applications et à exécuter des évaluations dans AWS Resilience Hub, nous vous recommandons de créer les personnages suivants :

- Gestionnaire d'applications d'infrastructure — Les utilisateurs possédant cette personnalité sont responsables de la mise en place, de la configuration et de la maintenance des ressources de l'infrastructure et des applications, afin de garantir la fiabilité et la sécurité de l'application. Leurs responsabilités sont notamment les suivantes :
  - Veiller à ce que les applications soient déployées et mises à jour régulièrement
  - Surveillance des performances du système
  - Résolution des problèmes
  - Mise en œuvre de plans de sauvegarde et de reprise après sinistre
- Responsable de la continuité des activités : les utilisateurs dotés de cette personnalité sont chargés de dicter les politiques des applications et de déterminer le caractère critique des applications pour l'entreprise. Leurs responsabilités sont notamment les suivantes :
  - Prendre des décisions clés lors de l'élaboration des politiques

  - Évaluation de la criticité de l'activité
  - Allocation de ressources pour les applications critiques
  - Évaluation et gestion des risques
- Propriétaire de l'application — Les utilisateurs possédant cette personnalité ont la responsabilité de garantir la haute disponibilité et la fiabilité des applications. Leurs responsabilités sont notamment les suivantes :
  - Définition d'identifiants de performance clés pour mesurer et surveiller les performances des applications et identifier les goulots d'étranglement
  - Organisation de formations pour de multiples parties prenantes
  - S'assurer que la documentation suivante est up-to-date :
    - Architecture d'application
    - Processus de déploiement
    - Configurations de surveillance
    - Techniques d'optimisation des performances
- Accès en lecture seule : les utilisateurs possédant ce personnage sont limités aux autorisations en lecture seule. Leurs responsabilités incluent le maintien de la visibilité et la supervision des performances et de l'état de santé d'une application en surveillant le score de résilience, les recommandations opérationnelles et les recommandations de résilience. En outre, ils sont également chargés d'identifier les problèmes, les tendances et les domaines à améliorer afin de garantir que l'application répond aux objectifs de l'organisation.

AWS Resilience Hub ressources prises en charge

Les ressources qui affectent les performances des applications en cas d'interruption sont entièrement prises en charge par des ressources AWS Resilience Hub de haut niveau telles que `AWS::RDS::DBInstance` et`AWS::RDS::DBCluster`.

Pour en savoir plus sur les autorisations requises AWS Resilience Hub pour inclure les ressources de tous les services pris en charge dans votre évaluation, consultezthe section called “AWSResilienceHubAsssessmentExecutionPolicy”.

AWS Resilience Hub prend en charge les ressources des AWS services suivants :

- Calcul
  - Amazon Elastic Compute Cloud (Amazon EC2)

> **Note**
>
> AWS Resilience Hub ne prend pas en charge l'ancien format Amazon Resource Name (ARN) pour accéder aux EC2 ressources Amazon. Le nouveau format ARN utilise votre identifiant de AWS compte et permet d'améliorer la capacité de baliser les ressources de votre cluster. Il permet également de suivre le coût des services et des tâches exécutés dans votre cluster.
>
> - Ancien format (obsolète) — `arn:aws:ec2:<region>::instance/<instance-id>`
> - Nouveau format — `arn:aws:ec2:<region>:<account-id>:instance/<instance-id>`
>
> Pour plus d'informations sur le nouveau format ARN, consultez la section Migration de votre déploiement Amazon ECS vers le nouveau format d'ARN et d'ID de ressource.

  - AWS Lambda
  - Amazon Elastic Kubernetes Service (Amazon EKS)
  - Amazon Elastic Container Service (Amazon ECS)
  - AWS Step Functions
- Base de données
  - Amazon Relational Database Service (Amazon RDS)
  - Amazon DynamoDB
  - Amazon DocumentDB
  - Amazon ElastiCache
- Réseau et diffusion de contenu
  - Amazon Route 53
  - Elastic Load Balancing
  - Traduction d'adresses réseau (NAT)
- Stockage
  - Amazon Elastic Block Store (Amazon EBS)
  - Amazon Elastic File System (Amazon EFS)
  - Amazon Simple Storage Service (Amazon S3)
  - Serveur FSx de fichiers Amazon pour Windows

- Autres
  - Amazon API Gateway
  - Contrôleur Amazon Application Recovery (ARC) (Amazon ARC)
  - Amazon Simple Notification Service
  - Amazon Simple Queue Service
  - AWS Auto Scaling
  - AWS Backup
  - AWS Reprise après sinistre élastique

> **Note**
>
> - AWS Resilience Hub fournit une transparence supplémentaire pour les ressources de votre application en vous permettant de visualiser les instances prises en charge pour chaque ressource. En outre, AWS Resilience Hub fournit des recommandations de résilience plus précises en identifiant une instance unique de chaque ressource tout en découvrant les instances de ressource au cours du processus d'évaluation. Pour plus d'informations sur l'ajout d'instances de ressources à votre application, consultezModification des ressources AWS Resilience Hub de l'application.
> - AWS Resilience Hub prend en charge Amazon EKS et Amazon ECS sur AWS Fargate.
> - AWS Resilience Hub soutient l'évaluation des AWS Backup ressources dans le cadre des services suivants :
> - Amazon EBS
> - Amazon EFS
> - Amazon S3
> - Base de données mondiale Amazon Aurora
> - Amazon DynamoDB
> - Services Amazon RDS
> - Serveur FSx de fichiers Amazon pour Windows
> - Amazon ARC in AWS Resilience Hub évalue uniquement Amazon DynamoDB global, Elastic Load Balancing, Amazon RDS et les groupes. AWS Auto Scaling
> - AWS Resilience Hub Pour évaluer les ressources interrégionales, regroupez-les dans un seul composant d'application. Pour plus d'informations sur les ressources prises en charge

par chacun des composants de l' AWS Resilience Hub application et les ressources de regroupement, consultez Regroupement de ressources dans un composant d'application.

- Actuellement, AWS Resilience Hub ne prend pas en charge les évaluations interrégionales pour les clusters Amazon EKS si le cluster Amazon EKS est situé ou si l'application est créée dans une région où l'option d'inscription est activée AWS .
- Actuellement, AWS Resilience Hub évalue uniquement les types de ressources Kubernetes suivants :
  - Déploiements
  - ReplicaSets
  - Capsules

AWS Resilience Hub ignore les types de ressources suivants :

- Ressources qui n'affectent pas le RTO de charge de travail estimé ou le RPO de charge de travail estimé — Les ressources telles que celles `AWS::RDS::DBParameterGroup` qui n'affectent pas le RTO de charge de travail estimé ou le RPO de charge de travail estimé sont ignorées par. AWS Resilience Hub
- Ressources non de niveau supérieur : importe AWS Resilience Hub uniquement des ressources de niveau supérieur, car elles peuvent obtenir d'autres propriétés en interrogeant les propriétés des ressources de niveau supérieur. Par exemple, `AWS::ApiGateway::RestApi` et `AWS::ApiGatewayV2::Api` sont des ressources prises en charge pour Amazon API Gateway. Cependant, il ne `AWS::ApiGatewayV2::Stage` s'agit pas d'une ressource de haut niveau. Il n'est donc pas importé par AWS Resilience Hub.

> **Note**
>
> Ressources non prises en charge
>
> - Vous ne pouvez pas identifier plusieurs ressources en utilisant AWS Resource Groups (Amazon Route 53 RecordSets et API-GW HTTP) et les ressources Amazon Aurora Global. Si vous souhaitez analyser ces ressources dans le cadre de votre évaluation, vous devez les ajouter manuellement à l'application. Toutefois, lorsque vous ajoutez des ressources Amazon Aurora Global à des fins d'évaluation, celles-ci doivent être regroupées avec le composant d'application de l'instance Amazon RDS. Pour plus d'informations sur la

modification des ressources, consultezthe section called "Modification des ressources de l'application".

- Ces ressources peuvent affecter la restauration des applications, mais elles ne sont pas totalement prises en charge pour le AWS Resilience Hub moment. AWS Resilience Hub s'efforce d'avertir les utilisateurs des ressources non prises en charge si l'application est sauvegardée par une AWS CloudFormation pile, un fichier d'état Terraform ou une application AWS Resource Groups MyApplications.
- Au cours du processus d'importation des ressources d'une application dans AWS Resilience Hub, certaines ressources peuvent être ignorées. Lorsque les ressources sont ignorées, cela signifie qu'elles ne peuvent pas du tout être importées. Cependant, les ressources marquées comme non prises en charge ne sont actuellement pas compatibles avec, AWS Resilience Hub mais elles pourraient être prises en charge à l'avenir, ce qui leur permettra d'être incluses dans la demande d'évaluation. En outre, AWS Resilience Hub vous pouvez ignorer certaines ressources si elles ne sont pas prises en charge par AWS Resource Groups. Pour plus d'informations sur les ressources prises en charge par AWS Resource Groups, consultez les sections Types de ressources que vous pouvez utiliser avec AWS Resource Groups et Éditeur de balises.

AWS Resilience Hub et MyApplications

Le widget Resiliency du tableau de bord MyApplications rationalise le processus d'évaluation et de surveillance de la résilience des applications. Il vous permet d'évaluer rapidement la résilience de vos applications définies dans MyApplications sans avoir à les recréer manuellement dans la AWS Resilience Hub console. Cette approche intégrée combine les capacités de gestion des applications de MyApplications avec les fonctionnalités d'évaluation de la résilience de AWS Resilience Hub, ce qui vous permet de tirer parti des points forts des deux plateformes. En réunissant les définitions des applications et les fonctionnalités d'évaluation de la résilience, le widget Resiliency simplifie le flux de travail, vous permettant d'accéder aux informations pertinentes et de prendre des mesures pour améliorer la résilience à partir d'un emplacement centralisé. Lorsqu'une application est évaluée à partir du widget Resiliency, AWS Resilience Hub effectue les opérations suivantes :

- Crée l'application sélectionnée dans AWS Resilience Hub.
- Découvre et cartographie automatiquement les ressources associées au modèle.
- Crée et attribue une nouvelle politique de résilience avec des valeurs prédéfinies pour l'objectif de temps de restauration (RTO) et l'objectif de point de restauration (RPO). Cela représente quatre

heures pour le RTO et une heure pour le RPO. Après avoir généré une évaluation, vous pouvez modifier la politique de résilience ou en attribuer une autre depuis la AWS Resilience Hub console. Pour plus d'informations sur la mise à jour de la politique de résilience et l'attachement d'une autre stratégie, consultezGestion des politiques de résilience.

- Évalue la résilience de l'application par rapport au RTO et au RPO définis dans la politique de résilience afin d'identifier les domaines nécessitant des améliorations de l'architecture de l'application. Les scénarios de défaillance incluent les défaillances de zone de disponibilité, les pannes régionales et d'autres perturbations potentielles.
- Surveille en permanence les ressources de l'application et les modifications de configuration après l'évaluation initiale, en fournissant des alertes ou des mises à jour si des modifications ont un impact sur la résilience de l'application.

> **Note**
>
> Avant de commencer les évaluations, nous vous recommandons d'évaluer les coûts potentiels liés à l'exécution des évaluations à l'aide de AWS Resilience Hub. Pour obtenir des informations détaillées sur les prix, consultez les AWS Resilience Hub tarifs.

Après avoir évalué votre application, vous pouvez accéder à toutes les fonctionnalités de AWS Resilience Hub depuis le widget en choisissant Go AWS Resilience Hub to pour afficher les détails de l'application dans la AWS Resilience Hub console. Le processus d'inclusion des candidatures de MyApplications dans AWS Resilience Hub est régi par les règles et contraintes suivantes :

- Vous ne pouvez associer qu'une seule application MyApplications à une application dans AWS Resilience Hub. En d'autres termes, vous pouvez associer une application MyApplications à une AWS Resilience Hub application soit en exécutant une évaluation à partir du widget Resiliency dans le tableau de bord MyApplications, soit en effectuant la Utilisation des applications MyApplications procédure tout en décrivant l'application dans la console. AWS Resilience Hub
- Vous ne pouvez inclure, évaluer et consulter que les applications MyApplications résidant dans la même AWS région et dans les mêmes limites de AWS compte que votre environnement MyApplications. Les applications créées dans différentes AWS régions ou sous AWS des comptes distincts ne seront pas visibles ou accessibles via ce widget.
- Vous pouvez uniquement ajouter, supprimer et mettre à jour des ressources depuis le tableau de bord MyApplications. Lorsque vous modifiez les ressources de l'application depuis le tableau

de bord MyApplications, vous devez les réimporter AWS Resilience Hub pour afficher les modifications apportées aux ressources dans. AWS Resilience Hub

En savoir plus

Pour plus d'informations sur la gestion des applications et des ressources dans le tableau de bord MyApplications, consultez les rubriques suivantes de la AWS Console Home documentation :

- À quoi sert MyApplications ? AWS
- Création de votre première application dans MyApplications
- Gestion des ressources
- Widget de résilience

Pour plus d'informations sur la description des applications et l'exécution d'évaluations dans AWS Resilience Hub, consultez les rubriques suivantes :

- Pour exécuter une évaluation de la résilience d'une application MyApplications existante à partir du widget Resiliency pour la première fois
- Pour réexécuter une évaluation de résilience pour une application MyApplications existante à partir du widget Resiliency
- Consulter le résumé de l'évaluation dans le widget Resiliency

Mise en route

Cette section décrit comment commencer à utiliser AWS Resilience Hub. Cela inclut la création d'autorisations AWS Identity and Access Management (IAM) pour un compte.

Rubriques

- Prérequis
- Ajoutez une application à AWS Resilience Hub

Prérequis

Avant de pouvoir utiliser le AWS Resilience Hub, vous devez remplir les conditions préalables suivantes :

- AWS comptes — Créez un ou plusieurs AWS comptes pour chaque type de compte (primary/secondary/resourcecomptes) que vous souhaitez utiliser dans ce cadre AWS Resilience Hub. Pour plus d'informations sur la création et la gestion de AWS comptes, consultez les rubriques suivantes :
  - Premier AWS utilisateur — Mise en route : Êtes-vous un nouvel AWS utilisateur ?
  - Gestion AWS du compte — https://docs.aws.amazon.com/accounts/latest/reference/managing-accounts.html
- AWS Identity and Access Management Autorisations (IAM) — Après avoir créé les AWS comptes, vous devez configurer les rôles requis et les autorisations IAM pour chacun des comptes que vous avez créés. Par exemple, si vous avez créé un AWS compte pour accéder aux ressources de l'application, vous devez configurer un nouveau rôle et configurer les autorisations IAM nécessaires pour accéder AWS Resilience Hub aux ressources de l'application depuis votre compte. Pour en savoir plus sur les autorisations IAM, consultez the section called "Comment AWS Resilience Hub fonctionne avec IAM" et pour plus d'informations sur l'ajout d'une politique au rôle, consultezthe section called "Définition de la politique de confiance à l'aide du fichier JSON".

  Pour commencer rapidement à ajouter des autorisations IAM aux utilisateurs, aux groupes et aux rôles, vous pouvez utiliser nos politiques AWS gérées (the section called "AWS politiques gérées"). Il est plus facile d'utiliser des politiques AWS gérées pour couvrir les cas d'utilisation courants disponibles chez vous Compte AWS que de rédiger vous-même des politiques. AWS Resilience

Hub ajoute des autorisations supplémentaires à une politique AWS gérée afin d'étendre le support à d'autres AWS services et d'inclure de nouvelles fonctionnalités. Par conséquent :

- Si vous êtes déjà client et que vous souhaitez que votre application utilise les dernières améliorations apportées à votre évaluation, vous devez publier une nouvelle version de l'application, puis exécuter une nouvelle évaluation. Pour plus d'informations, consultez les rubriques suivantes :
  - the section called "Publier une nouvelle version de l'application"
  - the section called "Exécution d'évaluations de résilience dans AWS Resilience Hub"
- Si vous n'utilisez pas de politiques AWS gérées pour attribuer les autorisations IAM appropriées aux utilisateurs, aux groupes et aux rôles, vous devez configurer ces autorisations manuellement. Pour plus d'informations sur les politiques AWS gérées, consultezthe section called "AWSResilienceHubAsssessmentExecutionPolicy".

Ajoutez une application à AWS Resilience Hub

AWS Resilience Hub propose une évaluation et une validation de la résilience qui s'intègrent au cycle de vie de développement de vos logiciels. AWS Resilience Hub vous aide à préparer et à protéger vos AWS applications de manière proactive contre les perturbations en :

- Découverte des faiblesses en matière de résilience.
- Estimation de la possibilité d'atteindre votre objectif de temps de restauration (RTO) et votre objectif de point de reprise (RPO) cibles.
- Résoudre les problèmes avant leur mise en production.

Cette section vous explique comment ajouter une application. Vous collectez des ressources à partir d'une application MyApplications existante, de AWS CloudFormation piles ou AWS Resource Groups créez une politique de résilience appropriée. Après avoir décrit une application, vous pouvez la publier et générer un rapport d'évaluation sur la résilience de votre application. AWS Resilience Hub Vous pouvez ensuite utiliser les recommandations issues de l'évaluation pour améliorer la résilience. Vous pouvez exécuter une autre évaluation, comparer les résultats, puis itérer jusqu'à ce que le RTO de charge de travail estimé et le RPO de charge de travail estimé atteignent vos objectifs de RTO et de RPO.

Rubriques

- Commencez par ajouter une application

- Sélectionnez le mode de gestion de cette application
- Ajouter des collections de ressources
- Définissez le RTO et le RPO
- Configuration des évaluations planifiées et des notifications de dérive
- Autorisations de configuration
- Configuration des paramètres de configuration de l'application
- Ajout de balises
- Révisez et publiez votre AWS Resilience Hub candidature
- Procédez à une évaluation de votre AWS Resilience Hub candidature

Commencez par ajouter une application

Commencez AWS Resilience Hub en décrivant les détails de votre AWS application et en rédigeant un rapport pour évaluer la résilience.

Pour commencer, sur la page d' AWS Resilience Hub accueil, sous Commencer, sélectionnez Ajouter une application.

Pour en savoir plus sur les coûts et la facturation associés AWS Resilience Hub, consultez la section AWS Resilience Hub tarification.

Décrivez les détails de votre candidature dans AWS Resilience Hub

Cette section explique comment décrire les détails de votre AWS application existante dans AWS Resilience Hub.

Pour décrire les détails de votre candidature

1. Entrez un nom pour l'application.
2. (Facultatif) Entrez une description de l'application.

Suivant

Sélectionnez le mode de gestion de cette application

Sélectionnez le mode de gestion de cette application

Outre les AWS CloudFormation piles AWS Resource Groups, les applications MyApplications et les fichiers d'état Terraform, vous pouvez ajouter des ressources situées sur des clusters Amazon Elastic Kubernetes Service (Amazon EKS). En d'autres termes, AWS Resilience Hub vous permet d'ajouter des ressources situées sur vos clusters Amazon EKS en tant que ressources facultatives. Cette section propose les options suivantes, qui vous aident à déterminer l'emplacement des ressources de votre application.

- Collections de ressources : sélectionnez cette option si vous souhaitez découvrir les ressources de l'une des collections de ressources. Les collections de ressources incluent des AWS CloudFormation piles AWS Resource Groups, des applications MyApplications et des fichiers d'état Terraform.

  Si vous sélectionnez cette option, vous devez effectuer l'une des procédures décrites dansthe section called "Ajouter des collections de ressources".
- EKS uniquement : sélectionnez cette option si vous souhaitez découvrir des ressources provenant d'espaces de noms au sein des clusters Amazon EKS.

  Si vous sélectionnez cette option, vous devez effectuer la procédure dans the section called "Ajouter des clusters EKS"
- Collections de ressources et EKS : sélectionnez cette option si vous souhaitez découvrir des ressources provenant de AWS CloudFormation piles AWS Resource Groups, de fichiers d'état Terraform et de clusters Amazon EKS.

  Si vous sélectionnez cette option, effectuez l'une des procédures dans, the section called "Ajouter des collections de ressources" puis terminez la procédure dansthe section called "Ajouter des clusters EKS".

> **Note**
>
> Pour plus d'informations sur le nombre de ressources prises en charge par application, consultez la section Service Quotas.

Suivant

Ajouter des collections de ressources

Ajouter des collections de ressources

Cette section décrit les options suivantes que vous pouvez utiliser pour constituer la base de la structure de votre application :

- Ajouter des collections de ressources
- Ajouter des clusters EKS

Ajouter des collections de ressources

Cette section décrit les méthodes suivantes que vous utilisez pour constituer la base de la structure de votre application :

- Utiliser des AWS CloudFormation piles
- En utilisant AWS Resource Groups
- Utilisation des applications MyApplications
- Utilisation des fichiers d'état Terraform

Utiliser des AWS CloudFormation piles

Choisissez les AWS CloudFormation piles contenant les ressources que vous souhaitez utiliser dans l'application que vous décrivez. Les piles peuvent provenir de celle Compte AWS que vous utilisez pour décrire l'application, ou elles peuvent provenir de différents comptes ou de différentes régions.

Pour découvrir les ressources qui constituent la base de la structure de votre application

1. Sélectionnez CloudFormation stack pour découvrir vos ressources basées sur stack.
2. Choisissez les piles dans la liste déroulante Choisissez les piles associées à votre région et à votre Compte AWS région.

   Pour utiliser des piles situées dans une région différente Compte AWS, ou les deux, cliquez sur la flèche droite à côté de Ajouter une pile en dehors de AWS la région et entrez le nom de ressource Amazon (ARN) de la pile dans le champ Entrez un ARN de pile, puis choisissez Ajouter un ARN de pile. Pour plus d'informations ARNs, consultez Amazon Resource Names (ARNs) dans le manuel de référence AWS général.

En utilisant AWS Resource Groups

Choisissez ceux AWS Resource Groups qui contiennent les ressources que vous souhaitez utiliser dans l'application que vous décrivez.

Pour découvrir les ressources qui constituent la base de la structure de votre application

1. Sélectionnez Groupes de ressources pour découvrir ceux AWS Resource Groups qui contiennent les ressources.
2. Choisissez des ressources dans la liste déroulante Choisissez un groupe de ressources.

   Pour AWS Resource Groups les utiliser dans une région différente Compte AWS, ou les deux, cliquez sur la flèche droite à côté de l'ARN du groupe de ressources : et entrez le nom de la ressource Amazon (ARN) AWS Resource Groups dans le champ Entrez un ARN de groupe de ressources, puis choisissez Ajouter un ARN de groupe de ressources. Pour plus d'informations ARNs, consultez Amazon Resource Names (ARNs) dans le manuel de référence AWS général.

Utilisation des applications MyApplications

Choisissez l'application MyApplications dans laquelle vous souhaitez inclure AWS Resilience Hub

Pour inclure l'application MyApplications dans AWS Resilience Hub

1. Sélectionnez MyApplications.
2. Choisissez une application dans la liste déroulante Sélectionner une application.

Utilisation des fichiers d'état Terraform

Choisissez le fichier d'état Terraform qui contient les ressources de votre compartiment Amazon S3 que vous souhaitez utiliser dans l'application que vous décrivez. Vous pouvez accéder à l'emplacement de votre fichier d'état Terraform ou fournir un lien vers un fichier d'état Terraform auquel vous avez accès et qui se trouve dans une autre région.

> **Note**
>
> AWS Resilience Hub prend en charge la version du fichier d'état Terraform `0.12` et les versions ultérieures.

Pour découvrir les ressources qui constituent la base de la structure de votre application

1. Sélectionnez les fichiers d'état Terraform pour découvrir les ressources de votre compartiment S3.
2. Dans la section Select state files : :, choisissez Browse S3 pour accéder à l'emplacement de votre fichier d'état Terraform.

   Pour utiliser les fichiers d'état Terraform situés dans une autre région, fournissez le lien vers l'emplacement du fichier d'état Terraform dans le champ URI S3, puis choisissez Ajouter une URL S3.

   La limite pour les fichiers d'état Terraform est de 4 mégaoctets (Mo).
3. Dans la boîte de dialogue Choisir une archive dans S3, sélectionnez votre bucket Amazon Simple Storage Service dans la section Buckets.
4. Dans la section Objets, sélectionnez une clé, puis choisissez Choisir.

Ajouter des clusters EKS

Cette section explique comment utiliser les clusters Amazon EKS pour constituer la base de la structure de votre application.

> **Note**
>
> Vous devez disposer d'autorisations Amazon EKS et de rôles IAM supplémentaires pour vous connecter au cluster Amazon EKS. Pour plus d'informations sur l'ajout d'autorisations Amazon EKS à compte unique et multicompte et sur des rôles IAM supplémentaires pour se connecter au cluster, consultez les rubriques suivantes :
>
> - AWS Resilience Hub référence des autorisations d'accès
> - the section called "Activation de AWS Resilience Hub l'accès à votre cluster Amazon EKS"

Choisissez les clusters et les espaces de noms Amazon EKS qui contiennent les ressources que vous souhaitez utiliser dans l'application que vous décrivez. Les clusters Amazon EKS peuvent être ceux Compte AWS que vous utilisez pour décrire l'application, ou ils peuvent provenir de différents comptes ou de différentes régions.

> **Note**
>
> AWS Resilience Hub Pour évaluer vos clusters Amazon EKS, vous devez ajouter manuellement les espaces de noms appropriés à chacun des clusters Amazon EKS dans la section Clusters et espaces de noms EKS. Le nom de l'espace de noms doit correspondre exactement au nom de l'espace de noms de vos clusters Amazon EKS.

Pour ajouter des clusters Amazon EKS

1. Dans 1. Sélectionnez la section Clusters EKS, choisissez les clusters Amazon EKS dans la liste déroulante Choisir les clusters EKS associés à votre région Compte AWS et à votre région.
2. Pour utiliser des clusters Amazon EKS situés dans une région différente Compte AWS, ou les deux, cliquez sur la flèche droite à côté de Ajouter un cluster EKS dans un compte ou une région différent et entrez le nom de ressource Amazon (ARN) du cluster Amazon EKS dans le champ Enter an EKS ARN, puis choisissez Add EKS ARN. Pour plus d'informations ARNs, consultez Amazon Resource Names (ARNs) dans le manuel de référence AWS général.

   Pour plus d'informations sur l'ajout d'autorisations permettant d'accéder aux clusters Amazon Elastic Kubernetes Service interrégionaux, consultez. the section called "Activation de AWS Resilience Hub l'accès à votre cluster Amazon EKS"

Pour ajouter des espaces de noms à partir des clusters Amazon EKS sélectionnés

1. Dans la section Ajouter des espaces de noms, dans le tableau des clusters et espaces de noms EKS, sélectionnez le bouton radio situé à gauche du nom du cluster Amazon EKS, puis choisissez Mettre à jour les espaces de noms.

   Vous pouvez identifier les clusters Amazon EKS de la manière suivante :

   - Nom du cluster EKS : indique le nom des clusters Amazon EKS sélectionnés.
   - Nombre d'espaces de noms : indique le nombre d'espaces de noms sélectionnés dans les clusters Amazon EKS.
   - État — Indique si AWS Resilience Hub les espaces de noms des clusters Amazon EKS sélectionnés ont été inclus dans votre application. Vous pouvez identifier le statut à l'aide des options suivantes :

- Espace de noms requis : indique que vous n'avez inclus aucun espace de noms provenant du cluster Amazon EKS.
- Espaces de noms ajoutés : indique que vous avez inclus un ou plusieurs espaces de noms issus du cluster Amazon EKS.

2. Pour ajouter un espace de noms, dans la boîte de dialogue Mettre à jour les espaces de noms, choisissez Ajouter un nouvel espace de noms.

   La boîte de dialogue Mettre à jour les espaces de noms affiche tous les espaces de noms que vous avez sélectionnés dans votre cluster Amazon EKS, sous forme d'option modifiable.

3. Dans la boîte de dialogue Mettre à jour les espaces de noms, vous disposez des options de modification suivantes :

   - Pour ajouter un nouvel espace de noms, choisissez Ajouter un nouvel espace de noms, puis entrez le nom de l'espace de noms dans le champ Namespace.

     Le nom de l'espace de noms doit correspondre exactement au nom de l'espace de noms de votre cluster Amazon EKS.
   - Pour supprimer un espace de noms, choisissez Supprimer situé à côté de l'espace de noms.
   - Pour appliquer les espaces de noms sélectionnés à tous les clusters Amazon EKS, choisissez Appliquer les espaces de noms à tous les clusters EKS.

     Si vous choisissez cette option, votre sélection d'espace de noms précédente dans les autres clusters Amazon EKS sera remplacée par la sélection d'espace de noms actuelle.

4. Pour inclure les espaces de noms mis à jour dans votre application, choisissez Mettre à jour.

Suivant

Définissez le RTO et le RPO

Définissez le RTO et le RPO

Vous pouvez définir une nouvelle politique de résilience avec vos propres RTO/RPO targets, or you can choose an existing resiliency policy with predefined RTO/RPO cibles. Si vous souhaitez utiliser l'une des politiques de résilience existantes, sélectionnez Choisir une option de stratégie existante et sélectionnez une application cible existante dans la liste déroulante des options.

Pour définir vos propres objectifs RTO/RPO

1. Sélectionnez Créer une nouvelle option de politique de résilience.
2. Entrez le nom de la politique de résilience dans le champ Entrez le nom de la politique (sous Nom).

   Nous avons prérempli ce champ avec un nom généré automatiquement. Vous pouvez choisir d'utiliser le même nom ou de fournir un autre nom.
3. (Facultatif) Entrez une description de la politique de résilience dans la zone Description.
4. Définissez votre RTO/RPO dans la section Objectifs RTO/RPO.

   > **Note**
   >
   > - Nous avons prédéfini un RTO et un RPO par défaut pour votre application. Vous pouvez modifier le RTO et le RPO dès maintenant ou après avoir évalué l'application.
   > - AWS Resilience Hub vous permet de saisir une valeur zéro dans les champs RTO et RPO de votre politique de résilience. Cependant, lors de l'évaluation de votre candidature, le résultat d'évaluation le plus bas possible est proche de zéro. Par conséquent, si vous entrez une valeur zéro dans les champs RTO et RPO, les résultats du RTO de charge de travail estimé et du RPO de charge de travail estimé seront proches de zéro et le statut de conformité de votre application sera défini sur Policy violée.
5. Pour définir le RTO/RPO pour votre infrastructure et votre AZ, cliquez sur la flèche droite pour développer la section Infrastructure RTO et RPO.
6. Dans les cibles RTO/RPO, entrez une valeur numérique dans le champ, puis choisissez l'unité de temps que la valeur représente pour le RTO et le RPO.

   Répétez ces entrées pour l'infrastructure et la zone de disponibilité dans la section Infrastructure RTO et RPO.
7. (Facultatif) Si vous avez une application multirégionale et que vous souhaitez définir un RTO et un RPO régionaux, activez l'option Région - Facultatif.

   Dans RTO et RPO, entrez une valeur numérique dans le champ, puis choisissez l'unité de temps que la valeur représente pour le RTO et le RPO.

Suivant

the section called “Configuration de l'évaluation planifiée et de la notification de dérive”

Configuration des évaluations planifiées et des notifications de dérive

AWS Resilience Hub vous permet de configurer des évaluations planifiées et des notifications de dérive pour évaluer quotidiennement votre application et être averti lorsqu'une dérive est détectée.

Pour configurer la notification de dérive

1. Pour évaluer votre application au quotidien, activez l'option Évaluer automatiquement tous les jours.

   Si cette option est activée, le programme d'évaluation quotidien ne commence qu'après les périodes suivantes :

   - La demande est évaluée manuellement avec succès pour la première fois.
   - L'application est configurée avec un rôle IAM approprié.
   - Si votre application est configurée avec les autorisations utilisateur IAM actuelles, vous devez créer `AWSResilienceHubAsssessmentExecutionPolicy`

     rôle en utilisant la procédure appropriée dans the section called “Comment AWS Resilience Hub fonctionne avec IAM”.
2. Pour être averti en cas AWS Resilience Hub de détection de dérives par rapport aux politiques de résilience ou lorsque ses ressources ont dérivé, activez l'option Recevoir une notification lorsque l'application dérive.

   Si cette option est activée, pour recevoir des notifications de dérive, vous devez spécifier une rubrique Amazon Simple Notification Service (Amazon SNS). Pour fournir une rubrique Amazon SNS, dans la section Fournir une rubrique SNS, sélectionnez l'option Choisir une rubrique SNS et sélectionnez une rubrique Amazon SNS dans la liste déroulante Choisissez une rubrique SNS.

   > **Note**
   >
   > - Pour AWS Resilience Hub permettre de publier des notifications sur vos rubriques Amazon SNS, votre rubrique Amazon SNS doit être configurée avec les autorisations appropriées. Pour plus d'informations sur la configuration des autorisations,

consultezthe section called "Activation AWS Resilience Hub de la publication sur vos rubriques Amazon SNS".

- Les évaluations quotidiennes peuvent avoir un impact sur votre quota de courses. Pour plus d'informations sur les quotas, consultez la section AWS Resilience Hub Points de terminaison et quotas dans le manuel de référence AWS général.

Pour utiliser des rubriques Amazon SNS situées dans une région différente Compte AWS ou les deux, sélectionnez Enter SNS topic ARN (Enter SNS topic ARN) et entrez le nom de ressource Amazon (ARN) de la rubrique Amazon SNS dans le champ Provide an SNS topic. Pour plus d'informations ARNs, consultez Amazon Resource Names (ARNs) dans le manuel de référence AWS général.

Suivant

Autorisations de configuration

Autorisations de configuration

AWS Resilience Hub vous permet de configurer les autorisations nécessaires pour le compte principal et le compte secondaire afin de découvrir et d'évaluer les ressources. Cependant, vous devez exécuter la procédure séparément pour configurer les autorisations pour chaque compte.

Pour configurer les rôles IAM et les autorisations IAM

1. Pour sélectionner un rôle IAM existant qui sera utilisé pour accéder aux ressources du compte courant, sélectionnez un rôle IAM dans la liste déroulante Sélectionnez un rôle IAM.

> **Note**
>
> Pour une configuration entre comptes, si vous ne spécifiez pas les noms de ressources Amazon (ARNs) du rôle IAM dans le champ Entrez un rôle IAM ARN, vous AWS Resilience Hub utiliserez le rôle IAM que vous avez sélectionné dans la liste déroulante Sélectionnez un rôle IAM pour tous les comptes.

Si aucun rôle IAM n'est associé à votre compte, vous pouvez créer un rôle IAM en utilisant l'une des options suivantes :

- AWS Console IAM : si vous choisissez cette option, vous devez suivre la procédure décrite dans Pour créer votre AWS Resilience Hub rôle dans la console IAM.
- AWS CLI — Si vous choisissez cette option, vous devez effectuer toutes les étapes de la AWS CLI.
- CloudFormation modèle — Si vous choisissez cette option, selon le type de compte (compte principal ou compte secondaire), vous devez créer les rôles à l'aide du AWS CloudFormation modèle approprié.

2. Cliquez sur la flèche droite pour développer Ajouter un ou plusieurs rôles IAM à partir d'un compte croisé - Section facultative.
3. Pour sélectionner des rôles IAM à partir d'un compte croisé, entrez le ARNs rôle IAM dans le champ Entrez un ARN de rôle IAM. Assurez-vous que ARNs les rôles IAM que vous saisissez n'appartiennent pas au compte courant.
4. Si vous souhaitez utiliser l'utilisateur IAM actuel pour découvrir les ressources de votre application, cliquez sur la flèche droite pour développer la section Utiliser les autorisations utilisateur IAM actuelles et sélectionnez Je comprends que je dois configurer manuellement les autorisations pour activer les fonctionnalités requises. AWS Resilience Hub

   Si vous sélectionnez cette option, certaines AWS Resilience Hub fonctionnalités (telles que la notification de dérive) risquent de ne pas fonctionner comme prévu et les entrées que vous avez fournies pour créer une nouvelle application seront ignorées.

Suivant

Configuration des paramètres de configuration de l'application

Configuration des paramètres de configuration de l'application

Cette section vous permet de fournir les détails de votre prise en charge du basculement entre régions à l'aide de. AWS Elastic Disaster Recovery AWS Resilience Hub utilisera ces informations pour fournir des recommandations en matière de résilience.

Pour plus d'informations sur les paramètres de configuration de l'application, consultezParamètres de configuration de l'application.

Pour ajouter des paramètres de configuration d'application (facultatif)

1. Pour développer la section Paramètres de configuration de l'application, cliquez sur la flèche droite.
2. Entrez l'ID du compte de basculement dans le champ Identifiant du compte. Par défaut, nous avons prérempli ce champ avec votre identifiant de compte utilisé pour AWS Resilience Hub, qui peut être modifié.
3. Sélectionnez une région de basculement dans la liste déroulante des régions.

> **Note**
>
> Si vous souhaitez désactiver cette fonctionnalité, sélectionnez « — » dans la liste déroulante.

Suivant

Ajout de balises

Ajout de balises

Attribuez un tag ou un label à une AWS ressource pour rechercher et filtrer vos ressources, ou suivre vos AWS coûts.

(Facultatif) Pour ajouter des balises à votre application, choisissez Ajouter une nouvelle balise si vous souhaitez associer une ou plusieurs balises à l'application. Pour plus d'informations sur les balises, consultez la section Ressources de balisage dans le manuel de référence AWS général.

Choisissez Ajouter une application pour créer votre application.

Suivant

Révisez et publiez votre AWS Resilience Hub candidature

Révisez et publiez votre AWS Resilience Hub candidature

Après avoir créé l'application, vous pouvez toujours la consulter et modifier ses ressources. Lorsque vous avez terminé, choisissez Publier pour publier l'application.

> **Note**
>
> AWS Resilience Hub analyse les ressources de votre application en arrière-plan et vérifie si elles peuvent être regroupées de manière plus efficace afin d'améliorer la précision des évaluations. S'il AWS Resilience Hub identifie les ressources qui peuvent être regroupées selon les catégories pertinentes AppComponents, il affiche une alerte d'information sur les recommandations de regroupement de ressources dans l'onglet Structure de l'application de la page de l'application et vous pouvez les consulter en choisissant Réviser les recommandations. Pour de plus amples informations, veuillez consulter the section called "AWS Resilience Hub recommandations de regroupement de ressources".

Pour plus d'informations sur la révision de l'application et la modification de ses ressources, consultez les rubriques suivantes :

- the section called "Afficher le résumé de l'application"
- the section called "Modification des ressources de l'application"

Suivant

Procédez à une évaluation de votre AWS Resilience Hub candidature

Procédez à une évaluation de votre AWS Resilience Hub candidature

L'application que vous avez publiée est répertoriée sur la page Résumé.

Après avoir publié votre AWS Resilience Hub application, vous êtes redirigé vers la page de résumé de l'application où vous pouvez exécuter une évaluation de résilience. L'évaluation évalue la configuration de votre application par rapport à la politique de résilience attachée à votre application. Un rapport d'évaluation est généré qui montre comment votre application se mesure par rapport aux objectifs de votre politique de résilience.

Pour exécuter une évaluation de résilience

1. Sur la page de résumé des applications, choisissez Évaluer la résilience.
2. Dans la boîte de dialogue Exécuter l'évaluation de la résilience, entrez un nom unique pour le rapport ou utilisez le nom généré dans la zone Nom du rapport.
3. Cliquez sur Exécuter.

4. Après avoir été informé que le rapport d'évaluation a été généré, choisissez l'onglet Évaluations et votre évaluation pour afficher le rapport.
5. Cliquez sur l'onglet Révision pour consulter le rapport d'évaluation de votre demande.

En utilisant AWS Resilience Hub

AWS Resilience Hub vous aide à améliorer la résilience de vos applications AWS et à réduire le temps de restauration en cas de panne des applications.

Rubriques :

- AWS Resilience Hub résumé
- AWS Resilience Hub tableau de bord
- Décrire et gérer AWS Resilience Hub les applications
- Gestion des politiques de résilience
- Exécution et gestion d'évaluations de résilience dans AWS Resilience Hub
- Exécution et gestion des évaluations de résilience à partir du widget Resiliency
- Gérer les alarmes
- Gestion des procédures opérationnelles standard
- Gestion des AWS Fault Injection Service expériences
- Comprendre les scores de résilience
- Intégrer des recommandations opérationnelles dans votre application avec AWS CloudFormation

AWS Resilience Hub résumé

AWS Resilience Hub fournit un résumé visuel avec des tableaux et des graphiques qui vous donnent une at-a-glance vue de la posture de résilience de votre application sur plusieurs AWS services et ressources. Ce résumé visuel complet et concis vous permet d'identifier rapidement les lacunes potentielles en matière de résilience, de hiérarchiser les actions et de suivre les progrès réalisés pour améliorer la capacité de votre application à se remettre des perturbations. Lorsque vous choisissez Exporter, et si vous exportez les métriques pour la première fois, vous AWS Resilience Hub créez un nouveau compartiment Amazon S3 dans la région à partir de laquelle vous accédez AWS Resilience Hub. Ce compartiment Amazon S3 n'est créé que pour la première fois et sera utilisé pour enregistrer les métriques exportées une fois terminé avec succès. Des frais supplémentaires s'appliquent pour le stockage des données exportées dans Amazon S3. Pour plus d'informations sur ces frais, consultez la tarification d'Amazon S3.

Les tableaux et graphiques contenus dans les widgets vous aident à comprendre les points suivants :

- Vue d'ensemble du score de résilience global de l'application et de son état de fonctionnement actuel.
- Violations potentielles des politiques ou écarts par rapport aux meilleures pratiques en mettant en évidence les applications qui ne sont pas conformes aux politiques établies ou qui s'écartent des configurations recommandées. En outre, il met également en évidence des domaines spécifiques qui vous permettent de les prioriser et de les aborder.
- Ressources ou applications critiques qui nécessitent une attention immédiate.
- Recommandations pour améliorer les pratiques de résilience, telles que la mise en œuvre d'alarmes, la réalisation AWS Fault Injection Service (AWS FIS) d'expériences et l'établissement de procédures opérationnelles standard. Ces recommandations sont suivies au fil du temps, ce qui vous permet de suivre la progression de la mise en œuvre et de mesurer l'impact sur la posture de résilience globale de l'application.

Widgets

- État de la demande
- Principales recommandations en matière d'infrastructure par type de ressource
- Recommandations en matière d'infrastructure
- Recommandations opérationnelles non mises en œuvre
- Recommandations relatives aux alarmes
- Recommandations SOP
- AWS FIS recommandations d'expériences
- Applications présentant des dérives
- Score de résilience
- Les 10 meilleures applications en termes de score de résilience
- État de l'application par stratégie

État de la demande

Ce widget indique si vos applications sont conformes à la politique de résilience ou non. Choisissez le nombre adjacent au nombre d'applications dans la fenêtre contextuelle pour afficher toutes les applications associées dans le volet Applications. Pour afficher toutes les applications que vous avez créées, choisissez Afficher les applications. Pour plus d'informations sur la gestion des applications dans AWS Resilience Hub, consultezAfficher le résumé d'une AWS Resilience Hub demande.

Principales recommandations en matière d'infrastructure par type de ressource

Ce widget affiche le nombre de recommandations d'infrastructure pour chaque type de AWS ressource fourni lors de la dernière évaluation réussie afin d'améliorer leur niveau de résilience. Vous pouvez identifier les détails en les survolant ou en naviguant vers eux. Pour afficher toutes les applications que vous avez créées, choisissez Afficher les applications. Pour plus d'informations sur les recommandations en matière d'infrastructure, consultezRévision des recommandations en matière de résilience.

Recommandations en matière d'infrastructure

Ce widget répertorie jusqu'à 10 applications pour lesquelles le nombre maximum de recommandations en matière d'infrastructure a été fourni lors de la dernière évaluation réussie afin d'améliorer leur posture de résilience. Pour afficher toutes les applications que vous avez créées, choisissez Afficher les applications. Pour plus d'informations sur les recommandations en matière d'infrastructure, consultezRévision des recommandations en matière de résilience.

Vous pouvez identifier les détails à l'aide des éléments suivants :

- Nom de l'application : nom de l'application que vous avez fournie lors de sa définition AWS Resilience Hub.
- Nombre — Indique le nombre de recommandations en matière d'infrastructure fournies AWS Resilience Hub lors de la dernière évaluation réussie. Choisissez le numéro pour afficher toutes les recommandations relatives à l'infrastructure fournies dans le rapport d'évaluation.
- Dernière évaluation — Indique la date et l'heure auxquelles votre candidature a été évaluée avec succès pour la dernière fois.

Recommandations opérationnelles non mises en œuvre

Ce widget répertorie jusqu'à 10 applications présentant le nombre maximum de recommandations opérationnelles non mises en œuvre fournies lors de la dernière évaluation réussie afin d'améliorer leur posture de résilience. Pour afficher toutes les applications que vous avez créées, choisissez Afficher les applications. Pour plus d'informations sur les recommandations opérationnelles, consultezRévision des recommandations opérationnelles.

Vous pouvez identifier les détails à l'aide des éléments suivants :

- Nom de l'application : nom de l'application que vous avez fournie lors de sa définition AWS Resilience Hub.
- Nombre — Indique le nombre de recommandations opérationnelles fournies AWS Resilience Hub lors de la dernière évaluation réussie. Choisissez le numéro pour afficher toutes les recommandations opérationnelles non mises en œuvre dans le rapport d'évaluation.
- Heure de la dernière évaluation — Indique la date et l'heure auxquelles votre candidature a été évaluée avec succès pour la dernière fois.

Recommandations relatives aux alarmes

Ce widget répertorie toutes les recommandations CloudWatch d'Amazon relatives aux alarmes fournies pour améliorer la posture de résilience sur une période donnée. Les différentes catégories (Implémenté, Non implémenté et Exclu) indiquent leur état d'implémentation dans votre application. Vous pouvez consulter le nombre de recommandations CloudWatch d'alarme Amazon pour chaque catégorie en les survolant ou en accédant à celles-ci. Pour afficher toutes les applications que vous avez créées, choisissez Afficher les applications. Pour plus d'informations sur les recommandations relatives aux alarmes, consultezRévision des recommandations opérationnelles.

Recommandations SOP

Ce widget répertorie toutes les recommandations de procédures opérationnelles standard (SOP) fournies pour améliorer la posture de résilience sur une période sélectionnée. Les différentes catégories (Implémenté, Non implémenté et Exclu) indiquent leur état d'implémentation dans votre application. Vous pouvez consulter le nombre de recommandations SOP pour chaque catégorie en les survolant ou en naviguant jusqu'à elles. Pour afficher toutes les applications que vous avez créées, choisissez Afficher les applications. Pour plus d'informations sur les recommandations opérationnelles, consultezRévision des recommandations opérationnelles.

AWS FIS recommandations d'expériences

Ce widget répertorie toutes les recommandations d' AWS FIS expériences fournies pour améliorer la posture de résilience sur une période sélectionnée. Les différentes catégories (implémenté, non implémenté, partiellement implémenté et exclu) indiquent leur état d'implémentation dans votre application. Vous pouvez consulter le nombre de recommandations d' AWS FIS expériences pour chaque catégorie en les survolant ou en naviguant jusqu'à elles. Pour afficher toutes les applications que vous avez créées, choisissez Afficher les applications. Pour plus d'informations

sur les recommandations relatives aux AWS FIS expériences, consultezGestion des procédures opérationnelles standard.

Applications présentant des dérives

Ce widget répertorie toutes vos applications qui se sont éloignées de leur état de conformité précédent lors de la dernière évaluation réussie. Pour afficher toutes les applications que vous avez créées, choisissez Afficher les applications. Pour plus d'informations sur la gestion des applications dans AWS Resilience Hub, consultezAfficher le résumé d'une AWS Resilience Hub demande.

Vous pouvez identifier les détails à l'aide des éléments suivants :

- Nom de l'application : nom de l'application que vous avez fournie lors de sa définition AWS Resilience Hub.
- Dérives des politiques : choisissez le numéro adjacent au nom de l'application pour afficher tous les composants de l'application qui étaient conformes à la politique de l'évaluation précédente, mais qui ne l'étaient pas lors de l'évaluation en cours.
- Dérives des ressources : choisissez le chiffre ci-dessous pour afficher toutes les ressources dont la configuration a été modifiée lors de la dernière importation.

Score de résilience

Ce widget affiche la tendance du score de résilience de l'application sur une période sélectionnée pour un maximum de cinq applications. Vous pouvez consulter le score de résilience d'une application en survolant la ligne associée au nom de l'application ou en accédant à celle-ci, puis en choisissant le nom de l'application pour afficher le résumé de l'application. Pour afficher toutes les applications que vous avez créées, choisissez Afficher les applications. Pour plus d'informations sur le score de résilience, consultezComprendre les scores de résilience.

Les 10 meilleures applications en termes de score de résilience

Ce widget répertorie jusqu'à 10 applications ayant obtenu les scores de résilience les plus faibles lors de leurs évaluations les plus récentes, en mettant en évidence les applications qui nécessitent une attention immédiate pour améliorer leur résilience. Pour afficher toutes les applications que vous avez créées, choisissez Afficher les applications. Pour plus d'informations sur le score de résilience, consultezComprendre les scores de résilience.

Vous pouvez identifier les détails à l'aide des éléments suivants :

- Nom de l'application : nom de l'application que vous avez fournie lors de sa définition AWS Resilience Hub.
- Score de résilience : score de résilience global déterminé AWS Resilience Hub pour votre application après l'exécution de l'évaluation.
- Heure de la dernière évaluation — Indique la date et l'heure auxquelles votre candidature a été évaluée avec succès pour la dernière fois.

État de l'application par stratégie

Ce widget répertorie toutes vos politiques et le nombre d'applications qui ont été enfreintes, respectées ou qui n'ont pas encore été évaluées par rapport à celles-ci. Pour afficher toutes les politiques que vous avez créées, choisissez Afficher les politiques. Pour plus d'informations sur le score de résilience, consultezGestion des politiques de résilience.

Vous pouvez identifier les détails à l'aide des éléments suivants :

- Nom de la stratégie : indique le nom de la politique que vous avez indiqué lors de sa définition AWS Resilience Hub.
- Type — Indique le type de politique (politique de résilience) attaché à l'application.
- Nom de la politique — Indique le nombre d'applications qui ont dépassé les cibles RTO et RPO définies dans la politique de résilience.
- Applications satisfaites — Indique le nombre d'applications conformes à la politique de résilience.
- Applications non évaluées : indique le nombre d'applications qui n'ont pas encore été évaluées par rapport à la politique de résilience.
- Score de résilience : score de résilience global déterminé AWS Resilience Hub pour votre application après l'exécution de l'évaluation.
- Heure de la dernière évaluation — Indique la date et l'heure auxquelles votre candidature a été évaluée avec succès pour la dernière fois.

AWS Resilience Hub tableau de bord

Le tableau de bord fournit une vue complète de l'état de résilience de votre portefeuille d'applications. Le tableau de bord regroupe et organise les événements de résilience (par exemple, base de données indisponible ou échec de la validation de la résilience), les alertes et les informations provenant de services tels que CloudWatch et AWS Fault Injection Service (AWS FIS).

Le tableau de bord génère également un score de résilience pour chaque application évaluée. Ce score indique les performances de votre application lorsqu'elle est évaluée par rapport aux politiques de résilience, aux alarmes, aux procédures opérationnelles standard de restauration (SOPs) et aux tests recommandés. Vous pouvez utiliser ce score pour mesurer les améliorations de résilience au fil du temps.

Pour afficher le AWS Resilience Hub tableau de bord, choisissez Tableau de bord dans le menu de navigation. La page Tableau de bord contient les sections suivantes :

État de la demande

Les statuts des applications indiquent si la conformité des applications à la politique de résilience qui leur est attachée a été évaluée ou non. En outre, une fois l'évaluation terminée, le statut indique également si les sources d'entrée de vos applications ont été modifiées ou non. Choisissez un chiffre sous chacun des statuts suivants pour afficher toutes les applications ayant le même statut sur la page Applications :

- Applications incluses dans la politique : indique toutes les applications conformes à la politique de résilience qui leur est attachée.
- Violation de la politique d'application : indique toutes les applications qui ne sont pas conformes à la politique de résilience qui leur est attachée.
- Demandes non évaluées — Indique toutes les demandes dont la conformité n'a pas encore été évaluée ou suivie.
- Applications dérivées : indique toutes les applications qui ont dévié de leur politique de résilience ou si leurs ressources ont dérivé.

Score de résilience des applications au fil du temps

Grâce au score de résilience des applications au fil du temps, vous pouvez consulter un graphique de la résilience de votre application au cours des 30 derniers jours. Bien que le menu déroulant puisse répertorier 10 de vos applications, il AWS Resilience Hub ne vous montre qu'un graphique représentant un maximum de quatre applications à la fois. Pour plus d'informations sur le score de résilience, consultezComprendre les scores de résilience.

> **Note**
>
> AWS Resilience Hub n'exécute pas les évaluations planifiées en même temps. Par conséquent, vous devrez peut-être revenir ultérieurement au graphique du score de résilience dans le temps pour consulter l'évaluation quotidienne de vos applications.

AWS Resilience Hub utilise également Amazon CloudWatch pour générer ces graphiques. Choisissez Afficher les métriques CloudWatch pour créer et afficher des informations plus détaillées sur la résilience de votre application dans votre CloudWatch tableau de bord. Pour plus d'informations CloudWatch, consultez la section Utilisation des tableaux de bord dans le guide de l' CloudWatch utilisateur Amazon.

Alarmes mises en œuvre

Cette section répertorie toutes les alarmes que vous avez configurées dans Amazon CloudWatch pour surveiller toutes les applications. Pour plus d'informations, consultez Affichage des alarmes.

Expériences mises en œuvre

Cette section répertorie toutes les expériences d'injection de défauts que vous avez mises en œuvre dans toutes les applications. Pour de plus amples informations, veuillez consulter Visualisation AWS FIS des expériences.

Décrire et gérer AWS Resilience Hub les applications

Une AWS Resilience Hub application est un ensemble de AWS ressources structurées de manière à prévenir et à corriger les interruptions des AWS applications.

Pour décrire une AWS Resilience Hub application, vous devez fournir un nom d'application, des ressources provenant d'une ou de plusieurs AWS CloudFormation piles et une politique de résilience appropriée. Vous pouvez également utiliser n'importe quelle AWS Resilience Hub application existante comme modèle pour décrire votre application.

Après avoir décrit une AWS Resilience Hub application, vous devez la publier afin de pouvoir effectuer une évaluation de sa résilience. Vous pouvez ensuite utiliser les recommandations issues de l'évaluation pour améliorer la résilience en exécutant une autre évaluation, en comparant les

résultats, puis en réitérant le processus jusqu'à ce que votre RTO de charge de travail estimé et votre RPO de charge de travail estimé atteignent vos objectifs de RTO et de RPO.

Pour afficher la page Applications, sélectionnez Applications dans le volet de navigation. Vous pouvez identifier vos candidatures sur la page Applications de la manière suivante :

- Nom : nom de l'application que vous avez fournie lors de sa définition AWS Resilience Hub.
- Description : description de l'application que vous avez fournie lors de sa définition AWS Resilience Hub.
- État de conformité : AWS Resilience Hub définit le statut de l'application comme étant évalué, non évalué, politique violée ou si des modifications ont été détectées.
  - AWS Resilience Hub Évalué : a évalué votre candidature.
  - Non évalué : votre candidature n' AWS Resilience Hub a pas été évaluée.
  - Politique enfreinte : AWS Resilience Hub a déterminé que votre application n'atteignait pas les objectifs de votre politique de résilience en matière d'objectif de temps de restauration (RTO) et d'objectif de point de restauration (RPO). Passez en revue et utilisez les recommandations fournies par AWS Resilience Hub avant de réévaluer la résilience de votre demande. Pour plus d'informations sur les recommandations, consultezAjoutez une application à AWS Resilience Hub.
  - Modifications détectées : AWS Resilience Hub a détecté des modifications apportées à la politique de résilience associée à votre application. Vous devez réévaluer votre demande AWS Resilience Hub afin de déterminer si elle répond aux objectifs de votre politique de résilience.
- Évaluations planifiées : le type de ressource identifie la ressource composant de votre application. Pour plus d'informations sur les évaluations planifiées, consultezRésilience des applications.
  - Actif - Cela indique que votre candidature est automatiquement évaluée quotidiennement par AWS Resilience Hub.
  - Désactivé : cela indique que votre candidature n'est pas automatiquement évaluée quotidiennement par AWS Resilience Hub et que vous devez l'évaluer manuellement.
- État de dérivation : indique si votre candidature s'est écartée ou non de la précédente évaluation réussie et définit l'un des statuts suivants :
  - Dérivé : indique que l'application, qui était conforme à sa politique de résilience lors de la précédente évaluation réussie, a désormais enfreint la politique de résilience et que l'application est en danger. En outre, il indique également si les ressources contenues dans les sources d'entrée, incluses dans la version actuelle de l'application, ont été ajoutées ou supprimées.

- Non dérivée : indique que l'application est toujours censée atteindre ses objectifs de RTO et de RPO définis dans la politique. En outre, cela indique également que les ressources contenues dans les sources d'entrée, incluses dans la version actuelle de l'application, n'ont pas été ajoutées ou supprimées.
- RTO de charge de travail estimé — Indique le RTO de charge de travail estimé maximal possible de votre application. Cette valeur est le RTO de charge de travail maximal estimé de tous les types de perturbations depuis la dernière évaluation réussie.
- RPO de charge de travail estimé : indique le RPO de charge de travail estimé maximal possible de votre application. Cette valeur est le RTO de charge de travail maximal estimé de tous les types de perturbations depuis la dernière évaluation réussie.
- Heure de la dernière évaluation — Indique la date et l'heure auxquelles votre candidature a été évaluée avec succès pour la dernière fois.
- Heure de création : date et heure de création de l'application.
- ARN — Le nom de ressource Amazon (ARN) de votre application. Pour plus d'informations ARNs, consultez Amazon Resource Names (ARNs) dans le manuel de référence AWS général.

> **Note**
>
> AWS Resilience Hub peut évaluer pleinement la résilience des ressources Amazon ECS interrégionales uniquement si vous utilisez Amazon ECR pour le référentiel d'images.

En outre, vous pouvez également filtrer la liste des applications en utilisant l'une des options suivantes sur la page Applications :

- Rechercher des applications — Entrez le nom de votre application pour filtrer les résultats en fonction du nom de votre application.
- Filtrer l'heure de la dernière évaluation par plage de dates et d'heures : pour appliquer ce filtre, cliquez sur l'icône du calendrier et sélectionnez l'une des options suivantes pour filtrer en fonction des résultats correspondant à la plage de temps :
  - Plage relative : sélectionnez l'une des options disponibles et choisissez Appliquer.

    Si vous choisissez l'option Plage personnalisée, entrez une durée dans le champ Entrez la durée et sélectionnez l'unité de temps appropriée dans la liste déroulante des unités de temps, puis choisissez Appliquer.

- Plage absolue : pour spécifier la plage de dates et d'heures, indiquez l'heure de début et l'heure de fin, puis choisissez Appliquer.

Les rubriques suivantes présentent les différentes approches pour décrire une AWS Resilience Hub application et comment les gérer.

Rubriques

- Afficher le résumé d'une AWS Resilience Hub demande
- Modification des ressources AWS Resilience Hub de l'application
- Gestion des composants de l'application
- Publication d'une nouvelle version de AWS Resilience Hub l'application
- Afficher toutes les versions de AWS Resilience Hub l'application
- Affichage des ressources de l' AWS Resilience Hub application
- Supprimer une AWS Resilience Hub application
- Paramètres de configuration de l'application

Afficher le résumé d'une AWS Resilience Hub demande

La page de résumé de l'application dans la AWS Resilience Hub console fournit une vue d'ensemble des informations de votre application et de son état de résilience.

Pour consulter le résumé d'une demande

1. Choisissez Applications dans le volet de navigation.
2. Sur la page Applications, choisissez le nom de l'application que vous souhaitez consulter.

La page récapitulative des applications contient les sections suivantes.

Rubriques

- Résumé de l'évaluation
- Récapitulatif
- Résilience des applications
- Alarmes mises en œuvre
- Expériences mises en œuvre

Résumé de l'évaluation

Cette section fournit un résumé de la dernière évaluation réussie et met en évidence les recommandations critiques sous forme d'informations exploitables. AWS Resilience Hub utilise les fonctionnalités d'intelligence artificielle générative d'Amazon Bedrock pour aider les utilisateurs à se concentrer sur les recommandations de résilience les plus critiques fournies par AWS Resilience Hub. En vous concentrant sur les éléments critiques, vous pouvez vous concentrer sur les recommandations les plus critiques qui améliorent la posture de résilience de votre application. Choisissez une recommandation pour afficher son résumé, puis cliquez sur Afficher les détails pour afficher plus de détails sur les recommandations dans la section correspondante du rapport d'évaluation. Pour plus d'informations sur la révision du rapport d'évaluation, consultezthe section called “Révision des rapports d'évaluation”.

> **Note**
>
> - Ce résumé de l'évaluation n'est disponible que dans la région Est des États-Unis (Virginie du Nord).
> - Le résumé de l'évaluation généré par les grands modèles linguistiques (LLMs) sur Amazon Bedrock ne sont que des suggestions. Le niveau actuel de la technologie d'IA générative n'est pas parfait et LLMs n'est pas infaillible. Il faut s'attendre à des réponses biaisées et incorrectes, bien que rares. Passez en revue chaque recommandation du résumé de l'évaluation avant d'utiliser les résultats d'un LLM.

Récapitulatif

Cette section fournit un résumé de l'application sélectionnée dans les sections suivantes :

- Informations sur l'application — Cette section fournit les informations suivantes sur l'application sélectionnée :
  - État de la demande — Indique le statut de la demande.
  - Description — Description de l'application.
  - Version — Indique la version actuellement évaluée de l'application.
  - Politique de résilience — Indique la politique de résilience attachée à l'application. Pour plus d'informations sur les politiques de résilience, consultezGestion des politiques de résilience.

- Dérives des applications : cette section met en évidence les dérives détectées lors de l'exécution d'une évaluation pour l'application sélectionnée afin de vérifier si elle est conforme à sa politique de résilience. En outre, il vérifie également si des ressources ont été ajoutées ou supprimées depuis la dernière publication de la version de l'application. Cette section affiche les informations suivantes :
  - Dérives des politiques — Choisissez le chiffre ci-dessous pour afficher tous les composants de l'application qui étaient conformes à la politique de l'évaluation précédente, mais qui ne l'étaient pas lors de l'évaluation actuelle.
  - Ressources dérivées : choisissez le chiffre ci-dessous pour afficher toutes les ressources dérivées dans la dernière évaluation.

Résilience des applications

Les indicateurs présentés dans la section Score de résilience proviennent de l'évaluation de résilience la plus récente de l'application.

Score de résilience

Le score de résilience vous aide à quantifier votre capacité à faire face à une interruption potentielle. Ce score reflète dans quelle mesure votre application a suivi les AWS Resilience Hub recommandations relatives au respect de la politique de résilience, des alarmes, des procédures opérationnelles standard (SOPs) et des tests de l'application.

Le score de résilience maximal que votre application peut atteindre est de 100 %. Le score représente tous les tests recommandés exécutés sur une période prédéfinie. Cela indique que les tests déclenchent la bonne alarme et que l'alarme déclenche le bon SOP.

Supposons, par exemple, que cela AWS Resilience Hub recommande un test avec une alarme et une procédure opérationnelle normalisée. Lorsque le test est exécuté, l'alarme lance le SOP associé, puis s'exécute avec succès. Pour plus d'informations sur le score de résilience, consultez Comprendre les scores de résilience.

Alarmes mises en œuvre

La section Alarmes implémentées du résumé de l'application répertorie les alarmes que vous avez configurées dans Amazon CloudWatch pour surveiller l'application. Pour plus d'informations sur les alarmes, consultez Gérer les alarmes.

Expériences mises en œuvre

La section des expériences d'injection de défauts du résumé de l'application présente une liste des expériences d'injection de défauts. Pour plus d'informations sur les expériences d'injection de défauts, consultezGestion des AWS Fault Injection Service expériences.

Modification des ressources AWS Resilience Hub de l'application

Pour recevoir des évaluations de résilience précises et utiles, assurez-vous que la description de votre candidature est mise à jour et correspond à votre AWS application et à vos ressources réelles. Les rapports d'évaluation, la validation et les recommandations sont basés sur les ressources répertoriées. Si vous ajoutez ou supprimez des ressources d'une AWS application, vous devez refléter ces modifications dans AWS Resilience Hub.

AWS Resilience Hub fournit de la transparence sur les sources de vos applications. Vous pouvez identifier et modifier les ressources et les sources d'application de votre application.

> **Note**
>
> La modification des ressources modifie uniquement la AWS Resilience Hub référence de votre application. Aucune modification n'est apportée à vos ressources réelles.

Vous pouvez ajouter des ressources manquantes, modifier des ressources existantes ou supprimer des ressources dont vous n'avez pas besoin. Les ressources sont regroupées en composants d'application logiques (AppComponents). Vous pouvez les modifier AppComponents pour mieux refléter la structure de votre application.

Ajoutez ou mettez à jour les ressources de votre application en modifiant un brouillon de votre application et en publiant les modifications apportées à une nouvelle version (publication). AWS Resilience Hub utilise la version finale (qui inclut les ressources mises à jour) de votre application pour exécuter des évaluations de résilience.

Pour évaluer la résilience de votre application

1. Dans le volet de navigation, choisissez Applications.
2. Sur la page Applications, choisissez le nom de l'application que vous souhaitez modifier.
3. Dans le menu Actions, choisissez Évaluer la résilience.

4. Dans la boîte de dialogue Exécuter l'évaluation de la résilience, entrez un nom unique pour le rapport ou utilisez le nom généré dans la zone Nom du rapport.
5. Cliquez sur Exécuter.
6. Après avoir été informé que le rapport d'évaluation a été généré, choisissez l'onglet Évaluations et votre évaluation pour afficher le rapport.
7. Cliquez sur l'onglet Révision pour consulter le rapport d'évaluation de votre demande.

Pour activer l'évaluation planifiée

1. Dans le volet de navigation, choisissez Applications.
2. Sur la page Applications, sélectionnez l'application pour laquelle vous souhaitez activer l'évaluation planifiée.
3. Activez Évaluer automatiquement tous les jours.

Pour désactiver l'évaluation planifiée

1. Dans le volet de navigation, choisissez Applications.
2. Sur la page Applications, sélectionnez l'application pour laquelle vous souhaitez activer l'évaluation planifiée.
3. Désactiver l'évaluation automatique quotidienne.

> **Note**
>
> La désactivation de l'évaluation planifiée désactivera la notification de dérive.

4. Choisissez Désactiver.

Pour activer la notification de dérive pour votre application

1. Dans le volet de navigation, choisissez Applications.
2. Sur la page Applications, sélectionnez l'application pour laquelle vous souhaitez activer la notification de dérive ou modifier les paramètres de notification de dérive.
3. Vous pouvez modifier la notification de dérive en choisissant l'une des options suivantes :
   - Dans Actions, choisissez Activer la notification de dérive.

- Choisissez Activer les notifications dans la section Dérives des applications.

4. Effectuez les étapes décrites dansConfiguration des évaluations planifiées et des notifications de dérive, puis revenez à cette procédure.
5. Sélectionnez Activer.

   L'activation de la notification de dérive permettra également une évaluation planifiée.

Pour modifier la notification de dérive pour votre application

> **Note**
>
> Cette procédure est applicable si vous avez activé l'évaluation planifiée (l'évaluation quotidienne automatique est activée) et la notification de dérive.

1. Dans le volet de navigation, choisissez Applications.
2. Sur la page Applications, sélectionnez l'application pour laquelle vous souhaitez activer la notification de dérive ou modifier les paramètres de notification de dérive.
3. Vous pouvez modifier la notification de dérive en choisissant l'une des options suivantes :
   - Dans Actions, choisissez Modifier la notification de dérive.
   - Choisissez Modifier la notification dans la section Dérives de l'application.
4. Effectuez les étapes décrites dansConfiguration des évaluations planifiées et des notifications de dérive, puis revenez à cette procédure.
5. Choisissez Save (Enregistrer).

Pour mettre à jour les autorisations de sécurité de votre application

1. Dans le volet de navigation, choisissez Applications.
2. Sur la page Applications, sélectionnez l'application pour laquelle vous souhaitez mettre à jour les autorisations de sécurité.
3. Dans Actions, sélectionnez Mettre à jour les autorisations.
4. Pour mettre à jour les autorisations de sécurité, suivez les étapes Autorisations de configuration décrites, puis revenez à cette procédure.
5. Choisissez Enregistrer et mettre à jour.

Pour associer une politique de résilience à votre application

1. Dans le volet de navigation, choisissez Applications.
2. Sur la page Applications, choisissez le nom de l'application que vous souhaitez modifier.
3. Dans le menu Actions, choisissez Attacher une politique de résilience.
4. Dans la boîte de dialogue Joindre une politique, sélectionnez une politique de résilience dans la liste déroulante Sélectionner une politique de résilience.
5. Choisissez Attacher.

Pour modifier les sources d'entrée, les ressources et AppComponents celles de votre application

1. Dans le volet de navigation, choisissez Applications.
2. Sur la page Applications, choisissez le nom de l'application que vous souhaitez modifier.
3. Choisissez l'onglet Structure de l'application.
4. Choisissez le signe plus + avant Version, puis sélectionnez la version de l'application avec le statut Brouillon.
5. Pour modifier les sources d'entrée, les ressources et AppComponents celles de votre application, suivez les étapes décrites dans les procédures suivantes.

Pour modifier les sources d'entrée de votre application

1. Pour modifier les sources d'entrée de votre application, choisissez l'onglet Sources d'entrée.

   La section Sources d'entrée répertorie toutes les sources d'entrée des ressources de votre application. Vous pouvez identifier les sources d'entrée comme suit :

   - Nom de la source : nom de la source d'entrée. Choisissez un nom de source pour en afficher les détails dans l'application correspondante. Pour les sources d'entrée ajoutées manuellement, le lien ne sera pas disponible. Par exemple, si vous choisissez le nom de source importé depuis une AWS CloudFormation pile, vous serez redirigé vers la page des détails de la pile sur la AWS CloudFormation console.
   - ARN de la source : nom de ressource Amazon (ARN) de la source d'entrée. Choisissez un ARN pour afficher ses détails dans l'application correspondante. Pour les sources d'entrée ajoutées manuellement, le lien ne sera pas disponible. Par exemple, si vous choisissez un ARN importé depuis une AWS CloudFormation pile, vous serez redirigé vers la page des détails de la pile sur la AWS CloudFormation console.

- Type de source — Type de source d'entrée. Les sources d'entrée incluent les clusters Amazon EKS, les AWS CloudFormation piles, les applications MyApplications AWS Resource Groups, les fichiers d'état Terraform et les ressources ajoutées manuellement.
- Ressources associées : nombre de ressources associées à la source d'entrée. Choisissez un numéro pour afficher toutes les ressources associées à une source d'entrée dans l'onglet Ressources.

2. Pour ajouter des sources d'entrée à votre application, dans la section Sources d'entrée, choisissez Ajouter des sources d'entrée. Pour plus d'informations sur l'ajout de sources d'entrée, consultezthe section called "Ajoutez des ressources à votre AWS Resilience Hub application".
3. Pour modifier les sources d'entrée, sélectionnez-les et choisissez l'une des options suivantes dans Actions :

   - Réimporter les sources d'entrée (jusqu'à 5) — Réimporte jusqu'à cinq sources d'entrée sélectionnées.
   - Supprimer les sources d'entrée — Supprime les sources d'entrée sélectionnées.

     Pour publier une application, celle-ci doit contenir au moins une source d'entrée. Si vous supprimez toutes les sources d'entrée, la fonction Publier une nouvelle version sera désactivée.

Pour modifier les ressources de votre application

1. Pour modifier les ressources de votre application, cliquez sur l'onglet Ressources.

   > **Note**
   >
   > Pour voir la liste des ressources non évaluées, choisissez Afficher les ressources non évaluées.

   La section Ressources répertorie les ressources de l'application que vous avez choisi d'utiliser comme modèle pour la description de votre application. Pour améliorer votre expérience de recherche, AWS Resilience Hub a regroupé les ressources en fonction de plusieurs critères de recherche. Ces critères de recherche incluent les AppComponent types, les ressources non prises en charge et les ressources exclues. Pour filtrer les ressources en fonction d'un critère de

recherche dans le tableau Ressources, choisissez le numéro situé sous chacun des critères de recherche.

Vous pouvez identifier les ressources comme suit :

- ID logique — Un identifiant logique est un nom utilisé pour identifier les ressources de votre AWS CloudFormation pile, de votre fichier d'état Terraform, de votre application ajoutée manuellement, de votre application MyApplications ou. AWS Resource Groups

> **Note**
>
> - Terraform vous permet d'utiliser le même nom pour différents types de ressources. Par conséquent, vous voyez « - type de ressource » à la fin de l'ID logique pour les ressources portant le même nom.
> - Pour afficher les instances de toutes les ressources de l'application, choisissez le signe plus (+) avant l'ID logique. Pour afficher toutes les instances d'une ressource d'application, choisissez le signe plus (+) devant l'ID logique de chaque ressource.
>
> Pour plus d'informations sur les ressources prises en charge, consultezthe section called " AWS Resilience Hub Ressources prises en charge".

- Type de ressource : le type de ressource identifie la ressource du composant pour votre application. Par exemple, `AWS::EC2::Instance` déclare une EC2 instance Amazon. Pour plus d'informations sur le regroupement de AppComponent ressources, consultezRegroupement de ressources dans un composant d'application.
- Nom de la source : nom de la source d'entrée. Choisissez un nom de source pour en afficher les détails dans l'application correspondante. Pour les sources d'entrée ajoutées manuellement, le lien ne sera pas disponible. Par exemple, si vous choisissez le nom de la source qui est importé depuis une AWS CloudFormation pile, vous serez redirigé vers la page des détails de la pile sur le AWS CloudFormation.
- Type de source — Type de source d'entrée. Les sources d'entrée incluent les AWS CloudFormation piles, les applications MyApplications AWS Resource Groups, les fichiers d'état Terraform et les ressources ajoutées manuellement.

> **Note**
>
> Pour modifier vos clusters Amazon EKS, suivez les étapes de la section Pour modifier les sources d'entrée de votre procédure de AWS Resilience Hub candidature.

- Pile source : AWS CloudFormation pile contenant la ressource. Cette colonne dépend du type de structure d'application que vous avez sélectionné.
- ID physique : identifiant réellement attribué à cette ressource, tel qu'un identifiant d' EC2 instance Amazon ou un nom de compartiment S3.
- Inclus — Cela indique si AWS Resilience Hub ces ressources sont incluses dans l'application.
- Évaluable — Cela indique s'ils AWS Resilience Hub évalueront la résilience de votre ressource.
- AppComponents— Le AWS Resilience Hub composant qui a été affecté à cette ressource lorsque sa structure d'application a été découverte.
- Nom : nom de la ressource de l'application.
- Compte : AWS compte propriétaire de la ressource physique.

2. Pour rechercher une ressource qui ne figure pas dans la liste, entrez son ID logique dans le champ de recherche.
3. Pour supprimer une ressource de votre application, sélectionnez-la, puis choisissez Exclure la ressource des actions.
4. Pour résoudre les problèmes liés aux ressources de votre application, choisissez Actualiser les ressources.
5. Pour modifier les ressources existantes de votre application, procédez comme suit :
   a. Sélectionnez une ressource, puis choisissez Mettre à jour les piles dans Actions.
   b. Sur la page Mettre à jour les piles, pour mettre à jour vos ressources, effectuez les procédures appropriées dansAjouter des collections de ressources, puis revenez à cette procédure.
   c. Choisissez Save (Enregistrer).
6. Pour ajouter une ressource à votre application, dans Actions, sélectionnez Ajouter une ressource et procédez comme suit :
   a. Sélectionnez un type de ressource dans la liste déroulante des types de ressources.
   b. Sélectionnez-en un AppComponent dans la liste AppComponentdéroulante.

c. Entrez l'ID logique de la ressource dans le champ Nom de la ressource.
d. Entrez l'ID de ressource physique, ou le nom de la ressource, ou l'ARN de la ressource dans le champ Identifiant de ressource.
e. Choisissez Ajouter.

7. Pour modifier le nom de la ressource, sélectionnez une ressource, choisissez Modifier le nom de la ressource dans Actions, puis effectuez les étapes suivantes :
   a. Entrez l'ID logique de la ressource dans le champ Nom de la ressource.
   b. Choisissez Save (Enregistrer).
8. Pour modifier l'identifiant de ressource, sélectionnez une ressource, choisissez Modifier l'identifiant de ressource dans Actions, puis effectuez les étapes suivantes :
   a. Entrez l'ID de ressource physique, ou le nom de la ressource, ou l'ARN de la ressource dans le champ Identifiant de ressource.
   b. Choisissez Save (Enregistrer).
9. Pour modifier le AppComponent, sélectionnez une ressource, choisissez Modifier AppComponent dans Actions, puis procédez comme suit :
   a. Sélectionnez-en un AppComponent dans la liste AppComponentdéroulante.
   b. Choisissez Ajouter.
10. Pour supprimer une ressource, sélectionnez-la, puis choisissez Supprimer la ressource dans Actions.
11. Pour inclure une ressource, sélectionnez-la, puis choisissez Inclure la ressource dans Actions.

Pour modifier le AppComponents de votre application

1. Pour modifier votre application, choisissez l'AppComponentsonglet. AppComponents

> **Note**
>
> Pour plus d'informations sur le regroupement de AppComponent ressources, consultezRegroupement de ressources dans un composant d'application.

La AppComponentssection répertorie tous les composants logiques dans lesquels les ressources sont regroupées. Vous pouvez les AppComponents identifier comme suit :

- AppComponent name — Le nom du AWS Resilience Hub composant qui a été attribué à cette ressource lorsque sa structure d'application a été découverte.
- AppComponent type — Type de AWS Resilience Hub composant.
- Nom de la source : nom de la source d'entrée. Choisissez un nom de source pour en afficher les détails dans l'application correspondante. Par exemple, si vous choisissez le nom de la source qui est importé depuis une AWS CloudFormation pile, vous serez redirigé vers la page des détails de la pile sur le AWS CloudFormation.
- Nombre de ressources : nombre de ressources associées à la source d'entrée. Choisissez un numéro pour afficher toutes les ressources associées à une source d'entrée dans l'onglet Ressources.

2. Pour créer un AppComponent, dans le menu Actions, choisissez Créer un nouveau AppComponent et effectuez les étapes suivantes :

   a. Entrez un nom pour le AppComponent dans la zone de AppComponentnom. À titre de référence, nous avons prérempli ce champ avec un exemple de nom.
   b. Sélectionnez le type AppComponent de dans la liste déroulante des AppComponenttypes.
   c. Choisissez Save (Enregistrer).
3. Pour modifier un AppComponent, sélectionnez-en un AppComponent, puis choisissez Modifier AppComponent dans Actions.
4. Pour supprimer un AppComponent, sélectionnez-le AppComponent, puis choisissez Supprimer AppComponent des actions.

Après avoir apporté des modifications à votre liste de ressources, vous recevrez une alerte indiquant que des modifications ont été apportées à la version préliminaire de votre application. Pour effectuer une évaluation précise de la résilience, vous devez publier une nouvelle version de votre application. Pour plus d'informations sur la façon de publier une nouvelle version, consultezPublication d'une nouvelle version de AWS Resilience Hub l'application.

Gestion des composants de l'application

Un composant d'application (AppComponent) est un groupe de AWS ressources connexes qui fonctionnent et échouent en tant qu'unité unique. Par exemple, si vous avez une base de données principale et une base de données répliquée, les deux bases de données appartiennent à la même base de données AppComponent. AWS Resilience Hub comporte des règles qui régissent quelles AWS ressources peuvent appartenir à quel AppComponent type. Par exemple, un `DBInstance`

peut appartenir à `AWS::ResilienceHub::DatabaseAppComponent` et ne pas appartenir à`AWS::ResilienceHub::ComputeAppComponent`.

Les ressources suivantes sont prises en AWS Resilience Hub AppComponents charge :

- `AWS::ResilienceHub::ComputeAppComponent`
  - `AWS::ApiGateway::RestApi`
  - `AWS::ApiGatewayV2::Api`
  - `AWS::AutoScaling::AutoScalingGroup`
  - `AWS::EC2::Instance`
  - `AWS::ECS::Service`
  - `AWS::EKS::Deployment`
  - `AWS::EKS::ReplicaSet`
  - `AWS::EKS::Pod`
  - `AWS::Lambda::Function`
  - `AWS::StepFunctions::StateMachine`
- `AWS::ResilienceHub::DatabaseAppComponent`
  - `AWS::DocDB::DBCluster`
  - `AWS::DynamoDB::Table`
  - `AWS::ElastiCache::CacheCluster`
  - `AWS::ElastiCache::GlobalReplicationGroup`
  - `AWS::ElastiCache::ReplicationGroup`
  - `AWS::ElastiCache::ServerlessCache`
  - `AWS::RDS::DBCluster`
  - `AWS::RDS::DBInstance`
- `AWS::ResilienceHub::NetworkingAppComponent`
  - `AWS::EC2::NatGateway`
  - `AWS::ElasticLoadBalancing::LoadBalancer`
  - `AWS::ElasticLoadBalancingV2::LoadBalancer`
  - `AWS::Route53::RecordSet`
- `AWS:ResilienceHub::NotificationAppComponent`
  - `AWS::SNS::Topic`

- `AWS::ResilienceHub::QueueAppComponent`
  - `AWS::SQS::Queue`
- `AWS::ResilienceHub::StorageAppComponent`
  - `AWS::Backup::BackupPlan`
  - `AWS::EC2::Volume`
  - `AWS::EFS::FileSystem`
  - `AWS::FSx::FileSystem`

    > **Note**
    >
    > Actuellement, ne AWS Resilience Hub prend en charge que le serveur de fichiers Amazon FSx pour Windows.

  - `AWS::S3::Bucket`

Rubriques

- Regroupement de ressources dans un composant d'application

Regroupement de ressources dans un composant d'application

Lorsque l'application est importée AWS Resilience Hub avec ses ressources, faites de AWS Resilience Hub votre mieux pour regrouper les ressources connexes au même endroit AppComponent lorsque vous importez votre application, mais le regroupement peut ne pas toujours être précis à 100 %. Certaines ressources sont bloquées pour le regroupement manuel et seront regroupées automatiquement le cas échéant, car ces services ont des dépendances strictes qui nécessitent des configurations de regroupement spécifiques. Pour obtenir la liste complète des services dont le regroupement manuel est bloqué, consultezthe section called "Services bloqués pour le regroupement manuel".

AWS Resilience Hub exécute les activités suivantes une fois que votre application et ses ressources ont été importées avec succès :

- Analyse vos ressources pour vérifier si elles peuvent être regroupées en nouvelles AppComponents afin d'améliorer la précision de l'évaluation.
- S'il AWS Resilience Hub identifie les ressources qui peuvent être regroupées dans de nouvelles ressources AppComponents, il les affiche sous forme de recommandations et vous permet de

les accepter ou de les rejeter. En AWS Resilience Hub, le niveau de confiance attribué à une recommandation de regroupement indique le degré de certitude avec lequel les ressources doivent être regroupées en fonction de leurs attributs et de leurs métadonnées. Un niveau de confiance élevé indique AWS Resilience Hub qu'un niveau de confiance supérieur ou égal à 90 % indique que les ressources de ce groupe sont liées et doivent être regroupées. Un niveau de confiance moyen indique AWS Resilience Hub un niveau de confiance compris entre 70 % et 90 % quant au fait que les ressources de ce groupe sont liées et doivent être regroupées.

> **Note**
>
> AWS Resilience Hub nécessite le regroupement correct afin de pouvoir calculer le RTO de charge de travail estimé et le RPO de charge de travail estimé afin de générer des recommandations.

Voici des exemples de regroupements corrects :

- Regroupez les bases de données principales et les répliques au sein d'une même AppComponent base de données.
- Regroupez EC2 les instances Amazon qui exécutent la même application sous une seule instance AppComponent.
- Regroupez les services Amazon ECS dans une région et basculez les services Amazon ECS dans une autre région au sein d'une même AppComponent région.

Pour plus d'informations sur la révision et l'inclusion des recommandations de regroupement des ressources par AWS Resilience Hub, consultez les rubriques suivantes :

- AWS Resilience Hub recommandations de regroupement de ressources
- Regroupement manuel des ressources dans un AppComponent

Services bloqués pour le regroupement manuel

AWS Resilience Hub vous empêche de regrouper manuellement les ressources de certains AWS services afin d'éviter les erreurs de configuration susceptibles d'affecter l'évaluation de la résilience et les recommandations pour votre application. Ces services sont automatiquement regroupés en fonction de leurs dépendances et de leurs configurations. Lorsque vous définissez une application

incluant ces ressources AWS Resilience Hub, elle analyse leurs relations, leurs dépendances et leurs exigences de résilience afin de créer des regroupements optimaux garantissant des résultats d'évaluation précis.

Liste des AWS services bloqués pour le regroupement manuel :

- Amazon API Gateway
- Amazon DocumentDB
- Amazon DynamoDB
- Amazon Elastic Block Store
- Amazon Elastic File System
- Amazon Relational Database Service
- Amazon S3
- Amazon Simple Queue Service
- FSx pour le serveur de fichiers Windows
- Passerelle NAT

AWS Resilience Hub recommandations de regroupement de ressources

Cette section explique comment générer et examiner des recommandations de regroupement de ressources dans AWS Resilience Hub.

> **Note**
>
> Vous pouvez accorder les autorisations IAM nécessaires pour travailler avec AWS Resilience Hub en utilisant une politique `AWSResilienceHubAsssessmentExecutionPolicy` AWS gérée. Pour plus d'informations sur les politiques AWS gérées, consultezAWSResilienceHubAsssessmentExecutionPolicy.

Pour consulter les recommandations relatives au regroupement des ressources

1. Dans le volet de navigation, choisissez Applications.
2. Choisissez la page Ajouter une application, puis choisissez le nom de l'application pour laquelle vous souhaitez consulter les recommandations relatives au regroupement des ressources.

3. Choisissez l'onglet Structure de l'application.
4. S'il AWS Resilience Hub affiche une alerte d'information, choisissez Consulter les recommandations pour afficher toutes les recommandations de regroupement de ressources. Sinon, effectuez les étapes suivantes pour générer manuellement des recommandations de regroupement de ressources :

   a. Sélectionnez Ressources.
   b. Choisissez Obtenir des recommandations de regroupement dans le menu Actions.

      AWS Resilience Hub analyse vos ressources pour vérifier comment elles peuvent être regroupées de la meilleure façon possible en fonction de leur pertinence AppComponents afin d'améliorer la précision des évaluations. S' AWS Resilience Hub il apprend que vos ressources peuvent être regroupées, il affiche une alerte d'information les concernant.
   c. Si l'alerte d'information s'affiche, choisissez Consulter les recommandations pour afficher toutes les recommandations de regroupement de ressources.

   Vous pouvez les identifier AppComponents dans la section Réviser les recommandations de regroupement de ressources à l'aide des éléments suivants :

   - AppComponent name — Nom de la ressource AppComponent dans laquelle les ressources seront regroupées.
   - Niveau de confiance : indique le niveau de confiance d'AWS Resilience Hub dans la recommandation de regroupement.
   - Nombre de ressources — Indique le nombre de ressources qui seront regroupées dans le AppComponent.
   - AppComponent type — Indique le type de AppComponent.

Pour afficher les ressources qui seront regroupées dans AppComponents

1. Effectuez les étapes de Pour consulter les recommandations relatives au regroupement des ressourcesla procédure, puis revenez à cette procédure.
2. Dans la section Réviser les recommandations de regroupement de ressources, cochez la case (à côté du AppComponent nom) pour afficher toutes les ressources qui seront regroupées au sein des ressources sélectionnées AppComponent. Si vous cochez plusieurs cases, AWS Resilience Hub affiche une section sélectionnée de recommandations générée dynamiquement qui regroupe les recommandations sélectionnées AppComponents selon leur AppComponent

type respectif. Choisissez le numéro situé sous chaque AppComponent type pour afficher toutes les ressources qui seront regroupées dans les ressources sélectionnées AppComponent.

Vous pouvez identifier les ressources qui seront regroupées dans les ressources sélectionnées AppComponent dans la section Ressources à l'aide des méthodes suivantes :

- ID logique — Indique l'ID logique de la ressource. Un identifiant logique est un nom utilisé pour identifier les ressources de votre AWS CloudFormation pile, de votre fichier d'état Terraform, de votre application MyApplications ou. AWS Resource Groups
- ID physique : identifiant réellement attribué à la ressource, tel qu'un identifiant d' EC2 instance Amazon ou un nom de compartiment Amazon S3.
- Type — Indique le type de ressource.
- Région — AWS Région dans laquelle se trouve la ressource.

Pour accepter les recommandations de regroupement de ressources

1. Effectuez les étapes de Pour consulter les recommandations relatives au regroupement des ressourcesla procédure, puis revenez à cette procédure.
2. Dans la section Consulter les recommandations relatives au regroupement des ressources, cochez toutes les cases adjacentes au AppComponentnom. Pour trouver un objet spécifique AppComponent, entrez AppComponent son nom dans le AppComponents champ Rechercher.

   > **Note**
   >
   > Par défaut, AWS Resilience Hub affiche toutes les recommandations de regroupement de ressources. Pour filtrer le tableau avec les recommandations de regroupement de ressources précédemment rejetées, choisissez Précédemment rejeté dans le menu déroulant adjacent à la AppComponents zone Rechercher.

3. Choisissez Accepter.
4. Choisissez Accepter dans la boîte de dialogue Accepter les recommandations de regroupement de ressources.

   AWS Resilience Hub affiche une alerte d'information en cas de réussite du regroupement des ressources. Si vous n'avez accepté qu'un sous-ensemble de recommandations de regroupement de ressources, la section Consulter les recommandations de regroupement de ressources

affiche toutes les recommandations de regroupement de ressources que vous n'avez pas acceptées.

Pour rejeter les recommandations de regroupement de ressources

1. Effectuez les étapes de Pour consulter les recommandations relatives au regroupement des ressourcesla procédure, puis revenez à cette procédure.
2. Dans la section Consulter les recommandations relatives au regroupement des ressources, cochez toutes les cases adjacentes au AppComponentnom. Pour trouver un objet spécifique AppComponent, entrez AppComponent son nom dans le AppComponents champ Rechercher.

   > **Note**
   >
   > Par défaut, AWS Resilience Hub affiche toutes les recommandations de regroupement de ressources. Pour filtrer le tableau avec les recommandations de regroupement de ressources précédemment rejetées, sélectionnez Précédemment rejeté dans le menu déroulant adjacent à la AppComponents zone Rechercher.

3. Choisissez Reject (Refuser).
4. Sélectionnez l'une des raisons du rejet de la recommandation de regroupement de ressources, puis choisissez Rejeter dans la boîte de dialogue Rejeter la recommandation de regroupement de ressources.

   AWS Resilience Hub affiche une alerte d'information confirmant la même chose. Si vous n'avez rejeté qu'un sous-ensemble de recommandations de regroupement de ressources, la section Consulter les recommandations de regroupement de ressources affiche toutes les recommandations de regroupement de ressources que vous n'avez pas acceptées.

Regroupement manuel des ressources dans un AppComponent

Cette section explique comment regrouper manuellement des ressources dans un AppComponent et comment attribuer une autre ressource AppComponent à une ressource dans AWS Resilience Hub.

Pour regrouper les ressources

1. Dans le volet de navigation, choisissez Applications.

2. Sur la page Applications, choisissez le nom de l'application qui contient les ressources que vous souhaitez regrouper.
3. Choisissez l'onglet Structure de l'application.
4. Sous l'onglet Version, sélectionnez la version de l'application avec le statut Brouillon.
5. Sélectionnez l'onglet Ressources.
6. Cochez les cases adjacentes à Logical ID pour sélectionner toutes les ressources que vous souhaitez regrouper.

> **Note**
>
> Vous ne pouvez pas choisir les ressources ajoutées manuellement.

7. Choisissez Actions, puis sélectionnez Ressources de groupe.
8. AppComponent Choisissez une ressource dans la liste AppComponent déroulante Choisir dans laquelle vous souhaitez regrouper la ressource.
9. Choisissez Save (Enregistrer).
10. Choisissez Publish new version (Publier une nouvelle version).
11. Choisissez l'onglet Structure de l'application.
12. Pour consulter la version publiée de votre application, procédez comme suit :
    a. Sous l'onglet Version, sélectionnez la version de l'application avec l'état de publication actuel.
    b. Sélectionnez l'onglet Ressources.

Pour affecter des ressources à un AppComponent

1. Dans le volet de navigation, choisissez Applications.
2. Sur la page Applications, choisissez le nom de l'application qui contient la ressource que vous souhaitez regrouper.
3. Choisissez l'onglet Structure de l'application.
4. Sous Version, sélectionnez la version de l'application avec le statut Brouillon.
5. Sélectionnez l'onglet Ressources.
6. Cochez la case adjacente à l'ID logique pour sélectionner la ressource.
7. Choisissez Modifier AppComponent dans le menu Actions.

8. Pour supprimer le courant AppComponent de la AppComponentsection, choisissez X dans le coin supérieur droit de l'étiquette qui affiche votre nom actuel AppComponent .
9. Pour regrouper la ressource dans une autre catégorie AppComponent, choisissez-en une autre AppComponent dans la liste AppComponent déroulante Choisir.
10. Choisissez Ajouter.
11. Supprimez les espaces vides AppComponents de l'AppComponentsonglet.
12. Choisissez Publish new version (Publier une nouvelle version).
13. Choisissez l'onglet Structure de l'application.
14. Pour consulter la version publiée de votre application, procédez comme suit :
    a. Sous l'onglet Version, sélectionnez la version de l'application avec l'état de publication actuel.
    b. Sélectionnez l'onglet Ressources.

Publication d'une nouvelle version de AWS Resilience Hub l'application

Après avoir modifié les ressources de votre AWS Resilience Hub application comme décrit dansModification des ressources AWS Resilience Hub de l'application, vous devez publier une nouvelle version de votre application pour exécuter une évaluation précise de la résilience. En outre, vous devrez peut-être publier une nouvelle version de votre application si vous avez ajouté de nouvelles alertes et de nouveaux tests recommandés à votre application. SOPs

Pour publier une nouvelle version de votre application

1. Dans le volet de navigation, choisissez Applications.
2. Sur la page Applications, choisissez le nom de l'application.
3. Choisissez l'onglet Structure de l'application.
4. Choisissez Publish new version (Publier une nouvelle version).
5. Dans la boîte de dialogue Publier la version, dans la zone Nom, entrez le nom de la version de l'application ou vous pouvez utiliser le nom par défaut suggéré par AWS Resilience Hub.
6. Choisissez Publish.

   Lorsque vous publiez une nouvelle version de votre application, celle-ci devient la version qui est évaluée lorsque vous exécutez des évaluations de résilience. De plus, la version préliminaire sera identique à la version publiée jusqu'à ce que vous apportiez des modifications.

Après avoir publié une nouvelle version de votre application, nous vous recommandons d'exécuter un nouveau rapport d'évaluation de la résilience pour confirmer que votre application répond toujours à votre politique de résilience. Pour plus d'informations sur l'exécution d'une évaluation, consultezExécution et gestion d'évaluations de résilience dans AWS Resilience Hub.

Afficher toutes les versions de AWS Resilience Hub l'application

Pour faciliter le suivi des modifications apportées à l'application, AWS Resilience Hub affiche les versions précédentes de votre application depuis sa création AWS Resilience Hub.

Pour consulter toutes les versions de votre application

1. Dans le volet de navigation, choisissez Applications.
2. Sur la page Applications, choisissez le nom de l'application.
3. Choisissez l'onglet Structure de l'application.
4. Pour afficher toutes les versions précédentes de votre application, sélectionnez le signe plus (+) avant Afficher toutes les versions. AWS Resilience Hub indique la version préliminaire et la version récemment publiée de votre application en utilisant les statuts de version provisoire et actuelle, respectivement. Vous pouvez choisir n'importe quelle version de votre application pour afficher ses ressources AppComponent, ses sources d'entrée et les autres informations associées.

   En outre, vous pouvez également filtrer la liste en utilisant l'une des options suivantes :

   - Filtrer par nom de version — Entrez un nom pour filtrer les résultats en fonction du nom de la version de votre application.
   - Filtrer par plage de dates et d'heures : pour appliquer ce filtre, cliquez sur l'icône du calendrier et sélectionnez l'une des options suivantes pour filtrer en fonction des résultats correspondant à la plage horaire :
     - Plage relative : sélectionnez l'une des options disponibles et choisissez Appliquer.

       Si vous choisissez l'option Plage personnalisée, entrez une durée dans le champ Entrez la durée et sélectionnez l'unité de temps appropriée dans la liste déroulante des unités de temps, puis choisissez Appliquer.
     - Plage relative : pour spécifier la plage de dates et d'heures, indiquez l'heure de début et l'heure de fin, puis choisissez Appliquer.

Affichage des ressources de l' AWS Resilience Hub application

Pour consulter les ressources de votre application

1. Dans le volet de navigation, choisissez Applications.
2. Sur la page Applications, sélectionnez l'application pour laquelle vous souhaitez mettre à jour les autorisations de sécurité.
3. Dans Actions, choisissez Afficher les ressources.

   Dans l'onglet Ressources, vous pouvez identifier les ressources dans le tableau Ressources comme suit :

   - ID logique — Un identifiant logique est un nom utilisé pour identifier les ressources de votre AWS CloudFormation pile, de votre fichier d'état Terraform, de votre application MyApplications ou. AWS Resource Groups

     > **Note**
     >
     > - Terraform vous permet d'utiliser le même nom pour différents types de ressources. Par conséquent, vous voyez « - type de ressource » à la fin de l'ID logique pour les ressources portant le même nom.
     > - Pour afficher les instances de toutes les ressources de l'application, choisissez le signe plus (+) avant l'ID logique. Pour afficher toutes les instances d'une ressource d'application, choisissez le signe plus (+) devant l'ID logique de chaque ressource.
     >
     > Pour plus d'informations sur les ressources prises en charge, consultezthe section called “ AWS Resilience Hub Ressources prises en charge”.

   - État — Cela indique si la résilience de votre ressource AWS Resilience Hub sera évaluée.
   - Type de ressource : le type de ressource identifie la ressource du composant pour votre application. Par exemple, `AWS::EC2::Instance` déclare une EC2 instance Amazon. Pour plus d'informations sur le regroupement de AppComponent ressources, consultezRegroupement de ressources dans un composant d'application.
   - Nom de la source : nom de la source d'entrée. Choisissez un nom de source pour en afficher les détails dans l'application correspondante. Pour les sources d'entrée ajoutées manuellement, le lien ne sera pas disponible. Par exemple, si vous choisissez le nom de la

source qui est importé depuis une AWS CloudFormation pile, vous serez redirigé vers la page des détails de la pile sur le AWS CloudFormation.

- Type de source : type de source d'entrée.
- AppComponent type — Type de source d'entrée. Les sources d'entrée incluent les AWS CloudFormation piles, les applications MyApplications AWS Resource Groups, les fichiers d'état Terraform et les ressources ajoutées manuellement.

> **Note**
>
> Pour modifier vos clusters Amazon EKS, suivez les étapes de la section Pour modifier les sources d'entrée de votre procédure de AWS Resilience Hub candidature.

- ID physique : identifiant réellement attribué à cette ressource, tel qu'un identifiant d' EC2 instance Amazon ou un nom de compartiment S3.
- Inclus — Cela indique si AWS Resilience Hub ces ressources sont incluses dans l'application.
- AppComponents— Le AWS Resilience Hub composant qui a été affecté à cette ressource lorsque sa structure d'application a été découverte.
- Nom : nom de la ressource de l'application.
- Compte : AWS compte propriétaire de la ressource physique.

4. Choisissez Enregistrer et mettre à jour.

Supprimer une AWS Resilience Hub application

Une fois que vous avez atteint la limite maximale de 50 applications, vous devez supprimer une ou plusieurs applications avant de pouvoir en ajouter d'autres.

Pour supprimer une application

1. Dans le volet de navigation, choisissez Applications.
2. Sur la page Applications, sélectionnez l'application que vous souhaitez supprimer.
3. Choisissez Actions, puis Delete application (Supprimer l'application).
4. Pour confirmer la suppression, saisissez Supprimer dans le champ Supprimer, puis choisissez Supprimer.

Paramètres de configuration de l'application

AWS Resilience Hub fournit un mécanisme de saisie pour recueillir des informations supplémentaires sur les ressources associées à vos applications. Grâce à ces informations, AWS Resilience Hub vous aurez une meilleure compréhension de vos ressources et vous fournirez de meilleures recommandations en matière de résilience.

La section Paramètres de configuration de l'application répertorie tous les paramètres de configuration de votre prise en charge du basculement entre régions pour. AWS Elastic Disaster Recovery Vous pouvez identifier les paramètres de configuration comme suit :

- Rubrique — Indique le domaine de votre application qui est configuré. Par exemple, configuration de basculement.
- Objectif — Indique la raison pour laquelle les informations AWS Resilience Hub ont été demandées.
- Paramètre — Indique les détails spécifiques au domaine d'application, qui AWS Resilience Hub seront utilisés pour fournir des recommandations pour votre application. Actuellement, ce paramètre utilise la valeur clé d'une seule région de basculement et d'un compte associé.

Mise à jour des paramètres de configuration des applications

Cette section vous permet de mettre à jour les paramètres de configuration de votre application AWS Elastic Disaster Recovery et de publier l'application afin d'inclure les paramètres mis à jour pour les évaluations de résilience.

Pour mettre à jour les paramètres de configuration de l'application

1. Dans le volet de navigation, choisissez Applications.
2. Sur la page Applications, choisissez le nom de l'application que vous souhaitez modifier.
3. Choisissez l'onglet Paramètres de configuration de l'application.
4. Choisissez Mettre à jour.
5. Entrez l'ID du compte de basculement dans le champ Identifiant du compte.
6. Sélectionnez une région de basculement dans la liste déroulante des régions.

> **Note**
>
> Si vous souhaitez désactiver cette fonctionnalité, sélectionnez « — » dans la liste déroulante.

7. Choisissez Mettre à jour et publier.

Gestion des politiques de résilience

Cette section explique comment créer des politiques de résilience pour vos applications. La définition correcte des politiques de résilience vous permet de comprendre le niveau de résilience de votre application. Une politique de résilience contient des informations et des objectifs que vous utilisez pour évaluer si votre application est censée se rétablir après un type d'interruption, tel qu'un logiciel, un matériel, une zone de disponibilité ou une AWS région. Ces politiques ne modifient ni n'affectent une application réelle. Plusieurs applications peuvent avoir la même politique de résilience.

Lorsque vous créez une politique de résilience, vous définissez les objectifs cibles : objectif de temps de restauration (RTO) et objectif de point de reprise (RPO). Les objectifs déterminent si l'application répond à la politique de résilience. Associez la politique à votre application et effectuez une évaluation de la résilience. Vous pouvez créer différentes politiques pour les différents types d'applications de votre portefeuille. Par exemple, une application de trading en temps réel aurait une politique de résilience différente de celle d'une application de reporting mensuel.

> **Note**
>
> AWS Resilience Hub vous permet de saisir une valeur zéro dans les champs RTO et RPO de votre politique de résilience. Cependant, lors de l'évaluation de votre candidature, le résultat d'évaluation le plus bas possible est proche de zéro. Par conséquent, si vous entrez une valeur zéro dans les champs RTO et RPO, le résultat du RTO de charge de travail estimé et du RPO de charge de travail estimé sera proche de zéro et le statut de conformité de votre application sera défini sur Policy violated.

L'évaluation évalue la configuration de votre application par rapport à la politique de résilience ci-jointe. À la fin du processus, AWS Resilience Hub fournit une évaluation de la manière dont votre application se situe par rapport aux objectifs de restauration définis dans votre politique de résilience.

Vous pouvez créer des politiques de résilience dans les applications, ainsi que dans les politiques de résilience. Vous pouvez accéder aux informations pertinentes concernant vos politiques, ainsi que les modifier et les supprimer.

AWS Resilience Hub utilise vos objectifs de RTO et de RPO pour mesurer la résilience face aux types de perturbations potentiels suivants :

- Application : perte d'un service ou d'un processus logiciel requis.
- Infrastructure cloud : perte de matériel, tel que EC2 des instances.
- Zone de disponibilité de l'infrastructure cloud (AZ) : une ou plusieurs zones de disponibilité ne sont pas disponibles.
- Région de l'infrastructure cloud : une ou plusieurs régions ne sont pas disponibles.

AWS Resilience Hub vous permet de créer des politiques de résilience personnalisées ou d'utiliser nos politiques de résilience standard ouvertes recommandées. Lorsque vous créez des politiques personnalisées, nommez et décrivez votre politique, puis choisissez le niveau ou le niveau approprié qui définit votre politique. Ces niveaux incluent : les services informatiques de base, essentiels à la mission, critiques, importants et non critiques.

Choisissez le niveau qui convient à votre catégorie d'applications. Par exemple, vous pouvez classer un système de trading en temps réel comme critique, tandis qu'une application de reporting mensuel peut être classée comme non critique. Lorsque vous utilisez nos politiques standard, vous pouvez choisir une politique de résilience avec un niveau et des valeurs préconfigurés pour les cibles RTO et RPO par type de perturbation. Si nécessaire, vous pouvez modifier le niveau ainsi que les objectifs RTO et RPO.

Vous pouvez créer des politiques de résilience dans les politiques de résilience ou lorsque vous décrivez une nouvelle application.

Création de politiques de résilience

Dans AWS Resilience Hub, vous pouvez créer une politique de résilience. Une politique de résilience contient des informations et des objectifs que vous pouvez utiliser pour évaluer si votre application peut se rétablir après un type d'interruption, qu'il s'agisse d'un logiciel, d'un matériel, d'une zone de disponibilité ou d'une AWS région. Ces politiques ne modifient ni n'affectent une application réelle. Plusieurs applications peuvent avoir la même politique de résilience.

Lorsque vous créez une politique de résilience, vous définissez les cibles d'objectif de temps de restauration (RTO) et d'objectif de point de restauration (RPO). Lorsque vous exécutez une évaluation, AWS Resilience Hub détermine si l'application est estimée comme répondant aux objectifs définis dans la politique de résilience.

L'évaluation évalue la configuration de votre application par rapport à la politique de résilience ci-jointe. À la fin du processus, AWS Resilience Hub fournit une évaluation de la manière dont votre application se situe par rapport aux objectifs de votre politique de résilience.

> **Note**
>
> AWS Resilience Hub vous permet de saisir une valeur zéro dans les champs RTO et RPO de votre politique de résilience. Cependant, lors de l'évaluation de votre candidature, le résultat d'évaluation le plus bas possible est proche de zéro. Par conséquent, si vous entrez une valeur zéro dans les champs RTO et RPO, le résultat du RTO de charge de travail estimé et du RPO de charge de travail estimé sera proche de zéro et le statut de conformité de votre application sera défini sur Policy violated.

Vous pouvez créer des politiques de résilience dans les applications, ainsi que dans les politiques de résilience. Vous pouvez accéder aux informations pertinentes concernant vos politiques, ainsi que les modifier et les supprimer.

Pour créer des politiques de résilience dans les applications

1. Dans le menu de navigation de gauche, sélectionnez Applications.
2. Effectuez les procédures du début à the section called “Commencez par ajouter une application” la finthe section called “Ajoutez des tags à votre application ”.
3. Dans la section Politiques de résilience, choisissez Créer une politique de résilience.

   La page Créer une politique de résilience s'affiche.
4. Dans la section Choisir une méthode de création, sélectionnez Créer une politique.
5. Entrez le nom de la politique.
6. (Facultatif) Entrez une description de la stratégie.
7. Choisissez l'une des options suivantes dans la liste déroulante des niveaux :

   - Services informatiques de base

- Essentiel à la mission
- Critical (Critique)
- Important
- Non critique

8. Pour les cibles RTO et RPO, sous Customer Application RTO et RPO, entrez une valeur numérique dans le champ, puis choisissez l'unité de temps que la valeur représente.

   Répétez ces entrées sous Infrastructure RTO et RPO pour Infrastructure et zone de disponibilité.

9. (Facultatif) Si vous avez une application multirégionale, vous souhaiterez peut-être définir les cibles RTO et RPO d'une région.

   Activez la région. Pour les cibles RTO et RPO de la région, sous RTO et RPO de l'application client, entrez une valeur numérique dans le champ, puis choisissez l'unité de temps que la valeur représente.

10. (Facultatif) Si vous souhaitez ajouter des balises, vous pourrez le faire ultérieurement au fur et à mesure que vous créerez votre politique. Pour plus d'informations sur les balises, consultez la section Ressources de balisage dans le manuel de référence AWS général.

11. Pour créer la politique, choisissez Create.

Pour créer des politiques de résilience dans les politiques de résilience

1. Dans le menu de navigation de gauche, sélectionnez Politiques.
2. Dans la section Politiques de résilience, choisissez Créer une politique de résilience.

   La page Créer une politique de résilience s'affiche.

3. Entrez le nom de la politique.
4. (Facultatif) Entrez une description de la stratégie.
5. Choisissez l'une des options suivantes dans le niveau :

   - Services informatiques de base
   - Essentiel à la mission
   - Critical (Critique)
   - Important
   - Non critique

6. Pour les cibles RTO et RPO, sous Customer Application RTO et RPO, entrez une valeur numérique dans le champ, puis choisissez l'unité de temps que la valeur représente.

   Répétez ces entrées sous Infrastructure RTO et RPO pour Infrastructure et zone de disponibilité.
7. (Facultatif) Si vous avez une application multirégionale, vous souhaiterez peut-être définir les cibles RTO et RPO d'une région.

   Activez la région. Pour les cibles RTO et RPO, sous Customer Application RTO et RPO, entrez une valeur numérique dans le champ, puis choisissez l'unité de temps que la valeur représente.
8. (Facultatif) Si vous souhaitez ajouter des balises, vous pourrez le faire ultérieurement au fur et à mesure que vous créerez votre politique. Pour plus d'informations sur les balises, consultez la section Ressources de balisage dans le manuel de référence AWS général.
9. Pour créer la politique, choisissez Create.

Pour créer des politiques de résilience basées sur une stratégie suggérée

1. Dans le menu de navigation de gauche, sélectionnez Politiques.
2. Dans la section Choisir une méthode de création, sélectionnez Sélectionner une politique en fonction d'une stratégie suggérée.
3. Dans la section Politiques de résilience, choisissez Créer une politique de résilience.

   La page Créer une politique de résilience s'affiche.
4. Entrez un nom pour la politique de résilience.
5. (Facultatif) Entrez une description de la stratégie.
6. Dans la section Stratégies de résilience suggérées, consultez et choisissez l'un des niveaux de politique de résilience prédéterminés suivants :

   - Application non critique
   - Application importante
   - Application critique
   - Application critique mondiale
   - Application critique
   - Application essentielle à la mission mondiale
   - Service de base
7. Pour créer la politique de résilience, choisissez Create policy.

Accès aux détails de la politique de résilience

Lorsque vous ouvrez une politique de résilience, des détails importants s'affichent à son sujet. Vous pouvez également modifier ou supprimer la résilience.

Les détails de la politique de résilience se déclinent en deux points de vue principaux : le résumé et les balises.

Récapitulatif

Informations de base

Fournit les informations suivantes sur la politique de résilience : nom, description, niveau, niveau de coût et date de création.

Charge de travail estimée RTO et RPO de charge de travail estimée

Indique le type d'interruption estimé du RTO de la charge de travail et le type d'interruption du RPO de charge de travail estimé associés à cette politique de résilience.

Balises

Utilisez cette vue pour gérer, ajouter et supprimer des balises internes à cette application.

Pour modifier les politiques de résilience dans les détails des politiques de résilience

1. Dans le menu de navigation de gauche, sélectionnez Politiques.
2. Dans Politiques de résilience, ouvrez une politique de résilience.
3. Choisissez Modifier. Entrez les modifications appropriées dans les champs Informations de base, RTO et RPO. Ensuite, choisissez Enregistrer les modifications.

Pour modifier les politiques de résilience dans la politique de résilience

1. Dans le menu de navigation de gauche, sélectionnez Politiques.
2. Dans Politiques de résilience, choisissez une politique de résilience.
3. Choisissez Actions, puis sélectionnez Modifier.
4. Entrez les modifications appropriées dans les champs Informations de base, RTO et RPO. Ensuite, choisissez Enregistrer les modifications.

Pour supprimer les politiques de résilience dans les détails des politiques de résilience

1. Dans le menu de navigation de gauche, sélectionnez Politiques.
2. Dans Politiques de résilience, ouvrez une politique de résilience.
3. Sélectionnez Delete (Supprimer). Confirmez votre suppression, puis choisissez Supprimer.

Pour supprimer les politiques de résilience dans la politique de résilience

1. Dans le menu de navigation de gauche, sélectionnez Politiques.
2. Dans Politiques de résilience, choisissez une politique de résilience.
3. Choisissez Actions, puis sélectionnez Supprimer.
4. Confirmez votre suppression, puis choisissez Supprimer.

Exécution et gestion d'évaluations de résilience dans AWS Resilience Hub

Lorsque votre application change, vous devez effectuer une évaluation de la résilience. L'évaluation compare la configuration de chaque composant d'application à la politique et émet des recommandations en matière d'alarme, de procédure opérationnelle normalisée et de test. Ces recommandations de configuration peuvent améliorer la rapidité des procédures de restauration.

Les recommandations relatives aux alarmes vous aident à configurer des alarmes qui détectent les pannes. Les recommandations SOP fournissent des scripts qui gèrent les processus de restauration courants, tels que la restauration à partir d'une sauvegarde. Les recommandations de test proposent des suggestions pour vérifier le bon fonctionnement de vos configurations. Par exemple, vous pouvez vérifier si une application se rétablit lors de processus de restauration automatique, tels que le dimensionnement automatique ou l'équilibrage de charge en raison de problèmes réseau. Vous pouvez vérifier si les alarmes des applications sont déclenchées lorsque les ressources atteignent leurs limites. Vous pouvez également tester votre SOPs efficacité dans les conditions que vous indiquez.

Rubriques :

- Exécution d'évaluations de résilience dans AWS Resilience Hub
- Révision des rapports d'évaluation
- Supprimer les évaluations de résilience

Exécution d'évaluations de résilience dans AWS Resilience Hub

Vous pouvez effectuer des évaluations de résilience à partir de plusieurs sites dans AWS Resilience Hub. Pour plus d'informations sur votre application, consultezthe section called "Gestion d'applications".

Pour exécuter une évaluation de la résilience à partir du menu Actions

1. Dans le menu de navigation de gauche, sélectionnez Applications.
2. Choisissez une application dans le tableau Applications.
3. Choisissez l'option Évaluer la résilience dans le menu Actions.
4. Dans la boîte de dialogue Exécuter l'évaluation de la résilience, vous pouvez saisir un nom unique ou utiliser le nom généré pour l'évaluation.
5. Cliquez sur Exécuter.

   Pour consulter le rapport d'évaluation, sélectionnez Évaluations dans votre application. Pour de plus amples informations, veuillez consulter the section called "Révision des rapports d'évaluation".

Pour exécuter une évaluation de la résilience à partir de l'onglet Évaluations

Vous pouvez exécuter une nouvelle évaluation de la résilience lorsque votre application ou votre politique de résilience change.

1. Dans le menu de navigation de gauche, sélectionnez Applications.
2. Choisissez une application dans le tableau Applications.
3. Choisissez l'onglet Évaluations.
4. Choisissez Exécuter l'évaluation de la résilience.
5. Dans la boîte de dialogue Exécuter l'évaluation de la résilience, vous pouvez saisir un nom unique ou utiliser le nom généré pour l'évaluation.
6. Cliquez sur Exécuter.

   Pour consulter le rapport d'évaluation, sélectionnez Évaluations dans votre application. Pour de plus amples informations, veuillez consulter the section called "Révision des rapports d'évaluation".

Révision des rapports d'évaluation

Vous trouverez les rapports d'évaluation dans la vue Évaluations de votre application.

Pour trouver un rapport d'évaluation

1. Dans le menu de navigation de gauche, sélectionnez Applications.
2. Dans Applications, ouvrez une application.
3. Dans l'onglet Évaluations, choisissez un rapport d'évaluation dans la section Évaluations de résilience.

Lorsque vous ouvrez le rapport, vous pouvez voir ce qui suit :

- Vue d'ensemble du rapport d'évaluation
- Recommandations pour améliorer la résilience.
- Recommandations pour configurer les alarmes SOPs et les tests
- Comment créer et gérer des balises pour rechercher et filtrer vos AWS ressources

Rapport d'évaluation

Cette section fournit une vue d'ensemble du rapport d'évaluation. AWS Resilience Hub répertorie chaque type d'interruption et le composant d'application associé. Il répertorie également vos politiques RTO et RPO réelles et détermine si le composant d'application peut atteindre les objectifs de la politique.

Présentation

Affiche le nom de l'application, le nom de la politique de résilience et la date de création du rapport.

Dérives de ressources détectées

Cette section répertorie toutes les ressources ajoutées ou supprimées après leur inclusion dans la dernière version de l'application publiée. Choisissez Réimporter les sources d'entrée pour réimporter toutes les sources d'entrée (qui contiennent des ressources dérivées) dans l'onglet Sources d'entrée. Choisissez Publier et évaluer pour inclure les ressources mises à jour dans l'application et recevoir une évaluation précise de la résilience.

Vous pouvez identifier les sources d'entrée dérivées à l'aide des méthodes suivantes :

- ID logique — Indique l'ID logique de la ressource. Un identifiant logique est un nom utilisé pour identifier les ressources de votre AWS CloudFormation pile, de votre fichier d'état Terraform, de votre application MyApplications ou. AWS Resource Groups
- Modifier — Indique si une ressource d'entrée a été ajoutée ou supprimée.
- Nom de la source — Indique le nom de la ressource. Choisissez un nom de source pour en afficher les détails dans l'application correspondante. Pour les sources d'entrée ajoutées manuellement, le lien ne sera pas disponible. Par exemple, si vous choisissez le nom de la source qui est importé depuis une AWS CloudFormation pile, vous serez redirigé vers la page des détails de la pile sur le AWS CloudFormation.
- Type de ressource — Indique le type de ressource.
- Compte — Indique le AWS compte propriétaire de la ressource physique.
- Région — Indique la AWS région dans laquelle se trouve la ressource.

RTO

Affiche une représentation graphique indiquant si l'application est estimée pour répondre aux objectifs de la politique de résilience. Ceci est basé sur la durée pendant laquelle une application peut être interrompue sans causer de dommages importants à l'organisation. L'évaluation fournit une estimation de la charge de travail RTO.

RPO

Affiche une représentation graphique indiquant si l'application est estimée pour répondre aux objectifs de la politique de résilience. Cela est basé sur le temps pendant lequel les données peuvent être perdues avant qu'un préjudice significatif ne se produise pour l'entreprise. L'évaluation fournit une estimation du RPO de charge de travail.

Détails

Fournit des descriptions détaillées de chaque type de perturbation à l'aide des onglets Tous les résultats et Dérives de conformité des applications. L'onglet Tous les résultats montre toutes les perturbations, y compris les écarts de conformité, et l'onglet Dérives de conformité des applications affiche uniquement les écarts de conformité. Le type de perturbation inclut l'application, l'infrastructure cloud (infrastructure et zone de disponibilité) et la région, et fournit les informations suivantes à ce sujet :

- AppComponent

Les ressources qui composent l'application. Par exemple, votre application peut comporter une base de données ou un composant de calcul.

- RTO estimé

  Indique si la configuration de votre politique est conforme à vos exigences en matière de politique. Nous fournissons deux valeurs, notre RTO estimé et votre RTO cible. Par exemple, si vous voyez une valeur de 2 h sous RTO ciblé et 40 m sous RTO de charge de travail estimée, cela indique que nous fournissons un RTO de charge de travail estimé à 40 minutes, alors que le RTO actuel de votre application est de deux heures. Nous basons notre calcul du RTO de la charge de travail estimée sur la configuration, et non sur la politique. Par conséquent, une base de données de zones de disponibilité multiples aura le même RTO de charge de travail estimé en cas de défaillance d'une zone de disponibilité, quelle que soit la politique sélectionnée.

- Dérive RTO

  Indique la durée pendant laquelle votre candidature s'est écartée de la charge de travail estimée jusqu'à la fin de l'évaluation réussie précédente. Nous fournissons deux valeurs, notre RTO estimé et notre dérive du RTO. Par exemple, si vous voyez une valeur de 2 h sous RTO estimé et 40 m sous Dérive du RTO, cela indique que votre application s'écarte de 40 minutes de la charge de travail estimée RTO de l'évaluation réussie précédente.

- RPO estimé

  Affiche la politique RPO de charge de travail estimée réelle qui est AWS Resilience Hub estimée, en fonction de la politique RPO ciblée que vous avez définie pour chaque composant de l'application. Par exemple, vous avez peut-être défini l'objectif du RPO dans votre politique de résilience pour les défaillances de zone de disponibilité à une heure. Le résultat estimé peut être calculé à une valeur proche de zéro. Cela suppose qu'Amazon Aurora, où nous validons chaque transaction, est réussie dans quatre nœuds sur six, répartis sur plusieurs zones de disponibilité. La point-in-time restauration peut prendre cinq minutes.

  La seule cible RTO et RPO que vous pouvez choisir de ne pas fournir est la région. Pour certaines applications, il est utile de planifier la restauration lorsqu'il existe une dépendance cruciale à l'égard d'un service AWS, qui peut devenir indisponible dans l'ensemble de la région.

Si vous choisissez cette option, telle que la définition d'objectifs RTO ou RPO pour la région, vous recevrez une estimation du temps de reprise et des recommandations opérationnelles pour de telles défaillances.

- Dérive du RPO

  Indique la durée pendant laquelle votre application s'est écartée du RPO de charge de travail estimé lors de la précédente évaluation réussie. Nous fournissons deux valeurs, notre RPO estimé et notre dérive du RPO. Par exemple, si vous voyez une valeur de 2 h sous RPO estimé et 40 m sous Dérive du RPO, cela indique que votre application s'écarte de 40 minutes du RPO de charge de travail estimé de la précédente évaluation réussie.

Révision des recommandations en matière de résilience

Les recommandations de résilience évaluent les composants de l'application et recommandent comment les optimiser en fonction du RTO estimé de la charge de travail et du RPO estimés, des coûts et des modifications minimales.

Avec AWS Resilience Hub, vous pouvez optimiser la résilience à l'aide de l'une des options recommandées suivantes dans Pourquoi choisir cette option :

> **Note**
>
> - AWS Resilience Hub propose jusqu'à trois options AWS Resilience Hub recommandées.
> - Si vous définissez des objectifs RTO et RPO régionaux, AWS Resilience Hub affiche Optimiser pour le RTO/RPO régional dans les options recommandées. Si les objectifs RTO et RPO régionaux ne sont pas définis, le RTO/RPO Optimize for Availability Zone (AZ) s'affiche. Pour plus d'informations sur la définition d'objectifs RTO/RPO régionaux lors de la création de politiques de résilience, consultez. Création de politiques de résilience
> - Les valeurs estimées du RTO de charge de travail et du RPO de charge de travail estimées pour les applications et leurs configurations sont déterminées en tenant compte de la quantité de données et des individus AppComponents. Toutefois, ces valeurs ne sont que des estimations. Vous devez utiliser vos propres tests (par exemple AWS Fault Injection Service) pour tester les temps de restauration réels de votre application.

Optimisation pour la zone de disponibilité RTO/RPO

Durée estimée de restauration de la charge de travail (RTO/RPO) la plus faible possible lors d'une interruption de zone de disponibilité (AZ). Si votre configuration ne peut pas être suffisamment modifiée pour atteindre les objectifs RTO et RPO, vous êtes informé des temps de restauration estimés les plus bas de la charge de travail AZ afin que votre configuration soit proche de la possibilité de respecter la politique.

Optimisation pour la région RTO/RPO

Durée estimée de reprise de la charge de travail (RTO/RPO) la plus faible possible lors d'une interruption régionale. Si votre configuration ne peut pas être suffisamment modifiée pour atteindre les objectifs de RTO et de RPO, vous êtes informé des temps de restauration estimés les plus bas de la région pour que votre configuration soit proche de la possibilité de respecter la politique.

Optimisez en fonction des coûts

Le coût le plus bas que vous puissiez encourir tout en respectant votre politique de résilience. Si votre configuration ne peut pas être suffisamment modifiée pour atteindre les objectifs d'optimisation, vous êtes informé du coût le plus bas que vous pouvez encourir pour que votre configuration soit proche de la possibilité de respecter la politique.

Optimisation pour un minimum de modifications

Les modifications minimales requises pour atteindre les objectifs de votre politique. Si votre configuration ne peut pas être suffisamment modifiée pour atteindre les objectifs d'optimisation, vous êtes informé des modifications recommandées qui peuvent rapprocher votre configuration de la possibilité de respecter la politique.

Les éléments suivants sont inclus dans la ventilation des catégories d'optimisation :

- Description

  Décrit les configurations proposées par AWS Resilience Hub.
- Modifications

  Liste des modifications de texte qui décrivent les tâches nécessaires pour passer à la configuration suggérée.
- Coût de base

  Le coût estimé associé aux modifications recommandées.

> **Note**
>
> Le coût de base peut varier en fonction de l'utilisation et n'inclut aucune remise ni aucune offre du programme de réduction Enterprise (EDP).

- Charge de travail estimée (RTO et RPO)

  Le RTO de charge de travail estimé et le RPO de charge de travail estimé après les modifications.

AWS Resilience Hub évalue si un composant d'application (AppComponent) peut être conforme à une politique de résilience. Si le AppComponent n'est pas conforme à une politique de résilience et qu'AWS Resilience Hub ne peut faire aucune recommandation pour faciliter la conformité, cela peut être dû au fait que le temps de restauration pour le produit sélectionné AppComponent ne peut pas être respecté dans les limites du AppComponent. Les exemples de AppComponent contraintes incluent le type de ressource, la taille du stockage ou la configuration des ressources.

Pour faciliter la conformité de la AppComponent politique de résilience, modifiez le type de ressource de la AppComponent ou mettez à jour la politique de résilience pour l'aligner sur ce que la ressource peut fournir.

Révision des recommandations opérationnelles

Les recommandations opérationnelles contiennent des recommandations pour configurer des alarmes et SOPs des AWS FIS expériences à l'aide AWS CloudFormation de modèles.

AWS Resilience Hub fournit des fichiers AWS CloudFormation modèles vous permettant de télécharger et de gérer l'infrastructure de l'application sous forme de code. Par conséquent, nous fournissons des recommandations AWS CloudFormation afin que vous puissiez les ajouter au code de votre application. Si la taille du fichier AWS CloudFormation modèle est supérieure à un Mo et contient plus de 500 ressources, AWS Resilience Hub génère plusieurs fichiers AWS CloudFormation modèles dont la taille ne dépasse pas un Mo et contient jusqu'à 500 ressources. Si le fichier AWS CloudFormation modèle est divisé en plusieurs fichiers, les noms des fichiers AWS CloudFormation modèles seront ajoutés`partXofY`, où `X` indique le numéro de fichier dans la séquence et `Y` indique le nombre total de fichiers dans lesquels le fichier AWS CloudFormation modèle est divisé. Par exemple, si le fichier modèle `big-app-template5-Alarm-104849185070-us-west-2.yaml` est divisé en quatre fichiers, les noms de fichiers seront les suivants :

- `big-app-template5-Alarm-104849185070-us-west-2-part1of4.yaml`

- `big-app-template5-Alarm-104849185070-us-west-2-part2of4.yaml`
- `big-app-template5-Alarm-104849185070-us-west-2-part3of4.yaml`
- `big-app-template5-Alarm-104849185070-us-west-2-part4of4.yaml`

Toutefois, dans le cas de AWS CloudFormation modèles volumineux, il vous est demandé de fournir l'URI Amazon Simple Storage Service au lieu d'utiliser la CLI/API avec un fichier local en entrée.

Dans AWS Resilience Hub, vous pouvez effectuer les actions suivantes :

- Vous pouvez configurer les alarmes et SOPs les AWS FIS expériences sélectionnées. Pour configurer des alarmes et AWS FIS des expériences, sélectionnez la recommandation appropriée et entrez un nom unique. SOPs AWS Resilience Hub crée un modèle basé sur les recommandations que vous avez sélectionnées. Dans Templates, vous pouvez accéder aux modèles que vous avez créés via une URL Amazon Simple Storage Service (Amazon S3).
- Vous pouvez inclure ou exclure certaines alarmes et AWS FIS expériences recommandées pour votre application à tout moment. SOPs Pour de plus amples informations, veuillez consulter the section called "Y compris ou excluant les recommandations opérationnelles".
- Vous pouvez également rechercher, créer, ajouter, supprimer et gérer des balises pour une application et voir toutes les balises qui lui sont associées.

Y compris ou excluant les recommandations opérationnelles

AWS Resilience Hub propose une option permettant d'inclure ou d'exclure SOPs les alarmes et les AWS FIS expériences (tests) recommandées pour améliorer le score de résilience de votre application à tout moment. L'inclusion et l'exclusion des recommandations opérationnelles n'auront d'impact sur le score de résilience de votre application qu'après avoir effectué une nouvelle évaluation. Nous vous recommandons donc d'effectuer une évaluation pour obtenir le score de résilience mis à jour et comprendre son impact sur votre application.

Pour plus d'informations sur la restriction des autorisations permettant d'inclure ou d'exclure des recommandations par application, consultezthe section called "Limiter les autorisations pour inclure ou exclure AWS Resilience Hub des recommandations".

Pour inclure ou exclure des recommandations opérationnelles dans les applications

1. Dans le menu de navigation de gauche, sélectionnez Applications.
2. Dans Applications, ouvrez une application.

3. Choisissez Évaluations et sélectionnez une évaluation dans le tableau des évaluations de résilience. Si vous n'avez pas d'évaluation, complétez la procédure the section called "Exécution d'évaluations de résilience dans AWS Resilience Hub" puis revenez à cette étape.
4. Sélectionnez l'onglet Recommandations opérationnelles.
5. Pour inclure ou exclure des recommandations opérationnelles de votre application, suivez les procédures suivantes :

Pour inclure ou exclure les alarmes recommandées dans votre application

1. Pour exclure les alarmes, procédez comme suit :
   a. Sous l'onglet Alarmes, dans le tableau des alarmes, sélectionnez toutes les alarmes (avec l'état Non implémenté) que vous souhaitez exclure. Vous pouvez identifier l'état d'implémentation actuel d'une alarme dans la colonne État.
   b. Dans Actions, choisissez Exclure la sélection.
   c. Dans la boîte de dialogue Exclure les recommandations, sélectionnez l'une des raisons suivantes (facultatif), puis choisissez Exclure la sélection pour exclure les alarmes sélectionnées de l'application.
      - Déjà implémenté — Choisissez cette option si vous avez déjà implémenté ces alarmes dans un AWS service tel qu'Amazon CloudWatch ou tout autre fournisseur de services tiers.
      - Non pertinent — Choisissez cette option si les alarmes ne répondent pas aux besoins de votre entreprise.
      - Trop compliqué à mettre en œuvre — Choisissez cette option si vous pensez que ces alarmes sont trop compliquées à implémenter.
      - Autre — Choisissez cette option pour indiquer tout autre motif d'exclusion de la recommandation.
2. Pour inclure des alarmes, procédez comme suit :
   a. Sous l'onglet Alarmes, dans le tableau des alarmes, sélectionnez toutes les alarmes (avec l'état Exclu) que vous souhaitez inclure. Vous pouvez identifier l'état d'implémentation actuel de l'alarme dans la colonne État.
   b. Dans Actions, sélectionnez Inclure la sélection.

c. Dans la boîte de dialogue Inclure les recommandations, choisissez Inclure la sélection pour inclure toutes les alarmes sélectionnées dans votre application.

Pour inclure ou exclure les procédures opérationnelles standard recommandées (SOPs) de votre application

1. Pour exclure les recommandations SOPs, procédez comme suit :

   a. Dans l'onglet Procédures opérationnelles standard, dans le SOPstableau, sélectionnez tous les éléments SOPs (avec l'état Implémenté ou Non implémenté) que vous souhaitez exclure. Vous pouvez identifier l'état d'implémentation actuel d'une SOP dans la colonne État.

   b. Dans Actions, choisissez Exclure les éléments sélectionnés pour exclure les éléments sélectionnés SOPs de votre application.

   c. Dans la boîte de dialogue Exclure les recommandations, sélectionnez l'une des raisons suivantes (facultatif), puis choisissez Exclure la sélection pour exclure la personne sélectionnée SOPs de l'application.

      - Déjà implémentés — Choisissez cette option si vous les avez déjà implémentés SOPs dans un AWS service ou dans tout autre fournisseur de services tiers.
      - Non pertinent — Choisissez cette option si elle SOPs ne répond pas aux besoins de votre entreprise.
      - Trop compliqués à mettre en œuvre : choisissez cette option si vous pensez qu' SOPs ils sont trop compliqués à mettre en œuvre.
      - Aucune — Choisissez cette option si vous ne souhaitez pas en préciser la raison.

2. Pour l'inclure SOPs, procédez comme suit :

   a. Dans l'onglet Procédures opérationnelles standard, dans le SOPstableau, sélectionnez toutes les alarmes (avec l'état Exclu) que vous souhaitez inclure. Vous pouvez identifier l'état d'implémentation actuel de l'alarme dans la colonne État.

   b. Dans Actions, sélectionnez Inclure la sélection.

   c. Dans la boîte de dialogue Inclure les recommandations, choisissez Inclure les éléments sélectionnés pour inclure tous les éléments sélectionnés SOPs dans votre application.

Pour inclure ou exclure les tests recommandés de votre application

1. Pour exclure les tests recommandés, procédez comme suit :
   a. Sous l'onglet Modèles d'expériences d'injection de défauts, dans le tableau Modèles d'expériences d'injection de défauts, sélectionnez tous les tests (avec l'état Implémenté ou Non implémenté) que vous souhaitez exclure. Vous pouvez identifier l'état d'implémentation actuel d'un test dans la colonne État.
   b. Dans Actions, choisissez Exclure la sélection.
   c. Dans la boîte de dialogue Exclure les recommandations, sélectionnez l'une des raisons suivantes (facultatif), puis choisissez Exclure la sélection pour exclure les AWS FIS expériences sélectionnées de l'application.
      - Déjà implémenté — Choisissez cette option si vous avez déjà implémenté ces tests dans un AWS service ou dans un autre fournisseur de services tiers.
      - Non pertinent — Choisissez cette option si les tests ne répondent pas aux exigences de votre entreprise.
      - Trop compliqué à implémenter — Choisissez cette option si vous pensez que ces tests sont trop compliqués à implémenter.
      - Aucune — Choisissez cette option si vous ne souhaitez pas en préciser la raison.
2. Pour inclure les tests recommandés, procédez comme suit :
   a. Sous l'onglet Modèles d'expériences d'injection de défauts, dans le tableau Modèles d'expériences d'injection de défauts, sélectionnez tous les tests (avec l'état Exclus) que vous souhaitez inclure. Vous pouvez identifier l'état d'implémentation actuel du test dans la colonne État.
   b. Dans Actions, sélectionnez Inclure la sélection.
   c. Dans la boîte de dialogue Inclure les recommandations, choisissez Inclure la sélection pour inclure tous les tests sélectionnés dans votre application.

Supprimer les évaluations de résilience

Vous pouvez supprimer les évaluations de résilience dans la vue Évaluations de votre application.

Pour supprimer une évaluation de résilience

1. Dans le menu de navigation de gauche, sélectionnez Applications.

2. Dans Applications, ouvrez une application.
3. Dans Évaluations, choisissez un rapport d'évaluation dans le tableau des évaluations de résilience.
4. Pour confirmer la suppression, choisissez Supprimer.

   Le rapport n'apparaît plus dans le tableau des évaluations de résilience.

Exécution et gestion des évaluations de résilience à partir du widget Resiliency

AWS Resilience Hub vous permet d'exécuter des évaluations pour les applications créées et gérées dans le widget MyApplications in Resiliency. Chaque fois que vous apportez des modifications à une application, il est recommandé d'exécuter une évaluation de résilience à partir du widget Resiliency ou de AWS Resilience Hub la console. Au cours de cette évaluation, la configuration de chaque composant d'application est évaluée par rapport aux politiques établies et aux meilleures pratiques. Sur la base de cette évaluation, l'évaluation génère des recommandations pour la configuration des alarmes, la création de procédures opérationnelles standard (SOPs) et la mise en œuvre de stratégies de test. La mise en œuvre de ces recommandations de configuration peut améliorer la rapidité et l'efficacité de vos procédures de restauration, en garantissant une réponse plus rapide aux incidents et en minimisant les temps d'arrêt potentiels.

Les recommandations relatives aux alarmes vous aident à configurer des alarmes qui détectent les pannes. Les recommandations SOP fournissent des scripts qui gèrent les processus de restauration courants, tels que la restauration à partir d'une sauvegarde. Les recommandations de test proposent des suggestions pour vérifier que vos configurations fonctionnent correctement. Par exemple, vous pouvez vérifier si une application se rétablit lors de processus de restauration automatique, tels que le dimensionnement automatique ou l'équilibrage de charge en raison de problèmes réseau. Vous pouvez vérifier si les alarmes des applications sont déclenchées lorsque les ressources atteignent leurs limites. Vous pouvez également tester votre SOPs efficacité dans les conditions que vous indiquez.

Rubriques :

- Exécution d'évaluations de résilience à partir du widget Resiliency
- Consulter le résumé de l'évaluation dans le widget Resiliency

Exécution d'évaluations de résilience à partir du widget Resiliency

Pour les applications créées dans le widget MyApplications, vous pouvez désormais exécuter des évaluations de résilience à partir du widget et de la console de résilience. AWS Resilience Hub Pour plus d'informations sur l'exécution d'évaluations de résilience depuis AWS Resilience Hub la console, consultezExécution d'évaluations de résilience dans AWS Resilience Hub.

Pour exécuter une évaluation de la résilience d'une application MyApplications existante à partir du widget Resiliency pour la première fois

1. Connectez-vous à la console AWS de gestion.
2. Développez la barre latérale gauche et choisissez MyApplications.
3. Sélectionnez l'application pour laquelle vous souhaitez exécuter une évaluation.

   Comme condition préalable, assurez-vous d'avoir ajouté le widget Resiliency dans votre AWS console. Pour ajouter ce widget, procédez comme suit.

   a. En haut ou en bas à droite du tableau de bord de la console d'accueil, choisissez +Ajouter des widgets.
   b. Choisissez l'indicateur de glissement, représenté par six points verticaux dans le coin supérieur gauche de la barre de titre du widget, puis faites-le glisser vers le tableau de bord de votre console d'accueil.
4. Choisissez Assess application.
5. Pour sélectionner un rôle IAM existant qui sera utilisé pour accéder aux ressources du compte courant, sélectionnez Utiliser un rôle IAM, puis sélectionnez un rôle IAM dans la liste déroulante Sélectionnez un rôle IAM.

   Si vous souhaitez utiliser l'utilisateur IAM actuel pour découvrir les ressources de votre application, choisissez Utiliser les autorisations utilisateur IAM actuelles et sélectionnez Je comprends que je dois configurer manuellement les autorisations pour activer les fonctionnalités requises AWS Resilience Hub dans la section Utiliser l'utilisateur IAM actuel pour découvrir les ressources de l'application.
6. Choisissez Assess.

   Vous pouvez également activer l'option Évaluer automatiquement tous les jours AWS Resilience Hub pour évaluer votre demande quotidiennement sans frais supplémentaires.

   AWS Resilience Hub exécute les actions suivantes :

- Crée une application dans AWS Resilience Hub , découvre et mappe automatiquement les ressources associées.
- Crée et attribue une nouvelle politique de résilience avec des valeurs prédéfinies pour l'objectif de temps de restauration (RTO) et l'objectif de point de restauration (RPO). C'est-à-dire quatre heures pour le RTO et une heure pour le RPO. Après avoir généré une évaluation, vous pouvez modifier la politique de résilience ou en attribuer une autre depuis la AWS Resilience Hub console. Pour plus d'informations sur la mise à jour de la politique de résilience et l'attachement d'une politique différente, consultez la section Gestion des politiques de résilience.
- Évalue la résilience de l'application par rapport au RTO et au RPO, surveille en permanence les ressources et les modifications de configuration, et publie les résultats.

> **Note**
>
> Avant de commencer les évaluations, il est conseillé d'évaluer les coûts potentiels liés à l'exécution des évaluations à l'aide de AWS Resilience Hub. Pour obtenir des informations détaillées sur les prix, consultez les AWS Resilience Hub tarifs.

Pour réexécuter une évaluation de résilience pour une application MyApplications existante à partir du widget Resiliency

1. Connectez-vous à la console AWS de gestion.
2. Développez la barre latérale gauche et choisissez MyApplications.
3. Sélectionnez l'application que vous souhaitez réévaluer.

   Comme condition préalable, assurez-vous d'avoir ajouté le widget Resiliency dans votre AWS console. Pour ajouter ce widget, procédez comme suit.

   a. En haut ou en bas à droite du tableau de bord de la console d'accueil, choisissez +Ajouter des widgets.
   b. Choisissez l'indicateur de glissement, représenté par six points verticaux dans le coin supérieur gauche de la barre de titre du widget, puis faites-le glisser vers le tableau de bord de votre console d'accueil.
4. Choisissez Réévaluer dans le widget Résilience.

Vous pouvez également activer l'option Évaluer automatiquement tous les jours AWS Resilience Hub pour évaluer votre demande quotidiennement sans frais supplémentaires.

Consulter le résumé de l'évaluation dans le widget Resiliency

Le widget Resiliency affiche un aperçu des résultats de l'évaluation qui vous fournira les informations les plus importantes et exploitables sur la résilience de l'application MyApplications, les vulnérabilités potentielles, les indicateurs de performance clés (KPIs) et les actions recommandées pour l'amélioration. Pour en savoir plus sur la posture de résilience de l'application, consultez l'évaluation la plus récente à l'aide des informations suivantes :

- Historique des scores de résilience : ce graphique affiche la tendance du score de résilience de l'application sur une période maximale d'un an.
- Score de résilience : indique le score de résilience de l'application évaluée lors de la dernière évaluation. Ce score reflète dans quelle mesure votre application suit nos recommandations pour respecter la politique de résilience de l'application et pour mettre en œuvre des alarmes, des procédures opérationnelles standard (SOPs) et des expériences AWS Fault Injection Service (AWS FIS). Choisissez le numéro pour afficher des informations supplémentaires dans la section Score de résilience sous l'onglet Résumé de la AWS Resilience Hub console. Pour de plus amples informations, veuillez consulter Rapport d'évaluation.
- Violations des politiques : choisissez le chiffre ci-dessous pour afficher tous les composants de l'application (AppComponents) qui enfreignent les politiques associées à votre application dans le volet Rapport d'évaluation de la AWS Resilience Hub console. Pour de plus amples informations, veuillez consulter Rapport d'évaluation.
- Dérives des politiques — AppComponents Indique celles qui étaient conformes à la politique lors de l'évaluation précédente, mais qui ne l'étaient pas lors de l'évaluation actuelle. Choisissez le numéro ci-dessous pour l'afficher AppComponents dans le volet Rapport d'évaluation de la AWS Resilience Hub console. Pour de plus amples informations, veuillez consulter Rapport d'évaluation.
- Dérives de ressources : choisissez le chiffre ci-dessous pour afficher toutes les ressources issues de la dernière évaluation dans le volet Rapport d'évaluation de la AWS Resilience Hub console. Pour de plus amples informations, veuillez consulter Rapport d'évaluation.
- Accédez à Resilience Hub : choisissez cette option pour ouvrir votre application dans la AWS Resilience Hub console.

Gérer les alarmes

Lorsque vous effectuez une évaluation de la résilience, dans le cadre des recommandations opérationnelles, il est AWS Resilience Hub recommandé de configurer des CloudWatch alarmes Amazon pour surveiller la résilience de votre application. Nous recommandons ces alarmes en fonction des ressources et des composants de la configuration actuelle de votre application. Si les ressources et les composants de votre application changent, vous devez effectuer une évaluation de résilience afin de vous assurer que les CloudWatch alarmes Amazon sont correctes pour votre application mise à jour.

En outre, il détecte et intègre AWS Resilience Hub désormais automatiquement toutes les CloudWatch alarmes Amazon déjà configurées dans ses évaluations de résilience, fournissant ainsi une vue plus complète de la posture de résilience de votre application. Cette nouvelle fonctionnalité associe les AWS Resilience Hub recommandations à votre configuration de surveillance actuelle, rationalisant ainsi la gestion des alarmes et améliorant la précision des évaluations. Si vous avez implémenté une CloudWatch alarme Amazon et que vous AWS Resilience Hub ne la détectez pas automatiquement, vous pouvez exclure l'alarme et sélectionner la raison comme Déjà implémentée. Pour plus d'informations sur l'exclusion des recommandations, consultezY compris ou excluant les recommandations opérationnelles.

AWS Resilience Hub fournit un fichier modèle (`README.md`) qui vous permet de créer des alarmes recommandées par l' AWS Resilience Hub intérieur AWS (Amazon, par exemple CloudWatch) ou par l'extérieur AWS. Les valeurs par défaut fournies dans les alarmes sont basées sur les meilleures pratiques utilisées pour créer ces alarmes.

Rubriques

- Création d'alarmes à partir des recommandations opérationnelles
- Affichage des alarmes

Création d'alarmes à partir des recommandations opérationnelles

AWS Resilience Hub crée un AWS CloudFormation modèle contenant des informations permettant de créer les alarmes sélectionnées sur Amazon CloudWatch. Une fois le modèle généré, vous pouvez y accéder via une URL Amazon S3, le télécharger et le placer dans votre pipeline de code ou créer une pile via la AWS CloudFormation console.

Pour créer une alarme basée sur AWS Resilience Hub des recommandations, vous devez créer un AWS CloudFormation modèle pour les alarmes recommandées et les inclure dans votre base de code.

Pour créer des alarmes dans les recommandations opérationnelles

1. Dans le menu de navigation de gauche, sélectionnez Applications.
2. Dans Applications, sélectionnez votre application.
3. Choisissez l'onglet Évaluations.

   Dans le tableau des évaluations de résilience, vous pouvez identifier vos évaluations à l'aide des informations suivantes :

   - Nom — Nom de l'évaluation que vous avez fournie au moment de la création.
   - État — Indique l'état d'exécution de l'évaluation.
   - État de conformité : indique si l'évaluation est conforme à la politique de résilience.
   - État de dérive de résilience : indique si votre application s'est écartée ou non de la précédente évaluation réussie.
   - Version de l'application : version de votre application.
   - Invocateur — Indique le rôle qui a invoqué l'évaluation.
   - Heure de début — Indique l'heure de début de l'évaluation.
   - Heure de fin — Indique l'heure de fin de l'évaluation.
   - ARN — Le nom de ressource Amazon (ARN) de l'évaluation.
4. Sélectionnez une évaluation dans le tableau des évaluations de résilience. Si vous n'avez pas d'évaluation, complétez la procédure the section called "Exécution d'évaluations de résilience dans AWS Resilience Hub" puis revenez à cette étape.
5. Choisissez Recommandations opérationnelles.
6. Si cette option n'est pas sélectionnée par défaut, choisissez l'onglet Alarmes.

   Dans le tableau des alarmes, vous pouvez identifier les alarmes recommandées à l'aide des méthodes suivantes :

   - Nom : nom de l'alarme que vous avez définie pour votre application.
   - Description — Décrit l'objectif de l'alarme.
   - État — Indique l'état actuel de mise en œuvre des CloudWatch alarmes Amazon.

Cette colonne affiche l'une des valeurs suivantes :

- Implémenté — Indique que les alarmes recommandées par AWS Resilience Hub sont implémentées dans votre application. Le nombre ci-dessous permet de filtrer le tableau des alarmes afin d'afficher toutes les alarmes recommandées mises en œuvre dans votre application.
- Non implémenté — Indique que les alarmes recommandées par AWS Resilience Hub sont incluses mais non implémentées dans votre application. Le nombre ci-dessous permet de filtrer le tableau des alarmes afin d'afficher toutes les alarmes recommandées qui ne sont pas implémentées dans votre application.
- Exclus : indique que les alarmes recommandées par AWS Resilience Hub sont exclues de votre application. Le nombre ci-dessous permet de filtrer le tableau des alarmes afin d'afficher toutes les alarmes recommandées qui sont exclues de votre application. Pour plus d'informations sur l'inclusion et l'exclusion des alarmes recommandées, voir Inclure ou exclure les recommandations opérationnelles.
- Inactif : indique que les alarmes sont déployées sur Amazon CloudWatch, mais que le statut est défini sur INSUSUFFISENT_DATA dans Amazon. CloudWatch Le choix du numéro ci-dessous filtrera le tableau des alarmes pour afficher toutes les alarmes implémentées et inactives.

- Configuration — Indique s'il existe des dépendances de configuration en attente qui doivent être traitées.
- Type — Indique le type d'alarme.
- AppComponent— Indique les composants de l'application (AppComponents) associés à cette alarme.
- ID de référence — Indique l'identifiant logique de l'événement de AWS CloudFormation pile dans AWS CloudFormation.
- ID de recommandation — Indique l'identifiant logique de la ressource de AWS CloudFormation pile dans AWS CloudFormation.

7. Dans l'onglet Alarmes, pour filtrer les recommandations d'alarme dans le tableau des alarmes en fonction d'un état spécifique, sélectionnez un chiffre en dessous de celui-ci.
8. Sélectionnez les alarmes recommandées que vous souhaitez configurer pour votre application, puis choisissez Créer un CloudFormation modèle.

9. Dans la boîte de dialogue Créer un CloudFormation modèle, vous pouvez utiliser le nom généré automatiquement ou entrer un nom pour le AWS CloudFormation modèle dans le champ Nom du CloudFormation modèle.
10. Sélectionnez Create (Créer). La création du AWS CloudFormation modèle peut prendre jusqu'à quelques minutes.

    Procédez comme suit pour inclure les recommandations dans votre base de code.

Pour inclure les AWS Resilience Hub recommandations, votre base de code

1. Choisissez l'onglet Modèles pour afficher le modèle que vous venez de créer. Vous pouvez identifier vos modèles à l'aide des éléments suivants :
   - Nom — Nom de l'évaluation que vous avez fournie au moment de la création.
   - État — Indique l'état d'exécution de l'évaluation.
   - Type — Indique le type de recommandation opérationnelle.
   - Format — Indique le format (JSON/texte) dans lequel le modèle est créé.
   - Heure de début — Indique l'heure de début de l'évaluation.
   - Heure de fin — Indique l'heure de fin de l'évaluation.
   - ARN — L'ARN du modèle
2. Sous Détails du modèle, cliquez sur le lien ci-dessous Templates S3 Path pour ouvrir l'objet modèle dans la console Amazon S3.
3. Dans la console Amazon S3, dans le tableau Objects, cliquez sur le lien du dossier Alarms.
4. Pour copier le chemin Amazon S3, cochez la case située devant le fichier JSON et choisissez Copier l'URL.
5. Créez une AWS CloudFormation pile depuis AWS CloudFormation la console. Pour plus d'informations sur la création d'une AWS CloudFormation pile, consultezhttps://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-console-create-stack.html.

   Lors de la création de la AWS CloudFormation pile, vous devez fournir le chemin Amazon S3 que vous avez copié à l'étape précédente.

Affichage des alarmes

Vous pouvez consulter toutes les alarmes actives que vous avez configurées pour surveiller la résilience de vos applications. AWS Resilience Hub utilise AWS CloudFormation un modèle pour stocker les détails des alarmes, qui sont ensuite utilisés pour créer les alarmes sur Amazon CloudWatch. Vous pouvez accéder au AWS CloudFormation modèle à l'aide de l'URL Amazon S3, le télécharger et le placer dans votre pipeline de code ou créer une pile via la AWS CloudFormation console.

Pour afficher les alarmes depuis le tableau de bord, choisissez Tableau de bord dans le menu de navigation de gauche. Dans le tableau des alarmes implémentées, vous pouvez identifier les alarmes implémentées à l'aide des informations suivantes :

- Application concernée : nom des applications qui ont implémenté cette alarme.
- Alarmes actives — Indique le nombre d'alarmes actives déclenchées par les applications.
- FIS en cours — Indique le AWS FIS test en cours d'exécution pour votre application.

Pour consulter les alarmes implémentées dans votre application

1. Dans le menu de navigation de gauche, sélectionnez Applications.
2. Sélectionnez une application dans le tableau Applications.
3. Dans la page récapitulative de l'application, le tableau des alarmes mises en œuvre affiche toutes les alarmes recommandées mises en œuvre dans votre application.

   Pour rechercher une alarme spécifique dans le tableau des alarmes mises en œuvre, dans la zone Rechercher des alarmes par texte, propriété ou valeur, sélectionnez l'un des champs suivants, choisissez une opération, puis tapez une valeur.

   - Nom de l'alarme : nom de l'alarme que vous avez définie pour votre application.
   - Description — Décrit l'objectif de l'alarme.
   - État — Indique l'état d'implémentation actuel de l' CloudWatch alarme Amazon.

     Cette colonne affiche l'une des valeurs suivantes :

     - Implémenté — Indique que les alarmes recommandées par AWS Resilience Hub sont implémentées dans votre application. Choisissez le numéro ci-dessous pour afficher toutes les alarmes recommandées et mises en œuvre dans l'onglet Recommandations opérationnelles.

- Non implémenté — Indique que les alarmes recommandées par AWS Resilience Hub sont incluses mais non implémentées dans votre application. Choisissez le numéro ci-dessous pour afficher toutes les alarmes recommandées et non implémentées dans l'onglet Recommandations opérationnelles.
- Exclus : indique que les alarmes recommandées par AWS Resilience Hub sont exclues de votre application. Choisissez le numéro ci-dessous pour afficher toutes les alarmes recommandées et exclues dans l'onglet Recommandations opérationnelles. Pour plus d'informations sur l'inclusion et l'exclusion des alarmes recommandées, voir Inclure ou exclure les recommandations opérationnelles.
- Inactif : indique que les alarmes sont déployées sur Amazon CloudWatch, mais que le statut est défini sur INSUSUFFISENT_DATA dans Amazon. CloudWatch Choisissez le numéro ci-dessous pour afficher toutes les alarmes implémentées et inactives dans l'onglet Recommandations opérationnelles.

- Modèle source : fournit le nom de ressource Amazon (ARN) de la AWS CloudFormation pile contenant les détails de l'alarme.
- Ressource : affiche les ressources auxquelles cette alarme est associée et pour lesquelles elle a été implémentée.
- Métrique : affiche la CloudWatch métrique Amazon attribuée à l'alarme. Pour plus d'informations sur CloudWatch les métriques Amazon, consultez Amazon CloudWatch Metrics.
- Dernière modification : affiche la date et l'heure de la dernière modification d'une alarme.

Pour afficher les alarmes recommandées à partir des évaluations

1. Dans le menu de navigation de gauche, sélectionnez Applications.
2. Sélectionnez une application dans le tableau Applications.

   Pour rechercher une application, entrez le nom de l'application dans le champ Rechercher des applications.
3. Choisissez l'onglet Évaluations.

   Dans le tableau des évaluations de résilience, vous pouvez identifier vos évaluations à l'aide des informations suivantes :

   - Nom — Nom de l'évaluation que vous avez fournie au moment de la création.
   - État — Indique l'état d'exécution de l'évaluation.

- État de conformité : indique si l'évaluation est conforme à la politique de résilience.
- État de dérive de résilience : indique si votre application s'est écartée ou non de la précédente évaluation réussie.
- Version de l'application : version de votre application.
- Invocateur — Indique le rôle qui a invoqué l'évaluation.
- Heure de début — Indique l'heure de début de l'évaluation.
- Heure de fin — Indique l'heure de fin de l'évaluation.
- ARN — Le nom de ressource Amazon (ARN) de l'évaluation.

4. Sélectionnez une évaluation dans le tableau des évaluations de résilience.
5. Choisissez l'onglet Recommandations opérationnelles.
6. Si cette option n'est pas sélectionnée par défaut, choisissez l'onglet Alarmes.

   Dans le tableau des alarmes, vous pouvez identifier les alarmes recommandées à l'aide des méthodes suivantes :

   - Nom : nom de l'alarme que vous avez définie pour votre application.
   - Description — Décrit l'objectif de l'alarme.
   - État — Indique l'état actuel de mise en œuvre des CloudWatch alarmes Amazon.

     Cette colonne affiche l'une des valeurs suivantes :

     - Implémenté — Indique que l'alarme est implémentée dans votre application. Le nombre ci-dessous permet de filtrer le tableau des alarmes afin d'afficher toutes les alarmes recommandées mises en œuvre dans votre application.
     - Non implémenté — Indique que l'alarme n'est pas implémentée ou incluse dans votre application. Le nombre ci-dessous permet de filtrer le tableau des alarmes afin d'afficher toutes les alarmes recommandées qui ne sont pas implémentées dans votre application.
     - Exclu : indique que l'alarme est exclue de l'application. Le nombre ci-dessous permet de filtrer le tableau des alarmes afin d'afficher toutes les alarmes recommandées qui sont exclues de votre application. Pour plus d'informations sur l'inclusion et l'exclusion des alarmes recommandées, consultezthe section called “Y compris ou excluant les recommandations opérationnelles”.
     - Inactif : indique que les alarmes sont déployées sur Amazon CloudWatch, mais que le statut est défini sur INSUSUFFISENT_DATA dans Amazon. CloudWatch Le choix du numéro ci-

dessous filtrera le tableau des alarmes pour afficher toutes les alarmes implémentées et inactives.

- Configuration — Indique s'il existe des dépendances de configuration en attente qui doivent être traitées.
- Type — Indique le type d'alarme.
- AppComponent— Indique les composants de l'application (AppComponents) associés à cette alarme.
- ID de référence — Indique l'identifiant logique de l'événement de AWS CloudFormation pile dans AWS CloudFormation.
- ID de recommandation — Indique l'identifiant logique de la ressource de AWS CloudFormation pile dans AWS CloudFormation.

Gestion des procédures opérationnelles standard

Une procédure opérationnelle standard (SOP) est un ensemble d'étapes prescriptives conçues pour restaurer efficacement votre application en cas de panne ou d'alarme. Préparez, testez et mesurez votre capacité SOPs à l'avance pour garantir une reprise rapide en cas de panne opérationnelle.

En fonction des composants de votre application, AWS Resilience Hub recommande ce SOPs que vous devez préparer. AWS Resilience Hub travaille avec Systems Manager pour automatiser vos étapes SOPs en fournissant un certain nombre de documents SSM que vous pouvez utiliser comme base pour celles-ci SOPs.

Par exemple, vous AWS Resilience Hub pouvez recommander un SOP pour ajouter de l'espace disque sur la base d'un document d'automatisation SSM existant. Pour exécuter ce document SSM, vous avez besoin d'un rôle IAM spécifique doté des autorisations appropriées. AWS Resilience Hub crée des métadonnées dans votre application indiquant le document d'automatisation SSM à exécuter en cas de pénurie de disque et le rôle IAM requis pour exécuter ce document SSM. Ces métadonnées sont ensuite enregistrées dans un paramètre SSM.

Outre la configuration de l'automatisation SSM, il est également recommandé de la tester dans le cadre d'une AWS FIS expérience. Par conséquent, fournit AWS Resilience Hub également une AWS FIS expérience qui appelle le document d'automatisation SSM. Ainsi, vous pouvez tester votre application de manière proactive pour vous assurer que le SOP que vous avez créé fait le travail prévu.

AWS Resilience Hub fournit ses recommandations sous la forme d'un AWS CloudFormation modèle que vous pouvez ajouter à la base de code de votre application. Ce modèle fournit :

- Le rôle IAM doté des autorisations requises pour exécuter le SOP.
- Une AWS FIS expérience que vous pouvez utiliser pour tester le SOP.
- Paramètre SSM qui contient les métadonnées de l'application indiquant quel document SSM et quel rôle IAM doivent être exécutés en tant que SOP, et sur quelle ressource. olpPar exemple : `$(DocumentName) for SOP $(HandleCrisisA) on $(ResourceA)`.

La création d'un SOP peut nécessiter quelques essais et erreurs. Exécuter une évaluation de la résilience de votre application et générer un AWS CloudFormation modèle à partir des AWS Resilience Hub recommandations constitue un bon début. Utilisez le AWS CloudFormation modèle pour générer une AWS CloudFormation pile, puis utilisez les paramètres SSM et leurs valeurs par défaut dans votre SOP. Exécutez les SOP et voyez quelles améliorations vous devez apporter.

Comme toutes les applications ont des exigences différentes, la liste par défaut des documents SSM AWS Resilience Hub fournis ne suffira pas à répondre à tous vos besoins. Vous pouvez toutefois copier les documents SSM par défaut et les utiliser comme base pour créer vos propres documents personnalisés adaptés à votre application. Vous pouvez également créer vos propres documents SSM entièrement nouveaux. Si vous créez vos propres documents SSM au lieu de modifier les valeurs par défaut, vous devez les associer à des paramètres SSM afin que le document SSM approprié soit appelé lors de l'exécution de la SOP.

Lorsque vous avez finalisé votre SOP en créant les documents SSM nécessaires et en mettant à jour les associations de paramètres et de documents selon les besoins, ajoutez les documents SSM directement à votre base de code et apportez-y les modifications ou personnalisations ultérieures. Ainsi, chaque fois que vous déploierez votre application, vous déploierez également le plus grand nombre de up-to-date SOP.

Rubriques

- Élaboration d'une SOP basée sur les recommandations AWS Resilience Hub
- Création d'un document SSM personnalisé
- Utiliser un document SSM personnalisé au lieu du document par défaut
- Tests SOPs
- Affichage des procédures opérationnelles standard

Élaboration d'une SOP basée sur les recommandations AWS Resilience Hub

Pour créer une SOP basée sur AWS Resilience Hub des recommandations, vous avez besoin d'une AWS Resilience Hub application associée à une politique de résilience, et vous devez avoir effectué une évaluation de la résilience de cette application. L'évaluation de la résilience génère les recommandations pour votre SOP.

Pour créer une SOP basée sur AWS Resilience Hub des recommandations, vous devez créer un AWS CloudFormation modèle pour les recommandations SOPs et les inclure dans votre base de code.

Création d'un AWS CloudFormation modèle pour les recommandations SOP

1. Ouvrez la AWS Resilience Hub console.
2. Dans le volet de navigation, choisissez Applications.
3. Dans la liste des applications, choisissez celle pour laquelle vous souhaitez créer une SOP.
4. Choisissez l'onglet Évaluations.
5. Sélectionnez une évaluation dans le tableau des évaluations de résilience. Si vous n'avez pas d'évaluation, complétez la procédure the section called "Exécution d'évaluations de résilience dans AWS Resilience Hub" puis revenez à cette étape.
6. Sous Recommandations opérationnelles, sélectionnez Procédures opérationnelles standard.
7. Sélectionnez toutes les recommandations SOP que vous souhaitez inclure.
8. Choisissez Créer un CloudFormation modèle. La création du AWS CloudFormation modèle peut prendre jusqu'à quelques minutes.

   Procédez comme suit pour inclure les recommandations SOP dans votre base de code.

Pour inclure les AWS Resilience Hub recommandations dans votre base de code

1. Dans Recommandations opérationnelles, sélectionnez Modèles.
2. Dans la liste des modèles, choisissez le nom du modèle SOP que vous venez de créer.

   Vous pouvez identifier ceux SOPs qui sont implémentés dans votre application à l'aide des informations suivantes :

   - Nom du SOP : nom du SOP que vous avez défini pour votre application.

- Description — Décrit l'objectif de la SOP.
- Document SSM : URL Amazon S3 du document SSM contenant la définition SOP.
- Test run : URL Amazon S3 du document contenant les résultats du dernier test.
- Modèle source — Fournit le nom de ressource Amazon (ARN) de la AWS CloudFormation pile contenant les détails du SOP.

3. Sous Détails du modèle, cliquez sur le lien dans Templates S3 Path pour ouvrir l'objet modèle dans la console Amazon S3.
4. Dans la console Amazon S3, dans le tableau Objects, choisissez le lien du dossier SOP.
5. Pour copier le chemin Amazon S3, cochez la case située devant le fichier JSON et choisissez Copier l'URL.
6. Créez une AWS CloudFormation pile depuis AWS CloudFormation la console. Pour plus d'informations sur la création d'une AWS CloudFormation pile, consultezhttps://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-console-create-stack.html.

   Lors de la création de la AWS CloudFormation pile, vous devez fournir le chemin Amazon S3 que vous avez copié à l'étape précédente.

Création d'un document SSM personnalisé

Pour automatiser complètement la restauration de votre application, vous devrez peut-être créer un document SSM personnalisé pour votre SOP dans la console Systems Manager. Vous pouvez modifier un document SSM existant comme base ou créer un nouveau document SSM.

Pour des informations détaillées sur l'utilisation de Systems Manager pour créer un document SSM, voir Procédure pas à pas : utilisation de Document Builder pour créer un runbook personnalisé.

Pour plus d'informations sur la syntaxe des documents SSM, voir Syntaxe des documents SSM.

Pour plus d'informations sur l'automatisation des actions sur les documents SSM, reportez-vous à la section Référence des actions d'automatisation de Systems Manager.

Utiliser un document SSM personnalisé au lieu du document par défaut

Pour remplacer le document SSM AWS Resilience Hub suggéré pour votre SOP par un document personnalisé que vous avez créé, travaillez directement dans votre base de code. En plus d'ajouter votre nouveau document d'automatisation SSM personnalisé, vous allez également :

1. Ajoutez les autorisations IAM requises pour exécuter l'automatisation.
2. Ajoutez un test pour AWS FIS tester votre document SSM.
3. Ajoutez un paramètre SSM qui pointe vers le document d'automatisation que vous souhaitez utiliser comme SOP.

En général, il est plus efficace de travailler avec les valeurs par défaut suggérées AWS Resilience Hub et de les personnaliser si nécessaire. Par exemple, ajoutez ou supprimez des autorisations selon les besoins pour le rôle IAM, modifiez la configuration de l' AWS FIS expérience pour qu'elle pointe vers le nouveau document SSM ou modifiez le paramètre SSM pour qu'il pointe vers votre nouveau document SSM.

Tests SOPs

Comme indiqué précédemment, la meilleure pratique consiste à ajouter AWS FIS des tests à vos pipelines CI/CD afin de les tester SOPs régulièrement ; cela garantit qu'ils sont prêts à fonctionner en cas de panne.

Testez à la fois les AWS Resilience Hub options fournies et personnalisées SOPs.

Affichage des procédures opérationnelles standard

Pour afficher les applications mises SOPs en œuvre

1. Dans le menu de navigation de gauche, sélectionnez Applications.
2. Dans Applications, ouvrez une application.
3. Choisissez l'onglet Procédures opérationnelles standard.

   Dans la section Récapitulatif des procédures opérationnelles standard, le tableau des procédures opérationnelles standard mises en œuvre affiche la liste de celles SOPs qui sont générées à partir des recommandations des SOP.

   Vous pouvez l'identifier SOPs par les moyens suivants :

   - Nom du SOP : nom du SOP que vous avez défini pour votre application.
   - Document SSM : URL S3 du document Amazon EC2 Systems Manager contenant la définition des SOP.
   - Description — Décrit l'objectif de la SOP.
   - Test run : URL S3 du document contenant les résultats du dernier test.

- ID de référence — Identifiant de la recommandation SOP référencée.
- ID de ressource — Identifiant de la ressource pour laquelle la recommandation SOP est mise en œuvre.

Pour consulter les recommandations SOPs issues des évaluations

1. Dans le menu de navigation de gauche, sélectionnez Applications.
2. Sélectionnez une application dans le tableau Applications.

   Pour rechercher une application, entrez le nom de l'application dans le champ Rechercher des applications.
3. Choisissez l'onglet Évaluations.

   Dans le tableau des évaluations de résilience, vous pouvez identifier vos évaluations à l'aide des informations suivantes :

   - Nom — Nom de l'évaluation que vous avez fournie au moment de la création.
   - État — Indique l'état d'exécution de l'évaluation.
   - État de conformité : indique si l'évaluation est conforme à la politique de résilience.
   - État de dérive de résilience : indique si votre application s'est écartée ou non de la précédente évaluation réussie.
   - Version de l'application : version de votre application.
   - Invocateur : indique le rôle qui a invoqué l'évaluation.
   - Heure de début — Indique l'heure de début de l'évaluation.
   - Heure de fin — Indique l'heure de fin de l'évaluation.
   - ARN — Le nom de ressource Amazon (ARN) de l'évaluation.
4. Sélectionnez une évaluation dans le tableau des évaluations de résilience.
5. Choisissez l'onglet Recommandations opérationnelles.
6. Choisissez l'onglet Procédures opérationnelles standard.

   Dans le tableau des procédures opérationnelles standard, vous pouvez en savoir plus sur les recommandations SOPs à l'aide des informations suivantes :

   - Nom — Nom de la procédure opérationnelle normalisée recommandée.
   - Description — Décrit l'objectif de la SOP.

- État — Indique l'état actuel de mise en œuvre du SOP. C'est-à-dire implémenté, non implémenté et exclu.
- Configuration — Indique s'il existe des dépendances de configuration en attente qui doivent être traitées.
- Type — Indique le type de SOP.
- AppComponent— Indique les composants de l'application (AppComponents) associés à cette SOP. Pour plus d'informations sur les ressources prises en charge AppComponents, consultez la section Regroupement des ressources dans un AppComponent.
- ID de référence — Indique l'identifiant logique de l'événement de AWS CloudFormation pile dans AWS CloudFormation.
- ID de recommandation — Indique l'identifiant logique de la ressource de AWS CloudFormation pile dans AWS CloudFormation.

Gestion des AWS Fault Injection Service expériences

Cette section décrit comment gérer AWS Fault Injection Service (AWS FIS) les expériences dans AWS Resilience Hub. Vous réalisez AWS FIS des tests pour mesurer la résilience de vos AWS ressources et le temps nécessaire à la restauration après un incident lié à une application, à une infrastructure, à une zone de disponibilité ou à une AWS région.

Pour mesurer la résilience, ces AWS FIS expériences simulent les perturbations de vos AWS ressources. Parmi les exemples de perturbations, citons les erreurs d'indisponibilité du réseau, les basculements, les processus interrompus sur Amazon EC2 ou AWS ASG, la restauration au démarrage sur Amazon RDS et les problèmes liés à votre zone de disponibilité. À la fin de l' AWS FIS expérience, vous pouvez estimer si une application peut se rétablir après les types de panne définis dans l'objectif RTO de la politique de résilience.

Toutes les expériences AWS Resilience Hub sont construites à l'aide d'actions AWS FIS et exécutent AWS FIS des actions. AWS FIS les expériences utilisent uniquement des actions AWS FIS d'automatisation personnalisées pour des AWS services spécifiques (telles que l'action Amazon EKS). Pour plus d'informations sur les AWS FIS actions, reportez-vous à la section Référence AWS FIS des actions.

Vous pouvez utiliser les AWS FIS tests dans leur état par défaut ou les personnaliser en fonction de vos besoins. Pour plus d'informations sur la gestion AWS FIS des tests depuis AWS Resilience Hub la AWS FIS console et la console, consultez les rubriques suivantes :

- AWS Resilience Hub console
  - Visualisation AWS FIS des expériences
    - Pour consulter la liste des AWS FIS expériences mises en œuvre à partir des applications
    - Pour consulter les AWS FIS expériences recommandées à partir des évaluations
  - the section called " AWS FIS Expériences en cours"
  - the section called "AWS Fault Injection Service échecs d'expérience/vérification de l'état"
- AWS FIS console
  - Gérer vos AWS FIS expériences
  - Utilisation de la bibliothèque de AWS FIS scénarios
  - Gestion des modèles AWS FIS d'expériences

Lancer, créer et exécuter AWS FIS des expériences

AWS Resilience Hub simplifie AWS FIS les expériences en les intégrant aux AWS FIS expériences. Il fournit des recommandations personnalisées et permet de lancer AWS FIS des expériences avec des modèles préremplis mappés à vos composants d'application (AppComponents), permettant ainsi des tests de résilience efficaces.

Pour lancer une AWS FIS expérience à partir des recommandations opérationnelles

1. Ouvrez la AWS Resilience Hub console.
2. Dans le volet de navigation, choisissez Applications.
3. Dans la liste des applications, choisissez l'application pour laquelle vous souhaitez créer un test.
4. Choisissez l'onglet Évaluations.
5. Sélectionnez une évaluation dans le tableau des évaluations de résilience. Si vous n'avez pas d'évaluation, complétez la procédure the section called "Exécution d'évaluations de résilience dans AWS Resilience Hub" puis revenez à cette étape.
6. Choisissez l'onglet Recommandations opérationnelles.
7. Cliquez sur la flèche droite avant les expériences d'injection de défauts.

   Cette section répertorie toutes les AWS FIS expériences recommandées par votre application AWS Resilience Hub pour effectuer des tests de résistance et améliorer sa résilience. En fonction de votre implémentation, les AWS FIS expériences sont classées dans les états suivants :

- Implémenté — Indique que les expériences recommandées par AWS Resilience Hub sont implémentées dans votre application. Choisissez le numéro ci-dessous pour afficher toutes les expériences mises en œuvre dans le tableau des expériences.
- Mise en œuvre partielle : indique que les expériences recommandées par AWS Resilience Hub sont partiellement mises en œuvre dans votre application. Choisissez le chiffre ci-dessous pour afficher toutes les expériences partiellement mises en œuvre dans le tableau des expériences.
- Non implémenté — Indique que les expériences recommandées par AWS Resilience Hub ne sont pas implémentées dans votre application. Choisissez le chiffre ci-dessous pour afficher toutes les expériences non mises en œuvre dans le tableau des expériences.
- Exclus — Indique que les expériences recommandées par AWS Resilience Hub sont exclues de votre application. Choisissez le numéro ci-dessous pour afficher toutes les expériences exclues dans le tableau des expériences. Pour plus d'informations sur l'inclusion et l'exclusion des expériences recommandées, voir Inclure ou exclure les recommandations opérationnelles.

Le tableau des expériences répertorie toutes les AWS FIS expériences mises en œuvre qui ont un impact sur le score de résilience de votre application. Vous pouvez identifier les AWS FIS expériences à l'aide des informations suivantes :

- Nom de l'action : indique l' AWS FIS action recommandée pour votre application. Choisissez le nom de l'action pour afficher toutes les actions recommandées AppComponents sur la page des détails de l'AWS FIS expérience. Lorsque l'état est défini sur Non traçable, cela indique que l' AWS FIS expérience est un scénario. Choisissez le nom du scénario pour en afficher les détails sur la page de la bibliothèque de scénarios de la AWS FIS console.
- État — Indique l'état actuel de mise en œuvre de l' AWS FIS expérience. C'est-à-dire, mis en œuvre, partiellement mis en œuvre, non mis en œuvre et exclu.

> **Note**
>
> AWS FIS Le scénario est une fonctionnalité réservée à la console avec plusieurs actions prédéfinies. Par conséquent, vous AWS Resilience Hub ne pouvez pas le suivre et l'état sera défini sur Non traçable.

- Description — Décrit l'objectif de l' AWS FIS action.

8. Sélectionnez une AWS FIS action pour laquelle vous souhaitez lancer un test.

Dans la section des recommandations d' AWS FIS expériences, vous pouvez en savoir plus sur les expériences que vous devez mettre en œuvre AppComponents à l'aide des informations suivantes :

- Nom — Nom du groupe AppComponent dans lequel les ressources sont regroupées.
- État — Indique l'état actuel de mise en œuvre de l' AWS FIS action. C'est-à-dire, mis en œuvre, partiellement mis en œuvre, non mis en œuvre et exclu.

> **Note**
>
> AWS FIS Le scénario est une fonctionnalité réservée à la console avec plusieurs actions prédéfinies. Par conséquent, vous AWS Resilience Hub ne pouvez pas le suivre et l'état sera défini sur Non traçable.

- Sélection de la cible : indique comment les ressources seront incluses dans l'expérience lorsque vous choisissez Lancer l'expérience. Si AWS Resilience Hub cela ne détermine pas automatiquement les ressources cibles, passez le curseur sur le champ de sélection cible correspondant pour savoir comment les ajouter.
- Ressources — Indique le nombre de ressources regroupées sous le AppComponent. Choisissez le numéro pour afficher ces ressources dans la boîte de dialogue Ressources. Vous pouvez identifier les ressources à l'aide des éléments suivants :
  - ID logique — Indique l'ID logique de la ressource. Un ID logique est un nom utilisé pour identifier les ressources de votre fichier d'état Terraform AWS CloudFormation, de votre application MyApplications, de votre AWS Resource Groups ressource ou de votre cluster Amazon Elastic Kubernetes Service.
  - ID physique : indique l'identifiant réellement attribué à la ressource, tel qu'un identifiant d' EC2 instance Amazon ou un nom de compartiment Amazon S3.
  - Type — Indique le type de ressource.
  - Région — Indique la AWS région dans laquelle se trouve la ressource.

9. Sélectionnez-en un AppComponent et choisissez Inclure ou Exclure pour l'inclure ou l'exclure AppComponent dans l' AWS FIS expérience, respectivement.
10. Choisissez Initiate experiment.

    AWS Resilience Hub vous redirigera vers la page Spécifier les détails du modèle dans la AWS FIS console, en l'ouvrant dans un nouvel onglet.

11. Pour créer un modèle d'expérience, suivez les étapes décrites dans Pour créer un modèle d'expérience à l'aide de la console.

    En outre, après avoir saisi les détails du modèle et choisi Suivant dans la page Spécifier les détails du modèle de la AWS FIS console en suivant les étapes décrites dans Pour créer un modèle d'expérience à l'aide de la console, essaie AWS Resilience Hub automatiquement de mapper les actions et les cibles pour vos types de ressources sur la page Actions et cibles. Toutefois, pour améliorer la couverture, vous pouvez ajouter manuellement des actions et des cibles en choisissant respectivement Ajouter une action et Ajouter une cible, puis terminer le reste de la procédure pour créer votre expérience.

AWS FIS Expériences en cours

Après avoir créé un test dans AWS FIS la console, suivez les étapes décrites dans Démarrer un test à partir d'un modèle pour exécuter un test dans AWS FIS la console. Si vous AWS Resilience Hub souhaitez détecter les dernières expériences auxquelles vous avez participé AWS FIS, vous devez effectuer une nouvelle évaluation. Pour plus d'informations sur l'exécution d'évaluations, consultezExécution d'évaluations de résilience dans AWS Resilience Hub.

Visualisation AWS FIS des expériences

Dans AWS Resilience Hub, consultez les AWS FIS tests que vous avez mis en place pour mesurer la résilience de vos AWS ressources et le temps nécessaire à la restauration après une application, une infrastructure, une zone de disponibilité et des Région AWS incidents.

Pour afficher la liste des AWS FIS expériences actives depuis le tableau de bord, choisissez Tableau de bord dans le menu de navigation de gauche.

Dans le tableau Expériences mises en œuvre, vous pouvez identifier les AWS FIS expériences à l'aide des informations suivantes :

- ID de l'expérience — Identifiant de l' AWS FIS expérience.
- Action — Indique l' AWS FIS action associée à l' AWS FIS expérience. De plus, s'il existe plusieurs actions, le nombre d' AWS FIS actions associées à l' AWS FIS expérience est mis en évidence. Vous pouvez identifier les détails en les survolant ou en naviguant vers eux.
- ID du modèle d'expérience — Identifiant du modèle d' AWS FIS expérience qui a été utilisé pour créer l' AWS FIS expérience.

Pour consulter la liste des AWS FIS expériences mises en œuvre à partir des applications

1. Dans le menu de navigation de gauche, sélectionnez Applications.
2. Sélectionnez une application dans le tableau Applications.

   Pour rechercher une application, entrez le nom de l'application dans le champ Rechercher des applications.
3. Choisissez Fault injection experiments.

   Dans le tableau Expériences mises en œuvre, vous pouvez identifier les AWS FIS expériences mises en œuvre dans votre application à l'aide des informations suivantes :

   - ID de l'expérience — Identifiant de l' AWS FIS expérience.
   - Action — Indique l' AWS FIS action associée à l' AWS FIS expérience. De plus, s'il existe plusieurs actions, le nombre d' AWS FIS actions associées à l' AWS FIS expérience est mis en évidence. Vous pouvez identifier les détails en les survolant ou en naviguant vers eux.
   - ID du modèle d'expérience — Identifiant du modèle d' AWS FIS expérience qui a été utilisé pour créer l' AWS FIS expérience.

Pour consulter les AWS FIS expériences recommandées à partir des évaluations

1. Dans le menu de navigation de gauche, sélectionnez Applications.
2. Sélectionnez une application dans le tableau Applications.

   Pour rechercher une application, entrez le nom de l'application dans le champ Rechercher des applications.
3. Choisissez l'onglet Évaluations.

   Dans le tableau Évaluations, vous pouvez identifier vos évaluations à l'aide des informations suivantes :

   - Nom — Nom de l'évaluation que vous avez fournie au moment de la création.
   - État — Indique l'état d'exécution de l'évaluation.
   - État de conformité : indique si l'évaluation est conforme à la politique de résilience.
   - Résilience : indique si votre application s'est écartée des objectifs RTO et RPO définis dans la politique de résilience ci-jointe ou non par rapport à l'évaluation réussie précédente.
   - Version de l'application : version de votre application qui a été évaluée.

- Invocateur — Indique le rôle qui a invoqué l'évaluation.
- Heure de début — Indique l'heure de début de l'évaluation.
- Heure de fin — Indique l'heure de fin de l'évaluation.
- ARN — Le nom de ressource Amazon (ARN) de l'évaluation.

4. Sélectionnez une évaluation dans le tableau Évaluations.
5. Choisissez Recommandations opérationnelles.
6. Cliquez sur la flèche droite avant les expériences d'injection de défauts.

   Cette section répertorie toutes les AWS FIS expériences recommandées par votre application AWS Resilience Hub pour effectuer des tests de résistance et améliorer sa résilience. En fonction de votre implémentation, les AWS FIS expériences sont classées dans les états suivants :

   - Implémenté — Indique que les expériences recommandées par AWS Resilience Hub sont implémentées dans votre application. Choisissez le numéro ci-dessous pour afficher toutes les expériences mises en œuvre dans le tableau des expériences.
   - Mise en œuvre partielle : indique que les expériences recommandées par AWS Resilience Hub sont partiellement mises en œuvre dans votre application. Choisissez le chiffre ci-dessous pour afficher toutes les expériences partiellement mises en œuvre dans le tableau des expériences.
   - Non implémenté — Indique que les expériences recommandées par AWS Resilience Hub ne sont pas implémentées dans votre application. Choisissez le chiffre ci-dessous pour afficher toutes les expériences non mises en œuvre dans le tableau des expériences.
   - Exclus — Indique que les expériences recommandées par AWS Resilience Hub sont exclues de votre application. Choisissez le numéro ci-dessous pour afficher toutes les expériences exclues dans le tableau des expériences. Pour plus d'informations sur l'inclusion et l'exclusion des expériences recommandées, voir Inclure ou exclure les recommandations opérationnelles.

   Le tableau des expériences répertorie toutes les AWS FIS expériences mises en œuvre qui ont un impact sur le score de résilience de votre application. Vous pouvez identifier les AWS FIS expériences à l'aide des informations suivantes :

   - Nom de l'action : indique l' AWS FIS action recommandée pour votre application. Lorsque l'état est défini sur Non traçable, cela indique que l' AWS FIS expérience est un scénario.

Choisissez le nom du scénario pour en afficher les détails sur la page de la bibliothèque de scénarios de la AWS FIS console.

- État — Indique l'état actuel de mise en œuvre de l' AWS FIS expérience. C'est-à-dire, mis en œuvre, partiellement mis en œuvre, non mis en œuvre et exclu.

> **Note**
>
> AWS FIS Le scénario est une fonctionnalité réservée à la console avec plusieurs actions prédéfinies. Par conséquent, vous AWS Resilience Hub ne pouvez pas le suivre et l'état sera défini sur Non traçable.

- Description — Décrit l'objectif de l' AWS FIS action.

AWS Fault Injection Service échecs d'expérience/vérification de l'état

AWS Resilience Hub vous permet de suivre l'état de l'expérience que vous avez commencée. Pour plus d'informations, consultez la Pour consulter les AWS FIS expériences recommandées à partir des évaluations procédure.

Rubriques

- Analyse de l'exécution des AWS FIS expériences à l'aide AWS de Systems Manager
- AWS FIS testez les échecs lors du test des pods Kubernetes exécutés dans vos clusters Amazon Elastic Kubernetes Service

Analyse de l'exécution des AWS FIS expériences à l'aide AWS de Systems Manager

Après avoir exécuté une AWS FIS expérience, vous pouvez consulter les détails de l'exécution dans le AWS Systems Manager.

1. Accédez à CloudTrail> Historique des événements.
2. Filtrez les événements par nom d'utilisateur à l'aide de l'ID de l'expérience.
3. Consultez l' StartAutomationExecution entrée. L'ID de demande est l'ID d'automatisation SSM.
4. Accédez à AWS Systems Manager > Automation.
5. Filtrez par ID d'exécution à l'aide de l'ID d'automatisation SSM et affichez les détails de l'automatisation.

Vous pouvez analyser l'exécution avec n'importe quelle automatisation de Systems Manager. Pour plus d'informations, consultez le guide de l'utilisateur d'AWS Systems Manager Automation. Les paramètres d'entrée d'exécution apparaissent dans la section Paramètres d'entrée du détail de l'exécution et incluent des paramètres facultatifs qui n'apparaissent pas dans l' AWS FIS expérience.

Vous pouvez trouver des informations sur le statut des étapes et d'autres détails sur les étapes en accédant aux étapes spécifiques dans les étapes d'exécution.

Défaillances courantes

Les défaillances les plus courantes rencontrées lors de l'exécution d'un rapport d'évaluation sont les suivantes :

- Le modèle d'alarme n'a pas été déployé avant l'exécution de l'expérience test/SOP. Cela provoque un message d'erreur lors de l'étape d'automatisation.
  - Message d'échec : `The following parameters were not found: [/ResilienceHub/Alarm/3dee49a1-9877-452a-bb0c-a958479a8ef2/nat-gw-alarm-bytes-out-to-source-2020-09-21_nat-02ad9bc4fbd4e6135]. Make sure all the SSM parameters in automation document are created in SSM Parameter Store.`
  - Correction : assurez-vous de générer l'alarme appropriée et de déployer le modèle obtenu avant de relancer l'expérience d'injection de défauts.
- Autorisations manquantes dans le rôle d'exécution. Ce message d'erreur apparaît si le rôle d'exécution fourni ne dispose pas d'une autorisation et apparaît dans les détails de l'étape.
  - Message d'échec :`An error occurred (Unauthorized Operation) when calling the DescribeInstanceStatus operation: You are not authorized to perform this operation. Please Refer to Automation Service Troubleshooting Guide for more diagnosis details.`
  - Correction : vérifiez que vous avez fourni le rôle d'exécution correct. Si cela a été fait, ajoutez l'autorisation requise et relancez l'évaluation.
- L'exécution a réussi mais n'a pas eu le résultat escompté. Cela est dû à des paramètres incorrects ou à un problème d'automatisation interne.
  - Message d'échec : l'exécution a réussi, aucun message d'erreur n'est donc affiché.

- Correction : vérifiez les paramètres d'entrée et examinez les étapes exécutées comme expliqué dans la section Analyser l'exécution de l' AWS FIS expérience avant d'examiner les différentes étapes pour déterminer les entrées et sorties attendues.

AWS FIS testez les échecs lors du test des pods Kubernetes exécutés dans vos clusters Amazon Elastic Kubernetes Service

Voici les défaillances courantes d'Amazon Elastic Kubernetes Service (Amazon EKS) rencontrées lors du test des pods Kubernetes exécutés dans vos clusters Amazon EKS :

- Configuration incorrecte des rôles IAM pour les AWS FIS expériences ou le compte de service Kubernetes.
  - Messages d'échec :
    - `Error resolving targets. Kubernetes API returned ApiException with error code 401`.
    - `Error resolving targets. Kubernetes API returned ApiException with error code 403`.
    - `Unable to inject AWS FIS Pod: Kubernetes API returned status code 403. Check Amazon EKS logs for more details`.
  - Correction : vérifiez les points suivants.
    - Assurez-vous d'avoir suivi les instructions de la section Utiliser les AWS FIS`aws:eks:pod` actions.
    - Assurez-vous d'avoir créé et configuré un compte de service Kubernetes avec les autorisations RBAC nécessaires et le bon espace de noms.
    - Assurez-vous d'avoir mappé le rôle IAM fourni (voir le résultat de la AWS CloudFormation pile du test) à l'utilisateur Kubernetes.
- Impossible de démarrer le AWS FIS Pod : le nombre maximum de conteneurs sidecar défaillants a été atteint. Cela se produit généralement lorsque la mémoire n'est pas suffisante pour exécuter le conteneur AWS FIS sidecar.
  - Message d'échec :`Unable to heartbeat FIS Pod: Max failed sidecar containers reached`.
  - Correction : L'une des options pour éviter cette erreur consiste à réduire le pourcentage de charge cible afin de l'aligner sur la mémoire ou le processeur disponible.

- L'assertion de l'alarme a échoué au début de l'expérience. Cette erreur se produit car l'alarme associée ne possède aucun point de données.
  - Message d'échec :`Assertion failed for the following alarms`. Répertorie toutes les alarmes pour lesquelles l'assertion a échoué.
  - Correction : assurez-vous que Container Insights est correctement installé pour les alarmes et que l'alarme n'est pas activée (en `ALARM` état).

Comprendre les scores de résilience

Cette section décrit comment AWS Resilience Hub quantifier le niveau de préparation des applications à partir de différents scénarios d'interruption.

AWS Resilience Hub fournit un score de résilience qui représente la posture de résilience de l'application. Ce score reflète dans quelle mesure l'application suit nos recommandations pour respecter la politique de résilience, les alarmes, les procédures opérationnelles standard (SOPs) et les tests de l'application. En fonction du type de ressources que l'application utilise, AWS Resilience Hub recommande des alarmes et effectue une série de tests pour chaque type d'interruption. SOPs

Le meilleur score de résilience est de 100 points. Pour obtenir le meilleur score possible ou le meilleur score, vous devez implémenter toutes les alarmes et tests recommandés dans votre application. SOPs Par exemple, AWS Resilience Hub recommande un test avec une alarme et un SOP. Le test s'exécute, déclenche l'alarme et lance le SOP associé. S'ils fonctionnent correctement et si l'application respecte la politique de résilience, elle reçoit un score de résilience proche ou égal à 100 points.

Après avoir effectué la première évaluation, AWS Resilience Hub propose une option permettant d'exclure les recommandations opérationnelles de votre application. Pour comprendre l'impact des recommandations exclues sur le score de résilience, vous devez effectuer une nouvelle évaluation. Cependant, vous pouvez toujours inclure les recommandations exclues dans votre candidature et effectuer une nouvelle évaluation. Pour plus d'informations sur l'inclusion et l'exclusion des recommandations relatives aux alarmes, aux SOP et aux tests, consultezthe section called “Y compris ou excluant les recommandations opérationnelles”.

Accès au score de résilience de vos applications

Vous pouvez consulter le score de résilience de votre application en choisissant Tableau de bord ou Applications dans le menu de navigation.

Accès au score de résilience depuis le tableau de bord

1. Dans le menu de navigation de gauche, choisissez Dashboard.
2. Dans Score de résilience des applications au fil du temps, choisissez une ou plusieurs applications dans la liste déroulante Choisissez jusqu'à 4 applications.
3. Le graphique du score de résilience affiche le score de résilience pour toutes les applications choisies.

Accès au score de résilience depuis les applications

1. Dans le menu de navigation de gauche, sélectionnez Applications.
2. Dans Applications, ouvrez une application.
3. Choisissez Résumé.

   Le graphique du score de résilience affiche l'évolution du score de résilience de votre application sur une période maximale d'un an. AWS Resilience Hub affiche les mesures à prendre, les violations des politiques de résilience et les recommandations opérationnelles qui doivent être prises en compte pour améliorer et atteindre le score de résilience maximal possible en utilisant les éléments suivants :

   - Pour afficher les actions à exécuter afin d'améliorer et d'atteindre le score de résilience maximal possible, choisissez l'onglet Actions à exécuter. Lorsque cette option est sélectionnée, AWS Resilience Hub affiche ce qui suit :
     - RTO/RPO — Indique le nombre de temps de récupération (RTO/RPOs) that need to be fixed to resolve the breaches in your application's resiliency policy. Choose the value to view the RTO/RPOdétails dans le rapport d'évaluation de votre application).
     - Alarmes — Indique le nombre d' CloudWatch alarmes Amazon recommandées qui doivent être implémentées dans votre application. Choisissez la valeur pour afficher les CloudWatch alarmes Amazon qui doivent être corrigées dans le rapport d'évaluation de votre application.
     - SOPs— Indique le nombre de recommandations SOPs qui doivent être mises en œuvre dans votre application. Choisissez la valeur pour afficher celle SOPs qui doit être corrigée dans le rapport d'évaluation de votre application.
     - FIS — Indique le nombre de tests recommandés qui doivent être implémentés dans votre application. Choisissez la valeur pour afficher les tests qui doivent être corrigés dans le rapport d'évaluation de votre application.

- Pour consulter le score de chaque composant qui influe sur votre score de résilience, choisissez Répartition du score. Lorsque cette option est sélectionnée, AWS Resilience Hub affiche ce qui suit :
  - Conformité RTO/RPO : indique dans quelle mesure les composants de l'application (AppComponents) sont conformes aux temps de restauration estimés de la charge de travail et aux délais de restauration cibles définis dans la politique de résilience de votre application. Choisissez la valeur pour afficher les estimations du RTO/RPO dans le rapport d'évaluation de votre application.
  - Alarmes mises en œuvre : indique la contribution réelle des CloudWatch alarmes Amazon implémentées par rapport à leur contribution maximale au score de résilience de votre application. Choisissez la valeur pour afficher les CloudWatch alarmes Amazon implémentées dans le rapport d'évaluation de votre application.
  - SOPs implémenté — Indique la contribution réelle de l'implémentation SOPs par rapport à sa contribution maximale au score de résilience de votre application. Choisissez la valeur pour afficher la valeur implémentée SOPs dans le rapport d'évaluation de votre application.
  - Expériences FIS mises en œuvre — Indique la contribution réelle des tests mis en œuvre par rapport à leur contribution maximale au score de résilience de votre application. Choisissez la valeur pour afficher les tests mis en œuvre dans le rapport d'évaluation de votre application.
- Pour consulter les violations des politiques de résilience et les recommandations opérationnelles, cliquez sur la flèche droite pour développer la section sur les violations des politiques et les recommandations opérationnelles. Lorsqu'il est développé, AWS Resilience Hub affiche ce qui suit :
  - Violations de la politique de résilience : indique le nombre de composants de l'application qui enfreignent la politique de résilience de votre application. Choisissez la valeur à côté de RTO/RPO pour afficher les détails dans l'onglet Recommandations de résilience du rapport d'évaluation de votre application.
  - Recommandations opérationnelles : indique les recommandations opérationnelles qui n'ont pas été mises en œuvre ou exécutées pour améliorer la résilience de votre application à l'aide des onglets En suspens et Exclus. Les recommandations opérationnelles incluent toutes les recommandations inactives et celles qui n'ont pas été mises en œuvre.

    Pour consulter les recommandations opérationnelles qui doivent être mises en œuvre, choisissez l'onglet En suspens. Lorsque cette option est sélectionnée, AWS Resilience Hub affiche ce qui suit :

- Alarmes — Indique le nombre d' CloudWatch alarmes Amazon recommandées qui doivent être mises en œuvre.
- SOPs— Indique le nombre de recommandations SOPs qui doivent être mises en œuvre.
- FIS — Indique le nombre de tests recommandés qui doivent être mis en œuvre.

Pour consulter les recommandations opérationnelles exclues de votre application, choisissez l'onglet Exclus. Lorsque cette option est sélectionnée, le message suivant AWS Resilience Hub s'affiche :

- Alarmes — Indique le nombre d' CloudWatch alarmes Amazon recommandées qui sont exclues de votre application.
- SOPs— Indique le nombre de recommandations SOPs exclues de votre application.
- FIS — Indique le nombre de tests recommandés qui sont exclus de votre application.

Calcul des scores de résilience

Les tableaux de cette section expliquent les formules utilisées AWS Resilience Hub pour déterminer les composantes de notation de chaque type de recommandation et le score de résilience de votre application. Toutes les valeurs résultantes déterminées par les composantes AWS Resilience Hub de notation de chaque type de recommandation et le score de résilience de votre application sont arrondies au point le plus proche. Par exemple, si deux alarmes sur trois étaient mises en œuvre, le score serait de 13,33 ((2/3) * 20) points. Cette valeur sera arrondie à 13 points. Pour plus d'informations sur les poids utilisés dans les formules des tableaux, voir the section called "Poids AppComponents et types de perturbations" la section.

Certains éléments de notation ne peuvent être obtenus que par le biais de l'`ScoringComponentResiliencyScore`API. Pour plus d'informations sur cette API, consultez ScoringComponentResiliencyScore.

Tables

- Formules pour calculer la composante de notation de chaque type de recommandation
- Formule pour calculer le score de résilience
- Formules pour calculer le score de résilience AppComponents et les types de perturbations

Le tableau suivant explique les formules utilisées AWS Resilience Hub pour calculer la composante de notation de chaque type de recommandation.

Formules pour calculer la composante de notation de chaque type de recommandation

Composante de notation	Description	Formule	exemple
Couverture des tests (T)	Un score normalisé (0 à 100 points) basé sur le nombre de tests mis en œuvre avec succès et exclus, sur le nombre total de tests AWS Resilience Hub recommandés. **Note** Pour calculer le score de résilience, les tests recommandés doivent avoir été exécutés avec succès au cours des 30 derniers jours AWS Resilience Hub pour qu'il soit considéré comme mis en œuvre.	`T = ((Total number of tests implemented) + (Total number of tests excluded)) / (Total number of tests recommended)` Les éléments de la formule sont les suivants : • Nombre total de tests configurés : indique le nombre total de tests configurés lorsque le AWS CloudFormation modèle est créé et téléchargé dans la AWS CloudFormation console. • Nombre total de tests recommandés : indique les tests recommandés en AWS Resilience Hub fonction des ressources de l'application. • Nombre total de tests exclus : indique le nombre de tests recommandés que vous avez exclus de l'application.	Si vous avez mis en œuvre 10 tests et exclu 5 tests sur les 20 tests AWS Resilience Hub recommandés, la couverture des tests est calculée comme suit : `T = (10 + 5) / 20` C'est-à-dire, `T = .75 or 75 points`

Composante de notation	Description	Formule	exemple
Couverture des alarmes (A)	Un score normalisé (0 à 100 points) basé sur le nombre d' CloudWatch alarmes Amazon correctement implémentées et exclues, sur le nombre total d'alarmes AWS Resilience Hub Amazon CloudWatch recommandées. **Note** Pour calculer le score de résilience, les alarmes recommandées doivent être à l'état Prêt AWS Resilience Hub pour être considérées comme implémentées.	`A = ((Total number of alarms implemented) + (Total number of alarms excluded)) / (Total number of alarms recommended)` Les éléments de la formule sont les suivants : • Nombre total d'alarmes configurées : indique le nombre total d' CloudWatch alarmes Amazon configurées lorsque le AWS CloudFormation modèle est créé et chargé dans la AWS CloudFormation console. • Nombre total d'alarmes recommandées : indique les CloudWatch alarmes Amazon recommandées en AWS Resilience Hub fonction des ressources de l'application. • Nombre total d'alarmes exclues : indique le nombre d' CloudWatch alarmes Amazon recommandées que	Si vous avez implémenté 10 CloudWatch alarmes Amazon et en avez exclu 5 sur les 20 CloudWatch alarmes Amazon AWS Resilience Hub recommandées, la couverture des CloudWatch alarmes Amazon est calculée comme suit : `A = (10 + 5) / 20` C'est-à-dire, `A = .75 or 75 points`

Composante de notation	Description	Formule	exemple
		vous avez exclues de l'application.	

Composante de notation	Description	Formule	exemple
Couverture SOP () `S`	Un score normalisé (0 à 100 points) basé sur le nombre de ceux SOPs qui ont été mis en œuvre avec succès et exclus, sur le nombre total de points recommandés. AWS Resilience Hub SOPs	`S = ((Total number of SOPs implemented) + (Total number of SOPs excluded)) / (Total number of SOPs recommended)` Les éléments de la formule sont les suivants : • Nombre total de SOPs configurations : indique le nombre total de SOPs configurations lorsque le AWS CloudFormation modèle est créé et téléchargé dans la AWS CloudFormation console. • Nombre total de SOPs recommandations : indique le par SOPs recommandé en AWS Resilience Hub fonction des ressources de l'application. • Nombre total de personnes SOPs exclues — Indique le nombre de personnes recommandées SOPs	Si vous en avez mis en œuvre 10 et SOPs exclu 5 des 20 AWS Resilience Hub recommandés SOPs, la couverture SOP est calculée comme suit : `S = (10 + 5) / 20` C'est-à-dire, `S = .75 or 75 points`

Composante de notation	Description	Formule	exemple
		que vous avez exclues de l'application.	

Composante de notation	Description	Formule	exemple
Conformité RTO/RPO () P	Un score normalisé (0 à 100 points) basé sur le respect par l'application de sa politique de résilience.	`P = Total weights of disruption types meeting the application's resiliency policy / Total weights of all disruption types .`	Si la politique de résilience de votre application répond uniquement aux types de zone de disponibilité (AZ) et de perturbat ion de l'infrast ructure, le score de la politique de résilience (P) est calculé comme suit : • Si vous avez défini des objectifs de RTO et de RPO régionaux, P il est calculé comme suit : `P = (20 + 30)/ 100` C'est-à-dire, P `= .5 or 50 points` • Si vous n'avez pas défini d'objectifs de RTO et de RPO régionaux, P

Composante de notation	Description	Formule	exemple
			il est calculé comme suit : `P = (22.22 + 33.33)/ 99.9` C'est-à-dire, `P = .55 or 55 points`

Le tableau suivant explique la formule utilisée pour AWS Resilience Hub calculer le score de résilience pour l'ensemble de votre application.

Formule pour calculer le score de résilience

Composante de notation	Description	Formule	exemple

Score de résilience de l'application () `RS`	Un score de résilience normalisé (0 à 100 points) basé sur le respect par votre application de sa politique de résilience. Le score de résilienc e par application est la moyenne pondérée de tous les types de recommand ations. C'est-à-dire : `RS = Weighted Average (T, A, S, P)`	Le score de résilience par application est calculé à l'aide de la formule suivante : `RS = (T * Weight(T) +`
		`A * Weight(A) +`
		`S * Weight(S) +`
		`P * Weight(P)) /`
		`(Weight(T) + Weight(A) + Weight(S) + Weight(P))`
			Les formules permettant de calculer la couverture de chaque tableau de type de recommandation sont les suivantes :
			• `Test coverage (T) = .75`
			• `Alarms (A) = .75`
			• `SOPs (S) = .75`
			• `Meeting resiliency`

Composante de notation	Description	Formule	exemple

			`policy (P) = .5`
			
			Le score de résilience par application est calculé comme suit :
			
			`RS = ((.75 * .2) + (.75 * .2) + (.75 * .2) + (.5 * .4)) /(.2 + .2 + .2 + .4)`
			
			C'est-à-dire, `RS = .65 or 65 points`

Le tableau suivant explique les formules utilisées pour AWS Resilience Hub calculer le score de résilience pour les composants d'application (AppComponents) et les types de perturbations. Toutefois, vous pouvez obtenir le score de résilience AppComponents et les types de perturbations uniquement via le AWS Resilience Hub APIs suivant :

- DescribeAppAssessmentpour obtenir `RSo`
- ListAppComponentCompliancespour obtenir `RSao` et `RSA`

Formules pour calculer le score de résilience AppComponents et les types de perturbations

Composante de notation	Description	Formule	exemple

Score de résilience par AppComponent et par type de perturbation () `RSao`	Un score normalisé (0 à 100 points) basé sur le AppComponent respect de sa politique de résilience par type de perturbation. Le score de résilience par AppComponent et par type de perturbation est la moyenne pondérée de tous les types de recommandations.
	
	C'est-à-dire : `RSao = Weighted Average (T, A, S, P)`
	
	Les valeurs pour `T, A, S, P` sont calculées pour tous les tests SOPs, alarmes
		Le score de résilience par type AppComponent de perturbation est calculé à l'aide de la formule suivante :
		
		`RSao = (T * Weight(T) +`
		
		`A * Weight(A) +`
		
		`S * Weight(S) +`
		
		`P * Weight(P)) /`
		
		`(Weight(T) + Weight(A) + Weight(S) + Weight(P))`
			`RSao`les hypothèses pour tous les types de recommandations sont les suivantes :
			
			• `Test coverage (T) = .75`
			• `Alarms (A) = .75`
			• `SOPs (S) = .75`
			• `Meeting resiliency policy (P) = .5`
			
			Le score de résilience par type AppComponent de perturbation est calculé comme suit :
			
			`RSao = ((.75 * .2) + (.75 * .2) + (.75 * .2) + (.5 * .4)) / (.2 + .2 + .2 + .4)`
			
			C'est-à-dire, `RSao = .65 or 65 points`

Composante de notation	Description	Formule	exemple
	et politiques de résilience recommandés du AppComponent type de perturbation.		

Composante de notation	Description	Formule	exemple

Score de résilience par AppComponent () `RSa`	Un score normalisé (0 à 100 points) basé sur le respect de sa politique de résilience. Le score de résilience per AppComponent est la moyenne pondérée de tous les types de recommandations. C'est-à-dire : `RSa = Weighted Average (T, A, S, P)`
	
	Les valeurs pour `T, A, S, P` sont calculées pour tous les tests recommandés, les alarmes et la politique de résilience du AppComponent. SOPs
		Le score de résilience par AppComponent est calculé à l'aide de la formule suivante :
		
		`RSa = (T * Weight(T) +`
		
		`A * Weight(A) +`
		
		`S * Weight(S) +`
		
		`P * Weight(P)) /`
		
		`(Weight(T) + Weight(A) + Weight(S) + Weight(P))`
			`RSa`les hypothèses pour tous les types de recommandations sont les suivantes :
			
			• `Test coverage (T) = .75`
			• `Alarms (A) = .75`
			• `SOPs (S) = .75`
			• `Meeting resiliency policy (P) = .5`
			
			Le score de résilience par AppComponent est calculé comme suit :
			
			`RSa = ((.75 * .2) + (.75 * .2) + (.75 * .2) + (.5 * .4)) / (.2 + .2 + .2 + .4)`
			
			C'est-à-dire, `RSa = .65 or 65 points`

Composante de notation	Description	Formule	exemple

Score de résilience par type de perturbation () `RSo`	Un score normalisé (0 à 100 points) basé sur le respect de sa politique de résilience. Le score de résilience par type de perturbation est la moyenne pondérée de tous les types de recommandations. C'est-à-dire : `RSo = Weighted Average (T, A, S, P)`
	
	Les valeurs pour `T, A, S, P` sont calculées pour tous les tests SOPs, alarmes et politiques de résilience recommandés du type d'interruption.
		Le score de résilience par type de perturbation est calculé à l'aide de la formule suivante :
		
		`RSo = (T * Weight(T) + A * Weight(A) +`
		
		`S * Weight(S) + P * Weight(P)) /`
		
		`(Weight(T) + Weight(A) + Weight(S) + Weight(P))`
			`RSo`les hypothèses pour tous les types de recommandations sont les suivantes :
			
			• `Test coverage (T) = .75`
			• `Alarms (A) = .75`
			• `SOPs (S) = .75`
			• `Meeting resiliency policy (P) = .5`
			
			Le score de résilience par type de perturbation est calculé comme suit :
			
			`RSo = ((.75 * .2) + (.75 * .2) + (.75 * .2) + (.5 *.4)) /`
			
			`(.2 + .2 + .2 + .4)`
			
			C'est-à-dire, `RSo = .65 or 65 points`

Poids

AWS Resilience Hub attribue une pondération à chaque type de recommandation pour le score de résilience total.

Les tableaux suivants indiquent le poids des alarmes, des tests SOPs, du respect de la politique de résilience et des types de perturbations. Les types de perturbations incluent l'application, l'infrastructure, l'AZ et la région.

> **Note**
>
> Si vous choisissez de ne pas définir d'objectifs RTO ou RPO régionaux pour votre politique, les pondérations pour les autres types de perturbations sont augmentées en conséquence, comme indiqué dans la colonne Poids lorsque la région n'est pas définie.

Pondérations pour les alarmes SOPs, les tests et les objectifs de politique

Type de recommandation	Weight
Alertes	20 points
SOPs	20 points
Tests	20 points
Respect de la politique de résilience	40 points

Pondérations par type de perturbation

Type de perturbation	Poids lorsque la région est définie	Poids lorsque la région n'est pas définie
Application	40 points	44,44 points
Infrastructure	30 points	33,33 points
Zone de disponibilité	20 points	22,22 points
Région	10 points	N/A

Intégrer des recommandations opérationnelles dans votre application avec AWS CloudFormation

Après avoir choisi Créer un CloudFormation modèle sur la page des recommandations opérationnelles, vous AWS Resilience Hub créez un AWS CloudFormation modèle qui décrit l'alarme, la procédure opérationnelle standard (SOP) ou l' AWS FIS expérience spécifique pour votre application. Le AWS CloudFormation modèle est stocké dans un compartiment Amazon S3, et vous pouvez vérifier le chemin S3 vers le modèle dans l'onglet Détails du modèle sur la page des recommandations opérationnelles.

Par exemple, la liste ci-dessous montre un AWS CloudFormation modèle au format JSON qui décrit une recommandation d'alarme émise par. AWS Resilience Hub Il s'agit d'une alarme de limitation de lecture pour une table DynamoDB appelée. `Employees`

La `Resources` section du modèle décrit l'`AWS::CloudWatch::Alarm`alarme qui est activée lorsque le nombre d'événements de limitation de lecture pour la table DynamoDB dépasse 1. Et les deux `AWS::SSM::Parameter` ressources définissent des métadonnées qui permettent AWS Resilience Hub d'identifier les ressources installées sans avoir à scanner l'application elle-même.

```
{
  "AWSTemplateFormatVersion" : "2010-09-09",
  "Parameters" : {
    "SNSTopicARN" : {
      "Type" : "String",
      "Description" : "The ARN of the Amazon SNS topic to which alarm status changes
 are to be sent. This must be in the same Region being deployed.",
      "AllowedPattern" : "^arn:(aws|aws-cn|aws-iso|aws-iso-[a-z]{1}|aws-us-gov):sns:
([a-z]{2}-((iso[a-z]{0,1}-)|(gov-)){0,1}[a-z]+-[0-9]):[0-9]{12}:[A-Za-z0-9/][A-Za-
z0-9:_/+=,@.-]{1,256}$"
    }
  },
  "Resources" : {

 "ReadthrottleeventsthresholdexceededEmployeesONDEMAND0DynamoDBTablePXBZQYH3DCJ9Alarm" :
 {
      "Type" : "AWS::CloudWatch::Alarm",
      "Properties" : {
        "AlarmDescription" : "An Alarm by AWS Resilience Hub that alerts when the
 number of read-throttle events are greater than 1.",
        "AlarmName" : "ResilienceHub-ReadThrottleEventsAlarm-2020-04-01_Employees-ON-
DEMAND-0-DynamoDBTable-PXBZQYH3DCJ9",
```

```
        "AlarmActions" : [ {
          "Ref" : "SNSTopicARN"
        } ],
        "MetricName" : "ReadThrottleEvents",
        "Namespace" : "AWS/DynamoDB",
        "Statistic" : "Sum",
        "Dimensions" : [ {
          "Name" : "TableName",
          "Value" : "Employees-ON-DEMAND-0-DynamoDBTable-PXBZQYH3DCJ9"
        } ],
        "Period" : 60,
        "EvaluationPeriods" : 1,
        "DatapointsToAlarm" : 1,
        "Threshold" : 1,
        "ComparisonOperator" : "GreaterThanOrEqualToThreshold",
        "TreatMissingData" : "notBreaching",
        "Unit" : "Count"
      },
      "Metadata" : {
        "AWS::ResilienceHub::Monitoring" : {
          "recommendationId" : "dynamodb:alarm:health-read_throttle_events:2020-04-01"
        }
      }
    },

 "dynamodbalarmhealthreadthrottleevents20200401EmployeesONDEMAND0DynamoDBTablePXBZQYH3DCJ9Alarm
 {
      "Type" : "AWS::SSM::Parameter",
      "Properties" : {
        "Name" : "/ResilienceHub/Alarm/3f904525-4bfa-430f-96ef-58ec9b19aa73/dynamodb-
alarm-health-read-throttle-events-2020-04-01_Employees-ON-DEMAND-0-DynamoDBTable-
PXBZQYH3DCJ9",
        "Type" : "String",
        "Value" : {
          "Fn::Sub" :
 "${ReadthrottleeventsthresholdexceededEmployeesONDEMAND0DynamoDBTablePXBZQYH3DCJ9Alarm}"
        },
        "Description" : "SSM Parameter for identifying installed resources."
      }
    },

 "dynamodbalarmhealthreadthrottleevents20200401EmployeesONDEMAND0DynamoDBTablePXBZQYH3DCJ9Alarm
 {
      "Type" : "AWS::SSM::Parameter",
```

```
      "Properties" : {
        "Name" : "/ResilienceHub/Info/Alarm/3f904525-4bfa-430f-96ef-58ec9b19aa73/
dynamodb-alarm-health-read-throttle-events-2020-04-01_Employees-ON-DEMAND-0-
DynamoDBTable-PXBZQYH3DCJ9",
        "Type" : "String",
        "Value" : {
          "Fn::Sub" : "{\"alarmName\":
\"${ReadthrottleeventsthresholdexceededEmployeesONDEMAND0DynamoDBTablePXBZQYH3DCJ9Alarm}\",
\"referenceId\":\"dynamodb:alarm:health_read_throttle_events:2020-04-01\",
\"resourceId\":\"Employees-ON-DEMAND-0-DynamoDBTable-PXBZQYH3DCJ9\",\"relatedSOPs\":
[\"dynamodb:sop:update_provisioned_capacity:2020-04-01\"]}"
        },
        "Description" : "SSM Parameter for identifying installed resources."
      }
    }
  }
}
```

Modifier le AWS CloudFormation modèle

Le moyen le plus simple d'intégrer une alarme, un SOP ou une AWS FIS ressource dans votre application principale consiste simplement à l'ajouter en tant que ressource supplémentaire dans le modèle qui décrit votre modèle d'application. Le fichier au format JSON fourni ci-dessous fournit un aperçu de base de la façon dont une table DynamoDB est décrite dans un modèle. AWS CloudFormation Une véritable application est susceptible d'inclure plusieurs ressources supplémentaires, telles que des tables supplémentaires.

```
{
   "AWSTemplateFormatVersion": "2010-09-09T00:00:00.000Z",
   "Description": "Application Stack with Employees Table",
   "Outputs": {
      "DynamoDBTable": {
         "Description": "The DynamoDB Table Name",
         "Value": {"Ref": "Employees"}
      }
   },
   "Resources": {
      "Employees": {
         "Type": "AWS::DynamoDB::Table",
         "Properties": {
            "BillingMode": "PAY_PER_REQUEST",
            "AttributeDefinitions": [
```

```
            {
               "AttributeName": "USER_ID",
               "AttributeType": "S"
            },
            {
               "AttributeName": "RANGE_ATTRIBUTE",
               "AttributeType": "S"
            }
         ],
         "KeySchema": [
            {
               "AttributeName": "USER_ID",
               "KeyType": "HASH"
            },
            {
               "AttributeName": "RANGE_ATTRIBUTE",
               "KeyType": "RANGE"
            }
         ],
         "PointInTimeRecoverySpecification": {
            "PointInTimeRecoveryEnabled": true
         },
         "Tags": [
            {
               "Key": "Key",
               "Value": "Value"
            }
         ],
         "LocalSecondaryIndexes": [
            {
               "IndexName": "resiliencehub-index-local-1",
               "KeySchema": [
                  {
                     "AttributeName": "USER_ID",
                     "KeyType": "HASH"
                  },
                  {
                     "AttributeName": "RANGE_ATTRIBUTE",
                     "KeyType": "RANGE"
                  }
               ],
               "Projection": {
                  "ProjectionType": "ALL"
               }
```

```
                }
            ],
            "GlobalSecondaryIndexes": [
                {
                    "IndexName": "resiliencehub-index-1",
                    "KeySchema": [
                        {
                            "AttributeName": "USER_ID",
                            "KeyType": "HASH"
                        }
                    ],
                    "Projection": {
                        "ProjectionType": "ALL"
                    }
                }
            ]
        }
    }
  }
}
```

Pour permettre le déploiement de la ressource d'alarme avec votre application, vous devez à présent remplacer les ressources codées en dur par une référence dynamique dans les piles d'applications.

Ainsi, dans la définition de la `AWS::CloudWatch::Alarm` ressource, modifiez les éléments suivants :

```
"Value" : "Employees-ON-DEMAND-0-DynamoDBTable-PXBZQYH3DCJ9"
```

à ce qui suit :

```
"Value" : {"Ref": "Employees"}
```

Et dans la définition de la `AWS::SSM::Parameter` ressource, modifiez ce qui suit :

```
"Fn::Sub" : "{\"alarmName\":
\"${ReadthrottleeventsthresholdexceededDynamoDBEmployeesONDEMAND0DynamoDBTablePXBZQYH3DCJ9Alarm
\"referenceId\":\"dynamodb:alarm:health_read_throttle_events:2020-04-01\",
\"resourceId\":\"Employees-ON-DEMAND-0-DynamoDBTable-PXBZQYH3DCJ9\",\"relatedSOPs\":
[\"dynamodb:sop:update_provisioned_capacity:2020-04-01\"]}"
```

à ce qui suit :

```
"Fn::Sub" : "{\"alarmName\":
\"${ReadthrottleeventsthresholdexceededEmployeesONDEMAND0DynamoDBTablePXBZQYH3DCJ9Alarm}\",
\"referenceId\":\"dynamodb:alarm:health_read_throttle_events:2020-04-01\",\"resourceId
\":\"${Employees}\",\"relatedSOPs\":
[\"dynamodb:sop:update_provisioned_capacity:2020-04-01\"]}"
```

Lorsque vous modifiez des AWS CloudFormation modèles SOPs et AWS FIS des expériences, vous adopterez la même approche, en remplaçant les références codées en dur par IDs des références dynamiques qui continuent de fonctionner même après des modifications matérielles.

En utilisant une référence à la table DynamoDB, vous AWS CloudFormation autorisez les opérations suivantes :

- Créez d'abord la table de base de données.
- Utilisez toujours l'identifiant réel de la ressource générée dans l'alarme et mettez à jour l'alarme de manière dynamique s'il est AWS CloudFormation nécessaire de remplacer la ressource.

> **Note**
>
> Vous pouvez choisir des méthodes plus avancées pour gérer les ressources de votre application, par AWS CloudFormation exemple en imbriquant des piles ou en faisant référence aux sorties de ressources dans une pile séparée AWS CloudFormation. (Mais si vous souhaitez séparer la pile de recommandations de la pile principale, vous devez configurer un moyen de transmettre les informations entre les deux piles.)
> En outre, des outils tiers, tels que Terraform by HashiCorp, peuvent également être utilisés pour provisionner l'infrastructure en tant que code (IaC).

Utilisation AWS Resilience Hub APIs pour décrire et gérer une application

Comme alternative à la description et à la gestion des applications à l'aide de AWS Resilience Hub la console, vous AWS Resilience Hub permet de décrire et de gérer les applications à l'aide de AWS Resilience Hub APIs. Ce chapitre explique comment créer une application à l'aide de AWS Resilience Hub APIs. Il définit également la séquence dans laquelle vous devez exécuter APIs et les valeurs des paramètres que vous devez fournir avec des exemples appropriés. Pour plus d'informations, consultez les rubriques suivantes :

- the section called "Préparation de la demande"
- the section called "Exécution et analyse de l'application"
- the section called "Modifiez votre candidature"

Préparation de la demande

Pour préparer une application, vous devez d'abord créer une application, attribuer une politique de résilience, puis importer les ressources de l'application à partir de vos sources d'entrée. Pour plus d'informations sur AWS Resilience Hub APIs les outils utilisés pour préparer une application, consultez les rubriques suivantes :

- the section called "Création d'une application"
- the section called "Création d'une politique de résilience"
- the section called "Importer les ressources de l'application et surveiller l'état de l'importation"
- the section called "Publiez votre application et attribuez une politique de résilience"

Création d'une application

Pour créer une nouvelle application dans AWS Resilience Hub, vous devez appeler l'`CreateApp`API et fournir un nom d'application unique. Pour plus d'informations sur cette API, consultez https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_CreateApp.html.

L'exemple suivant montre comment créer une nouvelle application `newApp` à l' AWS Resilience Hub aide de l'`CreateApp`API.

Demande

```
aws resiliencehub create-app --name newApp
```

Réponse

```
{
    "app": {
        "appArn": "<App_ARN>",
        "name": "newApp",
        "creationTime": "2022-10-26T19:48:00.434000+03:00",
        "status": "Active",
        "complianceStatus": "NotAssessed",
        "resiliencyScore": 0.0,
        "tags": {},
        "assessmentSchedule": "Disabled"
    }
}
```

Création d'une politique de résilience

Après avoir créé l'application, vous devez créer une politique de résilience qui vous permet de comprendre la posture de résilience de votre application à l'aide `CreateResiliencyPolicy` de l'API. Pour plus d'informations sur cette API, consultez https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_CreateResiliencyPolicy.html.

L'exemple suivant montre comment créer `newPolicy` pour votre application à l' AWS Resilience Hub aide de l'`CreateResiliencyPolicy`API.

Demande

```
aws resiliencehub create-resiliency-policy \
--policy-name newPolicy --tier NonCritical \
--policy '{"AZ": {"rtoInSecs": 172800,"rpoInSecs": 86400}, \
"Hardware": {"rtoInSecs": 172800,"rpoInSecs": 86400}, \
"Software": {"rtoInSecs": 172800,"rpoInSecs": 86400}}'
```

Réponse

```
{
    "policy": {
```

```
        "policyArn": "<Policy_ARN>",
        "policyName": "newPolicy",
        "policyDescription": "",
        "dataLocationConstraint": "AnyLocation",
        "tier": "NonCritical",
        "estimatedCostTier": "L1",
        "policy": {
            "AZ": {
                "rtoInSecs": 172800,
                "rpoInSecs": 86400
            },
            "Hardware": {
                "rtoInSecs": 172800,
                "rpoInSecs": 86400
            },
            "Software": {
                "rtoInSecs": 172800,
                "rpoInSecs": 86400
            }
        },
        "creationTime": "2022-10-26T20:48:05.946000+03:00",
        "tags": {}
    }
}
```

Importation de ressources depuis une source d'entrée et surveillance de l'état de l'importation

AWS Resilience Hub fournit les éléments suivants APIs pour importer des ressources dans votre application :

- `ImportResourcesToDraftAppVersion`— Cette API vous permet d'importer des ressources vers la version préliminaire de votre application à partir de différentes sources d'entrée. Pour plus d'informations sur cette API, consultez https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_ImportResourcesToDraftAppVersion.html.
- `PublishAppVersion`— Cette API publie une nouvelle version de l'application en même temps que la mise à jour AppComponents. Pour plus d'informations sur cette API, consultez https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_PublishAppVersion.html.
- `DescribeDraftAppVersionResourcesImportStatus`— Cette API vous permet de surveiller le statut d'importation de vos ressources vers une version de l'application. Pour plus d'informations

sur cette API, consultez https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_DescribeDraftAppVersionResourcesImportStatus.html.

L'exemple suivant montre comment importer des ressources dans votre application à l' AWS Resilience Hub aide de l'`ImportResourcesToDraftAppVersion`API.

Demande

```
aws resiliencehub import-resources-to-draft-app-version \
--app-arn <App_ARN> \
--terraform-sources '[{"s3StateFileUrl": <S3_URI>}]'
```

Réponse

```
{
    "appArn": "<App_ARN>",
    "appVersion": "draft",
    "sourceArns": [],
    "status": "Pending",
    "terraformSources": [
        {
            "s3StateFileUrl": <S3_URI>
        }
    ]
}
```

L'exemple suivant montre comment ajouter manuellement des ressources à votre application à l' AWS Resilience Hub aide de l'`CreateAppVersionResource`API.

Demande

```
aws resiliencehub create-app-version-resource \
--app-arn <App_ARN> \
--resource-name "backup-efs" \
--logical-resource-id '{"identifier": "backup-efs"}' \
--physical-resource-id '<Physical_resource_id_ARN>' \
--resource-type AWS::EFS::FileSystem \
--app-components '["new-app-component"]'
```

Réponse

```
{
    "appArn": "<App_ARN>",
    "appVersion": "draft",
    "physicalResource": {
        "resourceName": "backup-efs",
        "logicalResourceId": {
            "identifier": "backup-efs"
        },
        "physicalResourceId": {
            "identifier": "<Physical_resource_id_ARN>",
            "type": "Arn"
        },
        "resourceType": "AWS::EFS::FileSystem",
        "appComponents": [
            {
                "name": "new-app-component",
                "type": "AWS::ResilienceHub::StorageAppComponent",
                "id": "new-app-component"
            }
        ]
    }
}
```

L'exemple suivant montre comment surveiller le statut d'importation de vos ressources à AWS Resilience Hub l'aide de l'`DescribeDraftAppVersionResourcesImportStatus`API.

Demande

```
aws resiliencehub describe-draft-app-version-resources-import-status \
--app-arn <App_ARN>
```

Réponse

```
{
    "appArn": "<App_ARN>",
    "appVersion": "draft",
    "status": "Success",
    "statusChangeTime": "2022-10-26T19:55:18.471000+03:00"
}
```

Publication de la version préliminaire de votre application et attribution d'une politique de résilience

Avant d'exécuter une évaluation, vous devez d'abord publier le brouillon de votre application et attribuer une politique de résilience à la version publiée de votre application.

Pour publier le brouillon de votre application et attribuer une politique de résilience

1. Pour publier le brouillon de votre application, utilisez l'`PublishAppVersion`API. Pour plus d'informations sur cette API, consultez https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_PublishAppVersion.html.

   L'exemple suivant montre comment publier le brouillon de l'application à l' AWS Resilience Hub aide de l'`PublishAppVersion`API.

   Demande

   ```
   aws resiliencehub publish-app-version \
    --app-arn <App_ARN>
   ```

   Réponse

   ```
   {
       "appArn": "<App_ARN>",
       "appVersion": "release"
   }
   ```

2. Appliquez une politique de résilience à la version publiée de votre application à l'aide de l'`UpdateApp`API. Pour plus d'informations sur cette API, consultez https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_UpdateApp.html.

   L'exemple suivant montre comment appliquer une politique de résilience à la version publiée d'une application en AWS Resilience Hub utilisant l'`UpdateApp`API.

   Demande

   ```
   aws resiliencehub update-app \
   ```

```
--app-arn <App_ARN> \
--policy-arn <Policy_ARN>
```

Réponse

```
{
    "app": {
        "appArn": "<App_ARN>",
        "name": "newApp",
        "policyArn": "<Policy_ARN>",
        "creationTime": "2022-10-26T19:48:00.434000+03:00",
        "status": "Active",
        "complianceStatus": "NotAssessed",
        "resiliencyScore": 0.0,
        "tags": {
            "resourceArn": "<App_ARN>"
        },
        "assessmentSchedule": "Disabled"
    }
}
```

Exécution et gestion d' AWS Resilience Hub évaluations de résilience

Après avoir publié une nouvelle version de votre application, vous devez exécuter une nouvelle évaluation de la résilience et analyser les résultats pour vous assurer que votre application répond au RTO de charge de travail estimé et au RPO estimés définis dans votre politique de résilience. L'évaluation compare la configuration de chaque composant d'application à la politique et émet des recommandations en matière d'alarme, de procédure opérationnelle normalisée et de test.

Pour plus d'informations, consultez les rubriques suivantes :

- the section called "Exécuter et surveiller une évaluation de la résilience"
- the section called "Création d'une politique de résilience"

Exécution et surveillance des AWS Resilience Hub évaluations de résilience

Pour exécuter des évaluations de résilience AWS Resilience Hub et surveiller leur état, vous devez utiliser les éléments suivants : APIs

- `StartAppAssessment`— Cette API crée une nouvelle évaluation pour une application. Pour plus d'informations sur cette API, consultez https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_StartAppAssessment.html.
- `DescribeAppAssessment`— Cette API décrit une évaluation de l'application et indique l'état d'achèvement de l'évaluation. Pour plus d'informations sur cette API, consultez https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_DescribeAppAssessment.html.

L'exemple suivant montre comment démarrer une nouvelle évaluation à l' AWS Resilience Hub aide de l'`StartAppAssessment`API.

Demande

```
aws resiliencehub start-app-assessment \
--app-arn <App_ARN> \
--app-version release \
--assessment-name first-assessment
```

Réponse

```
{
    "assessment": {
        "appArn": "<App_ARN>",
        "appVersion": "release",
        "invoker": "User",
        "assessmentStatus": "Pending",
        "startTime": "2022-10-27T08:15:10.452000+03:00",
        "assessmentName": "first-assessment",
        "assessmentArn": "<Assessment_ARN>",
        "policy": {
            "policyArn": "<Policy_ARN>",
            "policyName": "newPolicy",
            "dataLocationConstraint": "AnyLocation",
            "policy": {
                "AZ": {
                    "rtoInSecs": 172800,
```

```
                    "rpoInSecs": 86400
                },
                "Hardware": {
                    "rtoInSecs": 172800,
                    "rpoInSecs": 86400
                },
                "Software": {
                    "rtoInSecs": 172800,
                    "rpoInSecs": 86400
                }
            }
        },
        "tags": {}
    }
}
```

L'exemple suivant montre comment surveiller le statut de votre évaluation à l' AWS Resilience Hub aide de l'`DescribeAppAssessment`API. Vous pouvez extraire le statut de votre évaluation à partir de la `assessmentStatus` variable.

Demande

```
aws resiliencehub describe-app-assessment \
--assessment-arn <Assessment_ARN>
```

Réponse

```
{
    "assessment": {
        "appArn": "<App_ARN>",
        "appVersion": "release",
        "cost": {
            "amount": 0.0,
            "currency": "USD",
            "frequency": "Monthly"
        },
        "resiliencyScore": {
            "score": 0.27,
            "disruptionScore": {
                "AZ": 0.42,
                "Hardware": 0.0,
                "Region": 0.0,
```

```
                "Software": 0.38
            }
        },
        "compliance": {
            "AZ": {
                "achievableRtoInSecs": 0,
                "currentRtoInSecs": 4500,
                "currentRpoInSecs": 86400,
                "complianceStatus": "PolicyMet",
                "achievableRpoInSecs": 0
            },
            "Hardware": {
                "achievableRtoInSecs": 0,
                "currentRtoInSecs": 2595601,
                "currentRpoInSecs": 2592001,
                "complianceStatus": "PolicyBreached",
                "achievableRpoInSecs": 0
            },
            "Software": {
                "achievableRtoInSecs": 0,
                "currentRtoInSecs": 4500,
                "currentRpoInSecs": 86400,
                "complianceStatus": "PolicyMet",
                "achievableRpoInSecs": 0
            }
        },
        "complianceStatus": "PolicyBreached",
        "assessmentStatus": "Success",
        "startTime": "2022-10-27T08:15:10.452000+03:00",
        "endTime": "2022-10-27T08:15:31.883000+03:00",
        "assessmentName": "first-assessment",
        "assessmentArn": "<Assessment_ARN>",
        "policy": {
            "policyArn": "<Policy_ARN>",
            "policyName": "newPolicy",
            "dataLocationConstraint": "AnyLocation",
            "policy": {
                "AZ": {
                    "rtoInSecs": 172800,
                    "rpoInSecs": 86400
                },
                "Hardware": {
                    "rtoInSecs": 172800,
                    "rpoInSecs": 86400
```

```
                },
                "Software": {
                    "rtoInSecs": 172800,
                    "rpoInSecs": 86400
                }
            }
        },
        "tags": {}
    }
}
```

Examen des résultats d'évaluation

Une fois votre évaluation terminée avec succès, vous pouvez examiner les résultats de l'évaluation à l'aide des méthodes suivantes APIs.

- `DescribeAppAssessment`— Cette API vous permet de suivre l'état actuel de votre application par rapport à la politique de résilience. En outre, vous pouvez également extraire l'état de conformité de la `complianceStatus` variable et le score de résilience pour chaque type de perturbation de la `resiliencyScore` structure. Pour plus d'informations sur cette API, consultez https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_DescribeAppAssessment.html.
- `ListAlarmRecommendations`— Cette API vous permet d'obtenir les recommandations d'alarme à l'aide de l'Amazon Resource Name (ARN) de l'évaluation. Pour plus d'informations sur cette API, consultez https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_ListAlarmRecommendations.html.

> **Note**
>
> Pour obtenir les recommandations des tests SOP et FIS, utilisez `ListSopRecommendations` et. `ListTestRecommendations` APIs

L'exemple suivant montre comment obtenir les recommandations d'alarme à l'aide de l'Amazon Resource Name (ARN) de l'évaluation à l'aide de l'`ListAlarmRecommendations`API.

> **Note**
>
> Pour obtenir les recommandations de test SOP et FIS, remplacez par ou`ListSopRecommendations`. `ListTestRecommendations`

Demande

```
aws resiliencehub list-alarm-recommendations \
--assessment-arn <Assessment_ARN>
```

Réponse

```
{
    "alarmRecommendations": [
        {
            "recommendationId": "78ece7f8-c776-499e-baa8-b35f5e8b8ba2",
            "referenceId": "app_common:alarm:synthetic_canary:2021-04-01",
            "name": "AWSResilienceHub-SyntheticCanaryInRegionAlarm_2021-04-01",
            "description": "A monitor for the entire application, configured to
 constantly verify that the application API/endpoints are available",
            "type": "Metric",
            "appComponentName": "appcommon",
            "items": [
                {
                    "resourceId": "us-west-2",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ],
            "prerequisite": "Make sure Amazon CloudWatch Synthetics is setup to monitor
 the application (see the <a href=\"https://docs.aws.amazon.com/AmazonCloudWatch/
latest/monitoring/CloudWatch_Synthetics_Canaries.html\" target=\"_blank\">docs</a>).
 \nMake sure that the Synthetics Name passed in the alarm dimension matches the name of
 the Synthetic Canary. It Defaults to the name of the application.\n"
        },
        {
            "recommendationId": "d9c72c58-8c00-43f0-ad5d-0c6e5332b84b",
            "referenceId": "efs:alarm:percent_io_limit:2020-04-01",
            "name": "AWSResilienceHub-EFSHighIoAlarm_2020-04-01",
```

```
            "description": "An alarm by AWS Resilience Hub that reports when Amazon EFS
 I/O load is more than 90% for too much time",
            "type": "Metric",
            "appComponentName": "storageappcomponent-rlb",
            "items": [
                {
                    "resourceId": "fs-0487f945c02f17b3e",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ]
        },
        {
            "recommendationId": "09f340cd-3427-4f66-8923-7f289d4a3216",
            "referenceId": "efs:alarm:mount_failure:2020-04-01",
            "name": "AWSResilienceHub-EFSMountFailureAlarm_2020-04-01",
            "description": "An alarm by AWS Resilience Hub that reports when volume
 failed to mount to EC2 instance",
            "type": "Metric",
            "appComponentName": "storageappcomponent-rlb",
            "items": [
                {
                    "resourceId": "fs-0487f945c02f17b3e",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ],
            "prerequisite": "* Make sure Amazon EFS utils are installed(see the <a
 href=\"https://github.com/aws/efs-utils#installation\" target=\"_blank\">docs</a>).
\n* Make sure cloudwatch logs are enabled in efs-utils (see the <a href=\"https://
github.com/aws/efs-utils#step-2-enable-cloudwatch-log-feature-in-efs-utils-config-
file-etcamazonefsefs-utilsconf\" target=\"_blank\">docs</a>).\n* Make sure that
 you've configured `log_group_name` in `/etc/amazon/efs/efs-utils.conf`, for example:
 `log_group_name = /aws/efs/utils`.\n* Use the created `log_group_name` in the
 generated alarm. Find `LogGroupName: REPLACE_ME` in the alarm and make sure the
 `log_group_name` is used instead of REPLACE_ME.\n"
        },
        {
            "recommendationId": "b0f57d2a-1220-4f40-a585-6dab1e79cee2",
            "referenceId": "efs:alarm:client_connections:2020-04-01",
            "name": "AWSResilienceHub-EFSHighClientConnectionsAlarm_2020-04-01",
```

```
            "description": "An alarm by AWS Resilience Hub that reports when client
 connection number deviation is over the specified threshold",
            "type": "Metric",
            "appComponentName": "storageappcomponent-rlb",
            "items": [
                {
                    "resourceId": "fs-0487f945c02f17b3e",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ]
        },
        {
            "recommendationId": "15f49b10-9bac-4494-b376-705f8da252d7",
            "referenceId": "rds:alarm:health-storage:2020-04-01",
            "name": "AWSResilienceHub-RDSInstanceLowStorageAlarm_2020-04-01",
            "description": "Reports when database free storage is low",
            "type": "Metric",
            "appComponentName": "databaseappcomponent-hji",
            "items": [
                {
                    "resourceId": "terraform-20220623141426115800000001",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ]
        },
        {
            "recommendationId": "c1906101-cea8-4f77-be7b-60abb07621f5",
            "referenceId": "rds:alarm:health-connections:2020-04-01",
            "name": "AWSResilienceHub-RDSInstanceConnectionSpikeAlarm_2020-04-01",
            "description": "Reports when database connection count is anomalous",
            "type": "Metric",
            "appComponentName": "databaseappcomponent-hji",
            "items": [
                {
                    "resourceId": "terraform-20220623141426115800000001",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ]
```

```
        },
        {
            "recommendationId": "f169b8d4-45c1-4238-95d1-ecdd8d5153fe",
            "referenceId": "rds:alarm:health-cpu:2020-04-01",
            "name": "AWSResilienceHub-RDSInstanceOverUtilizedCpuAlarm_2020-04-01",
            "description": "Reports when database used CPU is high",
            "type": "Metric",
            "appComponentName": "databaseappcomponent-hji",
            "items": [
                {
                    "resourceId": "terraform-20220623141426115800000001",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ]
        },
        {
            "recommendationId": "69da8459-cbe4-4ba1-a476-80c7ebf096f0",
            "referenceId": "rds:alarm:health-memory:2020-04-01",
            "name": "AWSResilienceHub-RDSInstanceLowMemoryAlarm_2020-04-01",
            "description": "Reports when database free memory is low",
            "type": "Metric",
            "appComponentName": "databaseappcomponent-hji",
            "items": [
                {
                    "resourceId": "terraform-20220623141426115800000001",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ]
        },
        {
            "recommendationId": "67e7902a-f658-439e-916b-251a57b97c8a",
            "referenceId": "ecs:alarm:health-service_cpu_utilization:2020-04-01",
            "name": "AWSResilienceHub-ECSServiceHighCpuUtilizationAlarm_2020-04-01",
            "description": "An alarm by AWS Resilience Hub that triggers when CPU
 utilization of ECS tasks of Service exceeds the threshold",
            "type": "Metric",
            "appComponentName": "computeappcomponent-nrz",
            "items": [
                {
                    "resourceId": "aws_ecs_service_terraform-us-east-1-demo",
```

```
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ]
        },
        {
            "recommendationId": "fb30cb91-1f09-4abd-bd2e-9e8ee8550eb0",
            "referenceId": "ecs:alarm:health-service_memory_utilization:2020-04-01",
            "name": "AWSResilienceHub-ECSServiceHighMemoryUtilizationAlarm_2020-04-01",
            "description": "An alarm by AWS Resilience Hub for Amazon ECS that
 indicates if the percentage of memory that is used in the service, is exceeding
 specified threshold limit",
            "type": "Metric",
            "appComponentName": "computeappcomponent-nrz",
            "items": [
                {
                    "resourceId": "aws_ecs_service_terraform-us-east-1-demo",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ]
        },
        {
            "recommendationId": "1bd45a8e-dd58-4a8e-a628-bdbee234efed",
            "referenceId": "ecs:alarm:health-service_sample_count:2020-04-01",
            "name": "AWSResilienceHub-ECSServiceSampleCountAlarm_2020-04-01",
            "description": "An alarm by AWS Resilience Hub for Amazon ECS that triggers
 if the count of tasks isn't equal Service Desired Count",
            "type": "Metric",
            "appComponentName": "computeappcomponent-nrz",
            "items": [
                {
                    "resourceId": "aws_ecs_service_terraform-us-east-1-demo",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ],
            "prerequisite": "Make sure the Container Insights on Amazon ECS is enabled:
 (see the <a href=\"https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/
deploy-container-insights-ECS-cluster.html\" target=\"_blank\">docs</a>)."
        }
```

```
    ]
}
```

L'exemple suivant montre comment obtenir les recommandations de configuration (recommandations sur la manière d'améliorer votre résilience actuelle) à l'aide de l'`ListAppComponentRecommendations`API.

Demande

```
aws resiliencehub list-app-component-recommendations \
--assessment-arn <Assessment_ARN>
```

Réponse

```
{
    "componentRecommendations": [
        {
            "appComponentName": "computeappcomponent-nrz",
            "recommendationStatus": "MetCanImprove",
            "configRecommendations": [
                {
                    "cost": {
                        "amount": 0.0,
                        "currency": "USD",
                        "frequency": "Monthly"
                },
                    "appComponentName": "computeappcomponent-nrz",
                    "recommendationCompliance": {
                        "AZ": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": " Estimated time to restore
 cluster with volumes. (Estimate is based on averages, real time restore may vary).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Based on the frequency of the
 backups"
                        },
                        "Hardware": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": " Estimated time to restore
 cluster with volumes. (Estimate is based on averages, real time restore may vary).",
```

```
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Based on the frequency of the
backups"
                        },
                        "Software": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": " Estimated time to restore
cluster with volumes. (Estimate is based on averages, real time restore may vary).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Based on the frequency of the
backups"
                        }
                    },
                    "optimizationType": "LeastCost",
                    "description": "Current Configuration",
                    "suggestedChanges": [],
                    "haArchitecture": "BackupAndRestore",
                    "referenceId": "original"
                },
                {
                    "cost": {
                        "amount": 0.0,
                        "currency": "USD",
                        "frequency": "Monthly"
                    },
                    "appComponentName": "computeappcomponent-nrz",
                    "recommendationCompliance": {
                        "AZ": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": " Estimated time to restore
cluster with volumes. (Estimate is based on averages, real time restore may vary).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Based on the frequency of the
backups"
                        },
                        "Hardware": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": " Estimated time to restore
cluster with volumes. (Estimate is based on averages, real time restore may vary).",
                            "expectedRpoInSecs": 86400,
```

```
                            "expectedRpoDescription": "Based on the frequency of the
backups"
                        },
                        "Software": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": " Estimated time to restore
cluster with volumes. (Estimate is based on averages, real time restore may vary).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Based on the frequency of the
backups"
                        }
                    },
                    "optimizationType": "LeastChange",
                    "description": "Current Configuration",
                    "suggestedChanges": [],
                    "haArchitecture": "BackupAndRestore",
                    "referenceId": "original"
                },
                {
                    "cost": {
                        "amount": 14.74,
                        "currency": "USD",
                        "frequency": "Monthly"
                    },
                    "appComponentName": "computeappcomponent-nrz",
                    "recommendationCompliance": {
                        "AZ": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 0,
                            "expectedRtoDescription": "No expected downtime. You're
launching using EC2, with DesiredCount > 1 in multiple AZs and CapacityProviders with
MinSize > 1",
                            "expectedRpoInSecs": 0,
                            "expectedRpoDescription": "ECS Service state is saved on
Amazon EFS file system. No data loss is expected as objects are be stored in multiple
AZs."
                        },
                        "Hardware": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 0,
                            "expectedRtoDescription": "No expected downtime. You're
launching using EC2, with DesiredCount > 1 and CapacityProviders with MinSize > 1",
                            "expectedRpoInSecs": 0,
```

```
                            "expectedRpoDescription": "ECS Service state is saved on
Amazon EFS file system. No data loss is expected as objects are be stored in multiple
AZs."
                        },
                        "Software": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": " Estimated time to restore
cluster with volumes. (Estimate is based on averages, real time restore may vary).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Based on the frequency of the
backups"
                        }
                    },
                    "optimizationType": "BestAZRecovery",
                    "description": "Stateful Amazon ECS service with launch type Amazon
EC2 and Amazon EFS storage, deployed in multiple AZs. AWS Backup is used to backup
Amazon EFS and copy snapshots in-Region.",
                    "suggestedChanges": [
                        "Add AWS Auto Scaling Groups and Capacity Providers in multiple
AZs",
                        "Change desired count of the setup",
                        "Remove Amazon EBS volume"
                    ],
                    "haArchitecture": "BackupAndRestore",
                    "referenceId": "ecs:config:ec2-multi_az-efs-backups:2022-02-16"
                }
            ]
        },
        {
            "appComponentName": "databaseappcomponent-hji",
            "recommendationStatus": "MetCanImprove",
            "configRecommendations": [
                {
                    "cost": {
                        "amount": 0.0,
                        "currency": "USD",
                        "frequency": "Monthly"
                    },
                    "appComponentName": "databaseappcomponent-hji",
                    "recommendationCompliance": {
                        "AZ": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
```

```
                            "expectedRtoDescription": "Estimated time to restore from
an RDS backup. (Estimates are averages based on size, real time may vary greatly from
estimate).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Estimate based on the backup
schedule. (Estimates are calculated from backup schedule, real time restore may
vary)."
                        },
                        "Hardware": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": "Estimated time to restore from
snapshot. (Estimates are averages based on size, real time may vary greatly from
estimate).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Estimate based on the backup
schedule. (Estimates are calculated from backup schedule, real time restore may
vary)."
                        },
                        "Software": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": "Estimated time to restore from
snapshot. (Estimates are averages based on size, real time may vary greatly from
estimate).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Estimate based on the backup
schedule. (Estimates are calculated from backup schedule, real time restore may
vary)."
                        }
                    },
                    "optimizationType": "LeastCost",
                    "description": "Current Configuration",
                    "suggestedChanges": [],
                    "haArchitecture": "BackupAndRestore",
                    "referenceId": "original"
                },
                {
                    "cost": {
                        "amount": 0.0,
                        "currency": "USD",
                        "frequency": "Monthly"
                    },
                    "appComponentName": "databaseappcomponent-hji",
```

```
                    "recommendationCompliance": {
                        "AZ": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": "Estimated time to restore from
an RDS backup. (Estimates are averages based on size, real time may vary greatly from
estimate).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Estimate based on the backup
schedule. (Estimates are calculated from backup schedule, real time restore may
vary)."
                        },
                        "Hardware": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": "Estimated time to restore from
snapshot. (Estimates are averages based on size, real time may vary greatly from
estimate).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Estimate based on the backup
schedule. (Estimates are calculated from backup schedule, real time restore may
vary)."
                        },
                        "Software": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": "Estimated time to restore from
snapshot. (Estimates are averages based on size, real time may vary greatly from
estimate).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Estimate based on the backup
schedule. (Estimates are calculated from backup schedule, real time restore may
vary)."
                        }
                    },
                    "optimizationType": "LeastChange",
                    "description": "Current Configuration",
                    "suggestedChanges": [],
                    "haArchitecture": "BackupAndRestore",
                    "referenceId": "original"
                },
                {
                    "cost": {
                        "amount": 76.73,
```

```
                        "currency": "USD",
                        "frequency": "Monthly"
                    },
                    "appComponentName": "databaseappcomponent-hji",
                    "recommendationCompliance": {
                        "AZ": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 120,
                            "expectedRtoDescription": "Estimated time to promote a
secondary instance.",
                            "expectedRpoInSecs": 0,
                            "expectedRpoDescription": "Aurora data is automatically
replicated across multiple Availability Zones in a Region."
                        },
                        "Hardware": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 120,
                            "expectedRtoDescription": "Estimated time to promote a
secondary instance.",
                            "expectedRpoInSecs": 0,
                            "expectedRpoDescription": "Aurora data is automatically
replicated across multiple Availability Zones in a Region."
                        },
                        "Software": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 900,
                            "expectedRtoDescription": "Estimate time to backtrack to a
stable state.",
                            "expectedRpoInSecs": 300,
                            "expectedRpoDescription": "Estimate for latest restorable
time for point in time recovery."
                        }
                    },
                    "optimizationType": "BestAZRecovery",
                    "description": "Aurora database cluster with one read replica, with
backtracking window of 24 hours.",
                    "suggestedChanges": [
                        "Add read replica in the same Region",
                        "Change DB instance to a supported class (db.t3.small)",
                        "Change to Aurora",
                        "Enable cluster backtracking",
                        "Enable instance backup with retention period 7"
                    ],
                    "haArchitecture": "WarmStandby",
```

```
                    "referenceId": "rds:config:aurora-backtracking"
                }
            ]
        },
        {
            "appComponentName": "storageappcomponent-rlb",
            "recommendationStatus": "BreachedUnattainable",
            "configRecommendations": [
                {
                    "cost": {
                        "amount": 0.0,
                        "currency": "USD",
                        "frequency": "Monthly"
                    },
                    "appComponentName": "storageappcomponent-rlb",
                    "recommendationCompliance": {
                        "AZ": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 0,
                            "expectedRtoDescription": "No data loss in your system",
                            "expectedRpoInSecs": 0,
                            "expectedRpoDescription": "No data loss in your system"
                        },
                        "Hardware": {
                            "expectedComplianceStatus": "PolicyBreached",
                            "expectedRtoInSecs": 2592001,
                            "expectedRtoDescription": "No recovery option configured",
                            "expectedRpoInSecs": 2592001,
                            "expectedRpoDescription": "No recovery option configured"
                        },
                        "Software": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 900,
                            "expectedRtoDescription": "Time to recover Amazon EFS from
backup. (Estimate is based on averages, real time restore may vary).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Recovery Point Objective for
Amazon EFS from backups, derived from backup frequency"
                        }
                    },
                    "optimizationType": "BestAZRecovery",
                    "description": "Amazon EFS with backups configured",
                    "suggestedChanges": [
                        "Add additional availability zone"
```

```
                    ],
                    "haArchitecture": "MultiSite",
                    "referenceId": "efs:config:with_backups:2020-04-01"
                },
                {
                    "cost": {
                        "amount": 0.0,
                        "currency": "USD",
                        "frequency": "Monthly"
                    },
                    "appComponentName": "storageappcomponent-rlb",
                    "recommendationCompliance": {
                        "AZ": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 0,
                            "expectedRtoDescription": "No data loss in your system",
                            "expectedRpoInSecs": 0,
                            "expectedRpoDescription": "No data loss in your system"
                        },
                        "Hardware": {
                            "expectedComplianceStatus": "PolicyBreached",
                            "expectedRtoInSecs": 2592001,
                            "expectedRtoDescription": "No recovery option configured",
                            "expectedRpoInSecs": 2592001,
                            "expectedRpoDescription": "No recovery option configured"
                        },
                        "Software": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 900,
                            "expectedRtoDescription": "Time to recover Amazon EFS from
backup. (Estimate is based on averages, real time restore may vary).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Recovery Point Objective for
Amazon EFS from backups, derived from backup frequency"
                        }
                    },
                    "optimizationType": "BestAttainable",
                    "description": "Amazon EFS with backups configured",
                    "suggestedChanges": [
                        "Add additional availability zone"
                    ],
                    "haArchitecture": "MultiSite",
                    "referenceId": "efs:config:with_backups:2020-04-01"
                }
```

```
            ]
        }
    ]
}
```

Modifier votre application

AWS Resilience Hub vous permet de modifier les ressources de votre application en éditant un brouillon de votre application et en publiant les modifications apportées à une nouvelle version (publiée). AWS Resilience Hub utilise la version publiée de votre application, qui inclut les ressources mises à jour, pour exécuter des évaluations de résilience.

Pour plus d'informations, consultez les rubriques suivantes :

- the section called "Ajouter des ressources manuellement"
- the section called "Regroupement des ressources dans un seul composant d'application"
- the section called "Exclure une ressource d'un AppComponent"

Ajout manuel de ressources à votre application

Si la ressource n'est pas déployée dans le cadre d'une source d'entrée, vous AWS Resilience Hub permet d'ajouter manuellement la ressource à votre application à l'aide de l'`CreateAppVersionResource`API. Pour plus d'informations sur cette API, consultez https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_CreateAppVersionResource.html.

Vous devez fournir les paramètres suivants à cette API :

- Amazon Resource Name (ARN) de l'application
- ID logique de la ressource
- Identifiant physique de la ressource
- AWS CloudFormation type

L'exemple suivant montre comment ajouter manuellement des ressources à votre application à l' AWS Resilience Hub aide de l'`CreateAppVersionResource`API.

Demande

```
aws resiliencehub create-app-version-resource \
--app-arn <App_ARN> \
--resource-name "backup-efs" \
--logical-resource-id '{"identifier": "backup-efs"}' \
--physical-resource-id '<Physical_resource_id_ARN>' \
--resource-type AWS::EFS::FileSystem \
--app-components '["new-app-component"]'
```

Réponse

```
{
    "appArn": "<App_ARN>",
    "appVersion": "draft",
    "physicalResource": {
        "resourceName": "backup-efs",
        "logicalResourceId": {
            "identifier": "backup-efs"
        },
        "physicalResourceId": {
            "identifier": "<Physical_resource_id_ARN>",
            "type": "Arn"
        },
        "resourceType": "AWS::EFS::FileSystem",
        "appComponents": [
            {
                "name": "new-app-component",
                "type": "AWS::ResilienceHub::StorageAppComponent",
                "id": "new-app-component"
            }
        ]
    }
}
```

Regroupement des ressources dans un seul composant d'application

Un composant d'application (AppComponent) est un groupe de AWS ressources connexes qui fonctionnent et échouent en tant qu'unité unique. Par exemple, lorsque vous avez des charges de travail interrégionales utilisées comme déploiements de secours. AWS Resilience Hub dispose de règles régissant quelles AWS ressources peuvent appartenir à quel type de AppComponent. AWS

Resilience Hub vous permet de regrouper les ressources en une seule à AppComponent l'aide de la gestion des ressources suivante APIs.

- `UpdateAppVersionResource`— Cette API met à jour les détails des ressources d'une application. Pour plus d'informations sur cette API, consultez UpdateAppVersionResource.
- `DeleteAppVersionAppComponent`— Cette API les supprime AppComponent de l'application. Pour plus d'informations sur cette API, consultez DeleteAppVersionAppComponent.

L'exemple suivant montre comment mettre à jour les détails des ressources de votre application à l' AWS Resilience Hub aide de l'`DeleteAppVersionAppComponent`API.

Demande

```
aws resiliencehub delete-app-version-app-component \
--app-arn <App_ARN> \
--id new-app-component
```

Réponse

```
{
    "appArn": "<App_ARN>",
    "appVersion": "draft",
    "appComponent": {
        "name": "new-app-component",
        "type": "AWS::ResilienceHub::StorageAppComponent",
        "id": "new-app-component"
    }
}
```

L'exemple suivant montre comment supprimer le vide créé dans AppComponent les exemples précédents à l' AWS Resilience Hub aide de l'`UpdateAppVersionResource`API.

Demande

```
aws resiliencehub delete-app-version-app-component \
--app-arn <App_ARN> \
--id new-app-component
```

Réponse

```
{
    "appArn": "<App_ARN>",
    "appVersion": "draft",
    "appComponent": {
        "name": "new-app-component",
        "type": "AWS::ResilienceHub::StorageAppComponent",
        "id": "new-app-component"
    }
}
```

Exclure une ressource d'un AppComponent

AWS Resilience Hub vous permet d'exclure des ressources des évaluations à l'aide de l'`UpdateAppVersionResource`API. Ces ressources ne seront pas prises en compte lors du calcul de la résilience de votre application. Pour plus d'informations sur cette API, consultez https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_UpdateAppVersionResource.html.

> **Note**
>
> Vous ne pouvez exclure que les ressources importées depuis une source d'entrée.

L'exemple suivant montre comment exclure une ressource de votre application lors de l' AWS Resilience Hub utilisation de l'`UpdateAppVersionResource`API.

Demande

```
aws resiliencehub update-app-version-resource \
--app-arn <App_ARN> \
--resource-name "ec2instance-nvz" \
--excluded
```

Réponse

```
{
    "appArn": "<App_ARN>",
    "appVersion": "draft",
    "physicalResource": {
```

```
        "resourceName": "ec2instance-nvz",
        "logicalResourceId": {
            "identifier": "ec2",
            "terraformSourceName": "test.state.file"
        },
        "physicalResourceId": {
            "identifier": "i-0b58265a694e5ffc1",
            "type": "Native",
            "awsRegion": "us-west-2",
            "awsAccountId": "123456789101"
        },
        "resourceType": "AWS::EC2::Instance",
        "appComponents": [
            {
                "name": "computeappcomponent-nrz",
                "type": "AWS::ResilienceHub::ComputeAppComponent"
            }
        ]
    }
}
```

Sécurité dans AWS Resilience Hub

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez de centres de données et d'architectures réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit cela comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de AWS conformité Programmes de de conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent à AWS Resilience Hub, voir 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 son utilisation AWS Resilience Hub. Les rubriques suivantes expliquent comment procéder à la configuration AWS Resilience Hub pour atteindre 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 AWS Resilience Hub ressources.

Table des matières

- Protection des données dans AWS Resilience Hub
- Identity and Access Management pour AWS Resilience Hub
- Sécurité de l'infrastructure dans AWS Resilience Hub

Protection des données dans AWS Resilience Hub

Le modèle de responsabilité AWS partagée de s'applique à la protection des données dans AWS Resilience Hub. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur

cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez Questions fréquentes (FAQ) sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagée AWS et RGPD (Règlement général sur la protection des données) sur le Blog de sécuritéAWS .

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- Utilisez le protocole SSL/TLS pour communiquer avec les ressources. AWS Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail. 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 Resilience Hub ou autre Services AWS à l'aide de la console AWS CLI, de l'API ou AWS SDKs. 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

AWS Resilience Hub chiffre vos données au repos. Les données entrantes AWS Resilience Hub sont cryptées au repos à l'aide d'un chiffrement transparent côté serveur. Cela réduit la lourdeur opérationnelle et la complexité induites par la protection des données sensibles. Le chiffrement au repos vous permet de créer des applications sensibles en matière de sécurité qui sont conformes aux exigences réglementaires et de chiffrement.

Chiffrement en transit

AWS Resilience Hub chiffre les données en transit entre le service et les autres AWS services intégrés. Toutes les données qui transitent entre AWS Resilience Hub les services intégrés sont cryptées à l'aide du protocole TLS (Transport Layer Security). AWS Resilience Hub fournit des actions préconfigurées pour des types spécifiques de cibles dans l'ensemble des AWS services et prend en charge les actions pour les ressources cibles.

Identity and Access Management pour AWS Resilience Hub

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

Rubriques

- Public ciblé
- Authentification par des identités
- Gestion des accès à l'aide de politiques
- Comment AWS Resilience Hub fonctionne avec IAM
- Configuration des rôles et autorisations IAM
- Résolution des problèmes d'identité et d'accès au AWS Resilience Hub
- AWS Resilience Hub référence des autorisations d'accès
- AWS politiques gérées pour AWS Resilience Hub
- AWS Resilience Hub référence aux personas et aux autorisations IAM
- Importation du fichier d'état Terraform dans AWS Resilience Hub

- Permettre AWS Resilience Hub l'accès à votre cluster Amazon Elastic Kubernetes Service
- Activation AWS Resilience Hub de la publication de sujets sur votre Amazon Simple Notification Service
- Limiter les autorisations pour inclure ou exclure AWS Resilience Hub des recommandations

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez dans AWS Resilience Hub.

Utilisateur du service : si vous utilisez le service AWS Resilience Hub pour effectuer votre travail, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Au fur et à mesure que vous utilisez de plus en plus de fonctionnalités de AWS Resilience Hub pour effectuer votre travail, vous aurez peut-être besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne pouvez pas accéder à une fonctionnalité dans AWS Resilience Hub, consultezRésolution des problèmes d'identité et d'accès au AWS Resilience Hub.

Administrateur du service — Si vous êtes responsable des ressources du AWS Resilience Hub dans votre entreprise, vous avez probablement un accès complet au AWS Resilience Hub. C'est à vous de déterminer les fonctionnalités et les ressources du AWS Resilience Hub auxquelles les utilisateurs de vos services doivent accéder. Vous devez ensuite soumettre les demandes à votre administrateur IAM pour modifier les autorisations des utilisateurs de votre service. Consultez les informations sur cette page pour comprendre les concepts de base d'IAM. Pour en savoir plus sur la manière dont votre entreprise peut utiliser l'IAM avec AWS Resilience Hub, consultezComment AWS Resilience Hub fonctionne avec IAM.

Administrateur IAM — Si vous êtes administrateur IAM, vous souhaiterez peut-être en savoir plus sur la manière dont vous pouvez rédiger des politiques pour gérer l'accès à AWS Resilience Hub. Pour consulter des exemples de politiques basées sur l'identité de AWS Resilience Hub que vous pouvez utiliser dans IAM, consultez. Exemples de politiques basées sur l'identité pour AWS Resilience Hub

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. Vous devez être authentifié (connecté à AWS) en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

Vous pouvez vous connecter en AWS tant qu'identité fédérée en utilisant les informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center Les utilisateurs (IAM Identity Center), l'authentification unique de votre entreprise et vos informations d'identification Google ou Facebook sont des exemples d'identités fédérées. Lorsque vous vous connectez avec une identité fédérée, votre administrateur aura précédemment configuré une fédération d'identités avec des rôles IAM. Lorsque vous accédez à AWS l'aide de la fédération, vous assumez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter au portail AWS Management Console ou au portail AWS d'accès. Pour plus d'informations sur la connexion à AWS, consultez la section Comment vous connecter à votre compte Compte AWS dans le guide de Connexion à AWS l'utilisateur.

Si vous y accédez AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. Si vous n'utilisez pas d' AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer des demandes vous-même, consultez AWS Signature Version 4 pour les demandes d'API dans le Guide de l'utilisateur IAM.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être fournir des informations de sécurité supplémentaires. Par exemple, il vous AWS recommande d'utiliser l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour plus d'informations, consultez Authentification multifactorielle dans le Guide de l'utilisateur AWS IAM Identity Center et Authentification multifactorielle AWS dans IAM dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes Services AWS les ressources du compte. Cette identité est appelée utilisateur Compte AWS root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent de vous connecter en tant qu'utilisateur racine, consultez Tâches nécessitant des informations d'identification d'utilisateur racine dans le Guide de l'utilisateur IAM.

Identité fédérée

La meilleure pratique consiste à obliger les utilisateurs humains, y compris ceux qui ont besoin d'un accès administrateur, à utiliser la fédération avec un fournisseur d'identité pour accéder à l'aide Services AWS d'informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, d'un fournisseur d'identité Web AWS Directory Service, du répertoire Identity Center ou de tout utilisateur qui y accède à l'aide des informations d'identification fournies Services AWS par le biais d'une source d'identité. Lorsque des identités fédérées y accèdent Comptes AWS, elles assument des rôles, qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Vous pouvez créer des utilisateurs et des groupes dans IAM Identity Center, ou vous pouvez vous connecter et synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité afin de les utiliser dans toutes vos applications Comptes AWS et applications. Pour obtenir des informations sur IAM Identity Center, consultez Qu'est-ce que IAM Identity Center ? dans le Guide de l'utilisateur AWS IAM Identity Center .

Utilisateurs et groupes IAM

Un utilisateur IAM est une identité au sein de vous Compte AWS qui possède des autorisations spécifiques pour une seule personne ou une seule application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des utilisateurs IAM ayant des informations d'identification à long terme telles que des mots de passe et des clés d'accès. Toutefois, si certains cas d'utilisation spécifiques nécessitent des informations d'identification à long terme avec les utilisateurs IAM, nous vous recommandons d'effectuer une rotation des clés d'accès. Pour plus d'informations, consultez Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification dans le Guide de l'utilisateur IAM.

Un groupe IAM est une identité qui concerne un ensemble d'utilisateurs IAM. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez nommer un groupe IAMAdminset lui donner les autorisations nécessaires pour administrer les ressources IAM.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin.

Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des informations d'identification temporaires. Pour plus d'informations, consultez Cas d'utilisation pour les utilisateurs IAM dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une identité au sein de vous Compte AWS dotée d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais le rôle IAM n'est pas associé à une personne en particulier. Pour assumer temporairement un rôle IAM dans le AWS Management Console, vous pouvez passer d'un rôle d'utilisateur à un rôle IAM (console). Vous pouvez assumer un rôle en appelant une opération d' AWS API AWS CLI ou en utilisant une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez Méthodes pour endosser un rôle dans le Guide de l'utilisateur IAM.

Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

- Accès utilisateur fédéré : pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour obtenir des informations sur les rôles pour la fédération, consultez Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM. Si vous utilisez IAM Identity Center, vous configurez un jeu d'autorisations. IAM Identity Center met en corrélation le jeu d'autorisations avec un rôle dans IAM afin de contrôler à quoi vos identités peuvent accéder après leur authentification. Pour plus d'informations sur les jeux d'autorisations, consultez Jeux d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .
- Autorisations d'utilisateur IAM temporaires : un rôle ou un utilisateur IAM peut endosser un rôle IAM pour profiter temporairement d'autorisations différentes pour une tâche spécifique.
- Accès intercompte : vous pouvez utiliser un rôle IAM pour permettre à un utilisateur (principal de confiance) d'un compte différent d'accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Toutefois, dans certains Services AWS cas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour en savoir plus sur la différence entre les rôles et les politiques basées sur les ressources pour l'accès intercompte, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.
- Accès multiservices — Certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service

peut le faire en utilisant les autorisations d'appel du principal, un rôle de service ou un rôle lié au service.

- Sessions d'accès direct (FAS) : lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez Transmission des sessions d'accès.
- Rôle de service : il s'agit d'un rôle IAM attribué à un service afin de réaliser des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer un rôle de service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.
- Rôle lié à un service — Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un rôle IAM pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une EC2 instance et qui envoient des demandes AWS CLI d' AWS API. Cela est préférable au stockage des clés d'accès dans l' EC2 instance. Pour attribuer un AWS rôle à une EC2 instance et le rendre disponible pour toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes exécutés sur l' EC2 instance d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez Utiliser un rôle IAM pour accorder des autorisations aux applications exécutées sur des EC2 instances Amazon dans le guide de l'utilisateur IAM.

Gestion des accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique est un objet AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal

(utilisateur, utilisateur root ou session de rôle) fait une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations sur la structure et le contenu des documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

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

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Les politiques IAM définissent les autorisations d'une action, quelle que soit la méthode que vous utilisez pour exécuter l'opération. Par exemple, supposons que vous disposiez d'une politique qui autorise l'action `iam:GetRole`. Un utilisateur appliquant cette politique peut obtenir des informations sur le rôle à partir de AWS Management Console AWS CLI, de ou de l' AWS API.

Politiques basées sur l'identité

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez 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 classées comme des politiques en ligne ou des politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les politiques gérées sont des politiques autonomes que vous pouvez associer à plusieurs utilisateurs, groupes et rôles au sein de votre Compte AWS. Les politiques gérées incluent les politiques AWS gérées et les politiques gérées par le client. Pour découvrir comment choisir entre une politique gérée et une politique en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

Politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. 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. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les politiques AWS gérées par IAM dans une stratégie basée sur les ressources.

Listes de contrôle d'accès (ACLs)

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.

Amazon S3 et AWS WAF Amazon VPC sont des exemples de services compatibles. ACLs Pour en savoir plus ACLs, consultez la présentation de la liste de contrôle d'accès (ACL) dans le guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de politiques moins courants. Ces types de politiques peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants.

- Limite d'autorisations : une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le nombre maximal d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM (utilisateur ou rôle IAM). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations en résultant représentent la combinaison des politiques basées sur l'identité d'une entité et de ses limites d'autorisation. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus

d'informations sur les limites d'autorisations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.

- Politiques de contrôle des services (SCPs) : SCPs politiques JSON qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans AWS Organizations. AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée Comptes AWS les multiples propriétés de votre entreprise. Si vous activez toutes les fonctionnalités d'une organisation, vous pouvez appliquer des politiques de contrôle des services (SCPs) à l'un ou à l'ensemble de vos comptes. Le SCP limite les autorisations pour les entités figurant dans les comptes des membres, y compris chacune Utilisateur racine d'un compte AWS d'entre elles. Pour plus d'informations sur les Organizations et consultez SCPs les politiques de contrôle des services dans le Guide de AWS Organizations l'utilisateur.
- Politiques de contrôle des ressources (RCPs) : RCPs politiques JSON que vous pouvez utiliser pour définir le maximum d'autorisations disponibles pour les ressources de vos comptes sans mettre à jour les politiques IAM associées à chaque ressource que vous possédez. Le RCP limite les autorisations pour les ressources des comptes membres et peut avoir un impact sur les autorisations effectives pour les identités, y compris Utilisateur racine d'un compte AWS, qu'elles appartiennent ou non à votre organisation. Pour plus d'informations sur les Organizations RCPs, y compris une liste de ces Services AWS supports RCPs, consultez la section Resource control policies (RCPs) dans le guide de AWS Organizations l'utilisateur.
- Politiques de séance : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de séance en résultant sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations, consultez Politiques de 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 AWS Resilience Hub fonctionne avec IAM

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

Fonctionnalités IAM que vous pouvez utiliser avec AWS Resilience Hub

Fonctionnalité IAM	AWS Support du Resilience Hub
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 (spécifiques au service)	Oui
ACLs	Non
ABAC (identifications dans les politiques)	Partielle
Informations d'identification temporaires	Oui
Transmission des sessions d'accès (FAS)	Oui
Rôles de service	Oui

Pour obtenir une vue d'ensemble de la façon dont AWS Resilience Hub et les autres AWS services fonctionnent 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 Resilience Hub AWS

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

Exemples de politiques basées sur l'identité pour AWS Resilience Hub

Pour consulter des exemples de politiques basées sur l'identité du AWS Resilience Hub, consultez. Exemples de politiques basées sur l'identité pour AWS Resilience Hub

Politiques basées sur les ressources au sein AWS de Resilience Hub

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. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. L'ajout d'un principal intercompte à une politique basée sur les ressources ne représente qu'une partie de l'instauration de la relation d'approbation. Lorsque le principal et la ressource sont différents Comptes AWS, un administrateur IAM du compte sécurisé doit également accorder à l'entité principale (utilisateur ou rôle) l'autorisation d'accéder à la ressource. Pour ce faire, il attache une politique basée sur une identité à l'entité. Toutefois, si une politique basée sur des ressources

accorde l'accès à un principal dans le même compte, aucune autre politique basée sur l'identité n'est requise. Pour plus d'informations, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Actions politiques pour AWS Resilience Hub

Prend en charge les actions de politique : oui

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

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

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

Pour consulter la liste des actions de AWS Resilience Hub, consultez la section Actions définies par AWS Resilience Hub dans la référence d'autorisation de service.

Les actions politiques dans AWS Resilience Hub utilisent le préfixe suivant avant l'action :

```
resiliencehub
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

```
"Action": [
      "resiliencehub:action1",
      "resiliencehub:action2"
         ]
```

Pour consulter des exemples de politiques basées sur l'identité du AWS Resilience Hub, consultez. Exemples de politiques basées sur l'identité pour AWS Resilience Hub

Ressources politiques pour AWS Resilience Hub

Prend en charge les ressources de politique : oui

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

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

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

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

Pour consulter la liste des types de ressources AWS Resilience Hub et leurs caractéristiques ARNs, consultez la section Ressources définies par AWS Resilience Hub dans la référence d'autorisation de service. Pour savoir avec quelles actions vous pouvez spécifier l'ARN de chaque ressource, voir Actions définies par AWS Resilience Hub.

Pour consulter des exemples de politiques basées sur l'identité du AWS Resilience Hub, consultez. Exemples de politiques basées sur l'identité pour AWS Resilience Hub

Clés de conditions politiques pour AWS Resilience Hub

Prend en charge les clés de condition de politique spécifiques au service : oui

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

L'élément `Condition` (ou le bloc `Condition`) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément `Condition` est facultatif. Vous pouvez créer des expressions

conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande.

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

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

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

Pour consulter la liste des clés de condition de AWS Resilience Hub, consultez la section Clés de condition pour AWS Resilience Hub dans la référence d'autorisation de service. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, consultez la section Actions définies par AWS Resilience Hub.

Pour consulter des exemples de politiques basées sur l'identité du AWS Resilience Hub, consultez. Exemples de politiques basées sur l'identité pour AWS Resilience Hub

ACLs dans AWS Resilience Hub

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.

ABAC avec AWS Resilience Hub

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

Le contrôle d'accès par attributs (ABAC) est une stratégie d'autorisation qui définit des autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et à de nombreuses AWS ressources. L'étiquetage des

entités et des ressources est la première étape d'ABAC. Vous concevez ensuite des politiques ABAC pour autoriser des opérations quand l'identification du principal correspond à celle de la ressource à laquelle il tente d'accéder.

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

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

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

Pour plus d'informations sur 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 AWS Resilience Hub

Prend en charge les informations d'identification temporaires : oui

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

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

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide de l' AWS API AWS CLI or. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour y accéder

AWS. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez Informations d'identification de sécurité temporaires dans IAM.

Sessions d'accès transféré pour AWS Resilience Hub

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

Lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez Transmission des sessions d'accès.

Rôles de service pour AWS Resilience Hub

Prend en charge les rôles de service : oui

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.

> **Warning**
>
> La modification des autorisations pour un rôle de service peut perturber les fonctionnalités de AWS Resilience Hub. Modifiez les rôles de service uniquement lorsque AWS Resilience Hub fournit des instructions à cet effet.

Exemples de politiques basées sur l'identité pour AWS Resilience Hub

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier les ressources du AWS Resilience Hub. Ils ne peuvent pas non plus effectuer de tâches à l'aide de l'API AWS

Management Console, AWS Command Line Interface (AWS CLI) ou de AWS l'API. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

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

Pour plus de détails sur les actions et les types de ressources définis par AWS Resilience Hub, y compris le ARNs format de chaque type de ressource, voir Actions, ressources et clés de condition pour AWS Resilience Hub dans la référence d'autorisation de service.

Rubriques

- Bonnes pratiques en matière de politiques
- Utilisation de la console AWS Resilience Hub
- Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations
- Liste des AWS Resilience Hub applications disponibles
- Commencer l'évaluation d'une candidature
- Supprimer une évaluation de candidature
- Création d'un modèle de recommandation pour une application spécifique
- Supprimer un modèle de recommandation pour une application spécifique
- Mettre à jour une application avec une politique de résilience spécifique

Bonnes pratiques en matière de politiques

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

Utilisation de la console AWS Resilience Hub

Pour accéder à la console AWS Resilience Hub, vous devez disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et d'afficher des informations détaillées sur les ressources du AWS Resilience Hub 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 AWS Resilience Hub, associez également le AWS Resilience Hub `ConsoleAccess` ou la politique `ReadOnly` AWS gérée aux entités. Pour plus d'informations, consultez Ajout d'autorisations à un utilisateur dans le Guide de l'utilisateur IAM.

La politique suivante accorde aux utilisateurs l'autorisation de répertorier et d'afficher toutes les ressources de la AWS Resilience Hub console, mais pas de les créer, de les mettre à jour ou de les supprimer.

```
{
     "Version": "2012-10-17",
     "Statement": [
         {
             "Effect": "Allow",
             "Action": [
                 "resiliencehub:List*",
                 "resiliencehub:Describe*"
             ],
             "Resource": "*"
         }
     ]
 }
```

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux utilisateurs IAM d'afficher les politiques en ligne et gérées attachées à leur identité d'utilisateur. Cette politique inclut les autorisations permettant d'effectuer cette action sur la console ou par programmation à l'aide de l'API AWS CLI or AWS .

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

```
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Liste des AWS Resilience Hub applications disponibles

La politique suivante autorise les utilisateurs à répertorier les AWS Resilience Hub applications disponibles.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PolicyExample",
      "Effect": "Allow",
      "Action": [
          "resiliencehub:ListApps"
```

```
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Commencer l'évaluation d'une candidature

La politique suivante autorise les utilisateurs à démarrer une évaluation pour une AWS Resilience Hub application spécifique.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PolicyExample",
      "Effect": "Allow",
      "Action": [
          "resiliencehub:StartAppAssessment"
      ],
      "Resource": [
        "arn:aws:resiliencehub:*:*:app/appId"
      ]
    }
  ]
}
```

Supprimer une évaluation de candidature

La politique suivante autorise les utilisateurs à supprimer une évaluation pour une AWS Resilience Hub application spécifique.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PolicyExample",
      "Effect": "Allow",
      "Action": [
          "resiliencehub:DeleteAppAssessment"
```

```
      ],
      "Resource": [
        "arn:aws:resiliencehub:*:*:app/appId"
      ]
    }
  ]
}
```

Création d'un modèle de recommandation pour une application spécifique

La politique suivante autorise les utilisateurs à créer un modèle de recommandation pour une AWS Resilience Hub application spécifique.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PolicyExample",
      "Effect": "Allow",
      "Action": [
          "resiliencehub:CreateRecommendationTemplate"
      ],
      "Resource": [
        "arn:aws:resiliencehub:*:*:app/appId"
      ]
    }
  ]
}
```

Supprimer un modèle de recommandation pour une application spécifique

La politique suivante autorise les utilisateurs à supprimer un modèle de recommandation pour une AWS Resilience Hub application spécifique.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PolicyExample",
      "Effect": "Allow",
      "Action": [
          "resiliencehub:DeleteRecommendationTemplate"
```

```
      ],
      "Resource": [
        "arn:aws:resiliencehub:*:*:app/appId"
      ]
    }
  ]
}
```

Mettre à jour une application avec une politique de résilience spécifique

La politique suivante accorde aux utilisateurs l'autorisation de mettre à jour une AWS Resilience Hub application avec une politique de résilience spécifique.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PolicyExample",
      "Effect": "Allow",
      "Action": [
          "resiliencehub:UpdateApp"
      ],
      "Resource": [
        "arn:aws:resiliencehub:*:*:app/appId"
      ],
      "Condition": {
        "StringLike" : { "resiliencehub:policyArn" : "arn:aws:resiliencehub:us-
west-2:111122223333:resiliency-policy/*" }
      }
    }
  ]
}
```

Configuration des rôles et autorisations IAM

AWS Resilience Hub vous permet de configurer les rôles IAM que vous souhaitez utiliser lors de l'exécution d'évaluations pour votre application. Il existe plusieurs méthodes de configuration pour AWS Resilience Hub obtenir un accès en lecture seule aux ressources de votre application. Cependant, AWS Resilience Hub recommande les méthodes suivantes :

- Accès basé sur les rôles : ce rôle est défini et utilisé dans le compte courant. AWS Resilience Hub assumera ce rôle pour accéder aux ressources de votre application.

Pour fournir un accès basé sur les rôles, le rôle doit inclure les éléments suivants :

- Autorisation en lecture seule pour lire vos ressources (il est AWS Resilience Hub recommandé d'utiliser la politique `AWSResilienceHubAsssessmentExecutionPolicy` gérée).
- Politique de confiance pour assumer ce rôle, ce qui permet au directeur du AWS Resilience Hub service d'assumer ce rôle. Si aucun rôle de ce type n'est configuré dans votre compte, les instructions pour créer ce rôle s' AWS Resilience Hub afficheront. Pour de plus amples informations, veuillez consulter the section called "Autorisations de configuration".

> **Note**
>
> Si vous fournissez uniquement le nom du rôle de l'invocateur et si vos ressources se trouvent dans un autre compte, AWS Resilience Hub vous utiliserez ce nom de rôle dans les autres comptes pour accéder aux ressources entre comptes. Vous pouvez éventuellement configurer le rôle ARNs pour d'autres comptes, qui seront utilisés à la place du nom du rôle de l'invocateur.

- Accès utilisateur IAM actuel : AWS Resilience Hub utilisera l'utilisateur IAM actuel pour accéder aux ressources de votre application. Lorsque vos ressources se trouvent dans un autre compte, il AWS Resilience Hub assumera les rôles IAM suivants pour accéder aux ressources :
  - `AwsResilienceHubAdminAccountRole`dans le compte courant
  - `AwsResilienceHubExecutorAccountRole`dans d'autres comptes

  En outre, lorsque vous configurez une évaluation planifiée, AWS Resilience Hub assumera le `AwsResilienceHubPeriodicAssessmentRole` rôle. Toutefois, son utilisation n'`AwsResilienceHubPeriodicAssessmentRole`est pas conseillée car vous devez configurer manuellement les rôles et les autorisations, et certaines fonctionnalités (telles que la notification Drift) risquent de ne pas fonctionner comme prévu.

Résolution des problèmes d'identité et d'accès au AWS Resilience Hub

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec AWS Resilience Hub et IAM.

Rubriques

- Je ne suis pas autorisé à effectuer une action dans AWS Resilience Hub

- Je ne suis pas autorisé à effectuer iam : PassRole
- Je souhaite permettre à des personnes extérieures à moi d'accéder Compte AWS aux ressources de mon AWS Resilience Hub

Je ne suis pas autorisé à effectuer une action dans AWS Resilience Hub

Si vous recevez une erreur qui indique que vous n'êtes pas autorisé à effectuer une action, vos politiques doivent être mises à jour afin de vous permettre d'effectuer l'action.

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 `resiliencehub:`*`GetWidget`* fictives.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 resiliencehub:GetWidget on resource: my-example-widget
```

Dans ce cas, la politique qui s'applique à l'utilisateur `mateojackson` doit être mise à jour pour autoriser l'accès à la ressource *`my-example-widget`* à l'aide de l'action `resiliencehub:`*`GetWidget`*.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

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 AWS Resilience Hub.

Certains vous Services AWS permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, un utilisateur doit disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un utilisateur IAM nommé `marymajor` essaie d'utiliser la console pour effectuer une action dans AWS Resilience Hub. Toutefois, l'action nécessite que le service ait des autorisations accordées par un rôle de service. Mary ne dispose pas des autorisations nécessaires pour transférer le rôle au service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je souhaite permettre à des personnes extérieures à moi d'accéder Compte AWS aux ressources de mon AWS Resilience Hub

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 AWS Resilience Hub prend en charge ces fonctionnalités, consultezComment AWS Resilience Hub fonctionne 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.

AWS Resilience Hub référence des autorisations d'accès

Vous pouvez utiliser AWS Identity and Access Management (IAM) pour gérer l'accès aux ressources de l'application et créer des politiques IAM qui s'appliquent aux utilisateurs, aux groupes ou aux rôles.

Chaque AWS Resilience Hub application peut être configurée pour utiliser the section called "Rôle d'invocateur" (un rôle IAM) ou utiliser les autorisations utilisateur IAM actuelles (ainsi qu'un ensemble de rôles prédéfinis pour les évaluations croisées et planifiées). Dans ce rôle, vous pouvez associer une politique qui définit les autorisations requises AWS Resilience Hub pour accéder à d'autres AWS ressources ou à des ressources d'application. Le rôle d'invocateur doit avoir une politique de confiance ajoutée à AWS Resilience Hub Service Principal.

Pour gérer les autorisations de votre application, nous vous recommandons d'utiliserthe section called "AWS politiques gérées". Vous pouvez utiliser ces politiques gérées sans aucune modification, ou vous pouvez les utiliser comme point de départ pour rédiger vos propres politiques restrictives. Les politiques peuvent restreindre les autorisations des utilisateurs au niveau des ressources pour différentes actions en utilisant des conditions facultatives supplémentaires.

Si les ressources de votre application se trouvent dans des comptes différents (comptes secondaires/de ressources), vous devez configurer un nouveau rôle dans chaque compte contenant les ressources de votre application.

> **Note**
>
> Si vous définissez des points de terminaison VPC pour vos ressources de charge de travail, assurez-vous que les politiques de point de terminaison VPC fournissent un accès en lecture seule pour accéder aux ressources. AWS Resilience Hub Pour plus d'informations, consultez Contrôler l'accès aux points de terminaison VPC à l'aide de politiques de point de terminaison.

Rubriques

- the section called "Utilisation du rôle IAM"
- the section called "Utilisation des autorisations utilisateur IAM actuelles"

Utilisation du rôle IAM

AWS Resilience Hub utilisera un rôle IAM prédéfini existant pour accéder à vos ressources dans le compte principal ou le compte secondaire/de ressources. Il s'agit de l'option d'autorisation recommandée pour accéder à vos ressources.

Rubriques

- the section called "Rôle d'invocateur"
- the section called "Rôles dans différents AWS comptes pour un accès entre comptes"

Rôle d'invocateur

Le rôle d' AWS Resilience Hub invocateur est un rôle AWS Identity and Access Management (IAM) censé accéder AWS Resilience Hub aux AWS services et aux ressources. Par exemple, vous pouvez créer un rôle d'invocateur autorisé à accéder à votre modèle CFN et à la ressource qu'il crée. Cette page fournit des informations sur la création, l'affichage et la gestion d'un rôle d'invocateur d'application.

Lorsque vous créez une application, vous fournissez un rôle d'invocateur. AWS Resilience Hub assume ce rôle pour accéder à vos ressources lorsque vous importez des ressources ou que vous lancez une évaluation. AWS Resilience Hub Pour assumer correctement votre rôle d'invocateur, la politique de confiance du rôle doit spécifier que le principal du AWS Resilience Hub service (resiliencehub.amazonaws.com) est un service fiable.

Pour afficher le rôle d'invocateur de l'application, choisissez Applications dans le volet de navigation, puis choisissez Mettre à jour les autorisations dans le menu Actions de la page Application.

Vous pouvez ajouter ou supprimer des autorisations associées à un rôle d'invocateur d'application à tout moment, ou configurer votre application pour qu'elle utilise un rôle différent pour accéder aux ressources de l'application.

Rubriques

- the section called "Création d'un rôle d'invocateur dans la console IAM"
- the section called "Gestion des rôles avec l'API IAM"
- the section called "Définition de la politique de confiance à l'aide du fichier JSON"

Création d'un rôle d'invocateur dans la console IAM

Pour permettre AWS Resilience Hub l'accès aux AWS services et aux ressources, vous devez créer un rôle d'invocateur dans le compte principal à l'aide de la console IAM. Pour plus d'informations sur la création de rôles à l'aide de la console IAM, consultez Création d'un rôle pour un AWS service (console).

Pour créer un rôle d'invocateur dans le compte principal à l'aide de la console IAM

1. Ouvrez la console IAM à l'adresse `https://console.aws.amazon.com/iam/`.
2. Dans le volet de navigation, sélectionnez Rôles, puis sélectionnez Créer un rôle.
3. Sélectionnez Politique de confiance personnalisée, copiez la politique suivante dans la fenêtre Politique de confiance personnalisée, puis choisissez Suivant.

> **Note**
>
> Si vos ressources se trouvent dans des comptes différents, vous devez créer un rôle dans chacun de ces comptes et utiliser la politique de confiance du compte secondaire pour les autres comptes.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "resiliencehub.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

4. Dans la section Politiques d'autorisations de la page Ajouter des autorisations, entrez `AWSResilienceHubAsssessmentExecutionPolicy` les politiques de filtrage par propriété ou par nom de politique et appuyez sur la case Entrée.
5. Sélectionnez la politique, puis cliquez sur Next.

6. Dans la section Détails du rôle, entrez un nom de rôle unique (tel que`AWSResilienceHubAssessmentRole`) dans la zone Nom du rôle.

   Ce champ n'accepte que les caractères alphanumériques et les caractères `+=,.@-_/` « ».

7. (Facultatif) Entrez une description du rôle dans la zone Description.
8. Choisissez Create Role (Créer le rôle).

   Pour modifier les cas d'utilisation et les autorisations, à l'étape 6, choisissez le bouton Modifier situé à droite des sections Étape 1 : Sélectionnez les entités de confiance ou Étape 2 : Ajouter des autorisations.

Après avoir créé le rôle d'invocateur et le rôle de ressource (le cas échéant), vous pouvez configurer votre application pour qu'elle utilise ces rôles.

> **Note**
>
> Vous devez disposer d'une `iam:passRole` autorisation dans votre utilisateur/rôle IAM actuel sur le rôle d'invocateur lors de la création ou de la mise à jour de l'application. Toutefois, vous n'avez pas besoin de cette autorisation pour exécuter une évaluation.

Gestion des rôles avec l'API IAM

La politique de confiance d'un rôle autorise le principal spécifié à assumer le rôle. Pour créer les rôles à l'aide de AWS Command Line Interface (AWS CLI), utilisez la `create-role` commande. Lorsque vous utilisez cette commande, vous pouvez spécifier la politique de confiance en ligne. L'exemple suivant montre comment accorder au AWS Resilience Hub service l'autorisation principale d'assumer votre rôle.

> **Note**
>
> L'obligation d'échapper aux guillemets (`'  '`) dans la chaîne JSON peut varier en fonction de la version de votre shell.

Exemple **`create-role`**

```
aws iam create-role --role-name AWSResilienceHubAssessmentRole --assume-role-policy-
document '{
  "Version": "2012-10-17","Statement":
  [
    {
      "Effect": "Allow",
      "Principal": {"Service": "resiliencehub.amazonaws.com"},
      "Action": "sts:AssumeRole"
    }
  ]
}'
```

Définition de la politique de confiance à l'aide du fichier JSON

Vous pouvez définir la politique de confiance pour le rôle à l'aide d'un fichier JSON distinct, puis exécuter la `create-role` commande. Dans l'exemple suivant, **`trust-policy.json`**il s'agit d'un fichier qui contient la politique de confiance dans le répertoire actuel. Cette politique est attachée à un rôle en exécutant une **`create-role`**commande. Le résultat de la **`create-role`** commande est affiché dans l'exemple de sortie. Pour ajouter des autorisations au rôle, utilisez la attach-policy-to-rolecommande et vous pouvez commencer par ajouter la politique `AWSResilienceHubAsssessmentExecutionPolicy` gérée. Pour plus d'informations sur cette politique gérée, consultezthe section called “AWSResilienceHubAsssessmentExecutionPolicy”.

Exemple **`trust-policy.json`**

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Principal": {
            "Service": "resiliencehub.amazonaws.com"
        },
        "Action": "sts:AssumeRole"
    }]
}
```

Exemple **`create-role`**

```
aws iam create-role --role-name AWSResilienceHubAssessmentRole --assume-
role-policy-document file://trust-policy.json
```

Exemple de sortie

```
{
    "Role": {
        "Path": "/",
        "RoleName": "AWSResilienceHubAssessmentRole",
        "RoleId": "AROAQFOXMPL6TZ6ITKWND",
        "Arn": "arn:aws:iam::123456789012:role/AWSResilienceHubAssessmentRole",
        "CreateDate": "2020-01-17T23:19:12Z",
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [{
                "Effect": "Allow",
                "Principal": {
                    "Service": "resiliencehub.amazonaws.com"
                },
                "Action": "sts:AssumeRole"
            }]
        }
    }
}
```

Exemple **`attach-policy-to-role`**

```
aws iam attach-role-policy --role-name AWSResilienceHubAssessmentRole --
policy-arn arn:aws:iam::aws:policy/
AWSResilienceHubAsssessmentExecutionPolicy
```

Rôles dans différents AWS comptes pour un accès entre comptes (facultatif)

Lorsque vos ressources se trouvent dans des comptes secondaires/de ressources, vous devez créer des rôles dans chacun de ces comptes afin de permettre une évaluation réussie AWS Resilience Hub de votre candidature. La procédure de création de rôle est similaire au processus de création de rôle d'invocateur, à l'exception de la configuration de la politique de confiance.

> **Note**
>
> Vous devez créer les rôles dans les comptes secondaires où se trouvent les ressources.

Rubriques

- the section called "Création d'un rôle dans la console IAM pour les comptes secondaires/de ressources"
- the section called "Gestion des rôles avec l'API IAM"
- the section called "Définition de la politique de confiance à l'aide du fichier JSON"

Création d'un rôle dans la console IAM pour les comptes secondaires/de ressources

Pour permettre AWS Resilience Hub l'accès aux AWS services et aux ressources d'autres AWS comptes, vous devez créer des rôles dans chacun de ces comptes.

Pour créer un rôle dans la console IAM pour les comptes secondaires/de ressources à l'aide de la console IAM

1. Ouvrez la console IAM à l'adresse `https://console.aws.amazon.com/iam/`.
2. Dans le volet de navigation, sélectionnez Rôles, puis sélectionnez Créer un rôle.
3. Sélectionnez Politique de confiance personnalisée, copiez la politique suivante dans la fenêtre Politique de confiance personnalisée, puis choisissez Suivant.

> **Note**
>
> Si vos ressources se trouvent dans des comptes différents, vous devez créer un rôle dans chacun de ces comptes et utiliser la politique de confiance du compte secondaire pour les autres comptes.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::primary_account_id:role/InvokerRoleName"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
```

```
}
```

4. Dans la section Politiques d'autorisations de la page Ajouter des autorisations, entrez `AWSResilienceHubAsssessmentExecutionPolicy` les politiques de filtrage par propriété ou par nom de politique et appuyez sur la case Entrée.
5. Sélectionnez la politique, puis cliquez sur Next.
6. Dans la section Détails du rôle, entrez un nom de rôle unique (tel que`AWSResilienceHubAssessmentRole`) dans la zone Nom du rôle.
7. (Facultatif) Entrez une description du rôle dans la zone Description.
8. Choisissez Create Role (Créer le rôle).

   Pour modifier les cas d'utilisation et les autorisations, à l'étape 6, choisissez le bouton Modifier situé à droite des sections Étape 1 : Sélectionnez les entités de confiance ou Étape 2 : Ajouter des autorisations.

En outre, vous devez également ajouter l'`sts:assumeRole`autorisation au rôle d'invocateur pour lui permettre d'assumer les rôles dans vos comptes secondaires.

Ajoutez la politique suivante à votre rôle d'invocateur pour chacun des rôles secondaires que vous avez créés :

```
{
    "Effect": "Allow",
    "Resource": [
      "arn:aws:iam::secondary_account_id_1:role/RoleInSecondaryAccount_1",
      "arn:aws:iam::secondary_account_id_2:role/RoleInSecondaryAccount_2",
      ...
      ],
      "Action": [
        "sts:AssumeRole"
      ]
}
```

Gestion des rôles avec l'API IAM

La politique de confiance d'un rôle autorise le principal spécifié à assumer le rôle. Pour créer les rôles à l'aide de AWS Command Line Interface (AWS CLI), utilisez la `create-role` commande. Lorsque vous utilisez cette commande, vous pouvez préciser la politique d'approbation en ligne. L'exemple

suivant montre comment accorder au directeur du AWS Resilience Hub service l'autorisation d'assumer votre rôle.

> **Note**
>
> L'obligation d'échapper aux guillemets (`'  '`) dans la chaîne JSON peut varier en fonction de la version de votre shell.

Exemple **`create-role`**

```
aws iam create-role --role-name AWSResilienceHubAssessmentRole --assume-role-policy-
document '{"Version": "2012-10-17","Statement": [{"Effect": "Allow","Principal":
 {"AWS": ["arn:aws:iam::primary_account_id:role/InvokerRoleName"]},"Action":
 "sts:AssumeRole"}]}'
```

Vous pouvez également définir la politique d'approbation pour le rôle à l'aide d'un fichier JSON séparé. Dans l'exemple suivant, le fichier `trust-policy.json` se trouve dans le répertoire actuel.

Définition de la politique de confiance à l'aide du fichier JSON

Vous pouvez définir la politique de confiance pour le rôle à l'aide d'un fichier JSON distinct, puis exécuter la `create-role` commande. Dans l'exemple suivant, **`trust-policy.json`**il s'agit d'un fichier qui contient la politique de confiance dans le répertoire actuel. Cette politique est attachée à un rôle en exécutant une **`create-role`**commande. Le résultat de la **`create-role`** commande est affiché dans l'exemple de sortie. Pour ajouter des autorisations à un rôle, utilisez la attach-policy-to-rolecommande et vous pouvez commencer par ajouter la politique `AWSResilienceHubAsssessmentExecutionPolicy` gérée. Pour plus d'informations sur cette politique gérée, consultezthe section called "AWSResilienceHubAsssessmentExecutionPolicy".

Exemple **`trust-policy.json`**

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
```

```
          "arn:aws:iam::primary_account_id:role/InvokerRoleName"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Exemple **`create-role`**

```
aws iam create-role --role-name AWSResilienceHubAssessmentRole --assume-role-policy-
document file://trust-policy.json
```

Exemple de sortie

```
{
    "Role": {
        "Path": "/",
        "RoleName": "AWSResilienceHubAssessmentRole2",
        "RoleId": "AROAT2GICMEDJML6EVQRG",
        "Arn": "arn:aws:iam::262412591366:role/AWSResilienceHubAssessmentRole2",
        "CreateDate": "2023-08-02T07:49:23+00:00",
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Effect": "Allow",
                    "Principal": {
                        "AWS": [
                            "arn:aws:iam::262412591366:role/
AWSResilienceHubAssessmentRole"
                        ]
                    },
                    "Action": "sts:AssumeRole"
                }
            ]
        }
    }
}
```

Exemple **`attach-policy-to-role`**

`aws iam attach-role-policy --role-name AWSResilienceHubAssessmentRole --policy-arn arn:aws:iam::aws:policy/AWSResilienceHubAsssessmentExecutionPolicy`.

Utilisation des autorisations utilisateur IAM actuelles

Utilisez cette méthode si vous souhaitez utiliser vos autorisations d'utilisateur IAM actuelles pour créer et exécuter une évaluation. Vous pouvez associer la politique `AWSResilienceHubAsssessmentExecutionPolicy` gérée à votre utilisateur IAM ou à un rôle associé à votre utilisateur.

Configuration d'un compte unique

L'utilisation de la politique gérée mentionnée ci-dessus est suffisante pour exécuter une évaluation sur une application gérée dans le même compte que l'utilisateur IAM.

Configuration de l'évaluation planifiée

Vous devez créer un nouveau rôle `AwsResilienceHubPeriodicAssessmentRole` pour pouvoir AWS Resilience Hub effectuer des tâches liées à l'évaluation planifiée.

> **Note**
>
> - Lors de l'utilisation de l'accès basé sur les rôles (avec le rôle d'invocateur mentionné ci-dessus), cette étape n'est pas obligatoire.
> - Le nom du rôle doit être`AwsResilienceHubPeriodicAssessmentRole`.

Pour permettre d' AWS Resilience Hub effectuer des tâches liées à l'évaluation planifiée

1. Associez la politique `AWSResilienceHubAsssessmentExecutionPolicy` gérée au rôle.
2. Ajoutez la politique suivante, où se `primary_account_id` trouve le AWS compte sur lequel l'application est définie et où sera exécutée l'évaluation. En outre, vous devez ajouter la politique de confiance associée au rôle de l'évaluation planifiée, (`AwsResilienceHubPeriodicAssessmentRole`), qui autorise le AWS Resilience Hub service à assumer le rôle de l'évaluation planifiée.

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

```
    {
      "Effect": "Allow",
      "Action": [
        "iam:GetRole",
        "sts:AssumeRole"
      ],
      "Resource": "arn:aws:iam::primary_account_id:role/
AwsResilienceHubAdminAccountRole"
    },
    {
      "Effect": "Allow",
      "Action": [
        "sts:AssumeRole"
      ],
      "Resource": [
        "arn:aws:iam::primary_account_id:role/
AwsResilienceHubAssessmentEKSAccessRole"
      ]
    }
  ]
}
```

Politique de confiance pour le rôle de l'évaluation planifiée (**`AwsResilienceHubPeriodicAssessmentRole`**)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "resiliencehub.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Configuration multi-comptes

Les politiques d'autorisation IAM suivantes sont requises si vous utilisez AWS Resilience Hub avec plusieurs comptes. Chaque AWS compte peut nécessiter des autorisations différentes en fonction de votre cas d'utilisation. Lors de la configuration AWS Resilience Hub de l'accès entre comptes, les comptes et rôles suivants sont pris en compte :

- Compte principal : AWS compte dans lequel vous souhaitez créer l'application et exécuter des évaluations.
- Compte (s) secondaire/de ressources — AWS compte (s) où se trouvent les ressources.

> **Note**
>
> - Lors de l'utilisation de l'accès basé sur les rôles (avec le rôle d'invocateur mentionné ci-dessus), cette étape n'est pas obligatoire.
> - Pour plus d'informations sur la configuration des autorisations d'accès à Amazon Elastic Kubernetes Service, consultez. the section called "Activation de AWS Resilience Hub l'accès à votre cluster Amazon EKS"

Configuration du compte principal

Vous devez créer un nouveau rôle `AwsResilienceHubAdminAccountRole` dans le compte principal et autoriser AWS Resilience Hub l'accès pour l'assumer. Ce rôle sera utilisé pour accéder à un autre rôle de votre AWS compte contenant vos ressources. Il ne doit pas être autorisé à lire les ressources.

> **Note**
>
> - Le nom du rôle doit être`AwsResilienceHubAdminAccountRole`.
> - Il doit être créé dans le compte principal.
> - Votre utilisateur/rôle IAM actuel doit être `iam:assumeRole` autorisé à assumer ce rôle.
> - `secondary_account_id_1/2/...`Remplacez-les par les identifiants de compte secondaires appropriés.

La politique suivante fournit des autorisations d'exécuteur testamentaire à votre rôle pour accéder aux ressources d'un autre rôle de votre AWS compte :

```
{
  {
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Resource": [
        "arn:aws:iam::secondary_account_id_1:role/AwsResilienceHubExecutorAccountRole",
        "arn:aws:iam::secondary_account_id_2:role/AwsResilienceHubExecutorAccountRole",
        ...
      ],
      "Action": [
        "sts:AssumeRole"
      ]
    }
  ]
}
```

La politique de confiance pour le rôle d'administrateur (`AwsResilienceHubAdminAccountRole`) est la suivante :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::primary_account_id:role/caller_IAM_role"
      },
      "Action": "sts:AssumeRole"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::primary_account_id:role/
AwsResilienceHubPeriodicAssessmentRole"
      },
      "Action": "sts:AssumeRole"
    }
  ]
```

```
}
```

Configuration d'un ou de plusieurs comptes secondaires/ressources

Dans chacun de vos comptes secondaires, vous devez créer un nouveau rôle `AwsResilienceHubExecutorAccountRole` et activer le rôle d'administrateur créé ci-dessus pour assumer ce rôle. Étant donné que ce rôle sera utilisé AWS Resilience Hub pour analyser et évaluer les ressources de votre application, il nécessitera également les autorisations appropriées.

Toutefois, vous devez associer la politique `AWSResilienceHubAsssessmentExecutionPolicy` gérée au rôle et associer la politique du rôle de l'exécuteur.

La politique de confiance relative au rôle de l'exécuteur est la suivante :

```
{
  {
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::primary_account_id:role/AwsResilienceHubAdminAccountRole"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

AWS politiques gérées pour AWS Resilience Hub

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.

AWSResilienceHubAsssessmentExecutionPolicy

Vous pouvez les associer `AWSResilienceHubAsssessmentExecutionPolicy` à vos identités IAM. Lors de l'exécution d'une évaluation, cette politique accorde des autorisations d'accès à d'autres AWS services pour exécuter des évaluations.

Détails de l'autorisation

Cette politique fournit les autorisations adéquates pour publier des alarmes AWS FIS et des modèles SOP dans votre compartiment Amazon Simple Storage Service (Amazon S3). Le nom du compartiment Amazon S3 doit commencer para`ws-resilience-hub-artifacts-`. Si vous souhaitez publier dans un autre compartiment Amazon S3, vous pouvez le faire en appelant `CreateRecommendationTemplate` l'API. Pour de plus amples informations, veuillez consulter CreateRecommendationTemplate.

Cette politique inclut les autorisations suivantes :

- Amazon CloudWatch (CloudWatch) — Obtient toutes les alarmes implémentées que vous avez configurées dans Amazon CloudWatch pour surveiller l'application. En outre, nous publions `cloudwatch:PutMetricData` des CloudWatch métriques pour le score de résilience de l'application dans l'espace de `ResilienceHub` noms.
- Amazon Data Lifecycle Manager : obtient et fournit `Describe` des autorisations pour les ressources Amazon Data Lifecycle Manager associées à votre AWS compte.
- Amazon DevOps Guru — Répertorie et fournit `Describe` des autorisations pour les ressources Amazon DevOps Guru associées à votre AWS compte.
- Amazon DocumentDB — Répertorie et fournit des `Describe` autorisations pour les ressources Amazon DocumentDB associées à votre compte. AWS

- Amazon DynamoDB (DynamoDB) : répertorie et fournit des `Describe` autorisations pour les ressources Amazon DynamoDB associées à votre compte. AWS
- Amazon ElastiCache (ElastiCache) — Fournit `Describe` des autorisations pour les ElastiCache ressources associées à votre AWS compte.
- Amazon ElastiCache (Redis OSS) Serverless (ElastiCache (Redis OSS) Serverless) — Fournit des `Describe` autorisations pour les configurations sans serveur ElastiCache (Redis OSS) associées à votre compte. AWS
- Amazon Elastic Compute Cloud (Amazon EC2) : répertorie et fournit `Describe` des autorisations pour les EC2 ressources Amazon associées à votre AWS compte.
- Amazon Elastic Container Registry (Amazon ECR) : fournit `Describe` des autorisations pour les ressources Amazon ECR associées à votre compte. AWS
- Amazon Elastic Container Service (Amazon ECS) : `Describe` fournit des autorisations pour les ressources Amazon ECS associées AWS à votre compte.
- Amazon Elastic File System (Amazon EFS) : fournit `Describe` des autorisations pour les ressources Amazon EFS associées à votre AWS compte.
- Amazon Elastic Kubernetes Service (Amazon EKS) : répertorie et `Describe` fournit des autorisations pour les ressources Amazon EKS associées à votre compte. AWS
- Amazon EC2 Auto Scaling — Répertorie et fournit `Describe` des autorisations pour les ressources Amazon EC2 Auto Scaling associées à votre AWS compte.
- Amazon EC2 Systems Manager (SSM) : fournit des `Describe` autorisations pour les ressources SSM associées à votre AWS compte.
- AWS Fault Injection Service (AWS FIS) — Répertorie et fournit `Describe` des autorisations pour les AWS FIS expériences et les modèles d'expériences associés à votre AWS compte.
- Amazon FSx pour Windows File Server (Amazon FSx) : répertorie et fournit `Describe` des autorisations pour les FSx ressources Amazon associées à votre AWS compte.
- Amazon RDS — Répertorie et fournit `Describe` des autorisations pour les ressources Amazon RDS associées à votre AWS compte.
- Amazon Route 53 (Route 53) — Répertorie et fournit `Describe` des autorisations pour les ressources Route 53 associées à votre AWS compte.
- Amazon Route 53 Resolver — Répertorie et fournit des `Describe` autorisations pour les Amazon Route 53 Resolver ressources associées à votre AWS compte.
- Amazon Simple Notification Service (Amazon SNS) : répertorie et `Describe` fournit des autorisations pour les ressources Amazon SNS associées à votre compte. AWS

- Amazon Simple Queue Service (Amazon SQS) — Répertorie et `Describe` fournit des autorisations pour les ressources Amazon SQS associées à votre compte. AWS
- Amazon Simple Storage Service (Amazon S3) — Répertorie et `Describe` fournit des autorisations pour les ressources Amazon S3 associées AWS à votre compte.

> **Note**
>
> Lors de l'exécution d'une évaluation, si des autorisations manquantes doivent être mises à jour à partir des politiques gérées, l'évaluation AWS Resilience Hub sera terminée avec succès en utilisant l'GetBucketLogging autorisation s3 :. Cependant, AWS Resilience Hub affichera un message d'avertissement répertoriant les autorisations manquantes et fournissant un délai de grâce pour les ajouter. Si vous n'ajoutez pas les autorisations manquantes dans le délai de grâce spécifié, l'évaluation échouera.

- AWS Backup — Répertorie et obtient `Describe` les autorisations pour les ressources Amazon EC2 Auto Scaling associées à votre AWS compte.
- AWS CloudFormation — Répertorie les ressources associées à AWS CloudFormation votre AWS compte et obtient des `Describe` autorisations pour celles-ci.
- AWS DataSync — Répertorie et fournit des `Describe` autorisations pour les AWS DataSync ressources associées à votre AWS compte.
- AWS Directory Service — Répertorie et fournit des `Describe` autorisations pour les AWS Directory Service ressources associées à votre AWS compte.
- AWS Elastic Disaster Recovery (Elastic Disaster Recovery) — Fournit `Describe` des autorisations pour les ressources Elastic Disaster Recovery associées à votre AWS compte.
- AWS Lambda (Lambda) — Répertorie et fournit des `Describe` autorisations pour les ressources Lambda associées à votre compte. AWS
- AWS Resource Groups (Resource Groups) — Répertorie et fournit des `Describe` autorisations pour les ressources Resource Groups associées à votre AWS compte.
- AWS Service Catalog (Service Catalog) — Répertorie et fournit `Describe` des autorisations pour les ressources Service Catalog associées à votre AWS compte.
- AWS Step Functions — Répertorie et fournit des `Describe` autorisations pour les AWS Step Functions ressources associées à votre AWS compte.
- Elastic Load Balancing — Répertorie et fournit `Describe` des autorisations pour les ressources Elastic Load Balancing associées à votre AWS compte.

- `ssm:GetParametersByPath`— Nous utilisons cette autorisation pour gérer les CloudWatch alarmes, les tests ou SOPs ceux qui sont configurés pour votre application.

La politique IAM suivante est requise pour qu'un AWS compte ajoute des autorisations pour les utilisateurs, les groupes d'utilisateurs et les rôles qui fournissent les autorisations requises pour que votre équipe puisse accéder aux AWS services lors de l'exécution d'évaluations.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSResilienceHubFullResourceStatement",
            "Effect": "Allow",
            "Action": [
                "application-autoscaling:DescribeScalableTargets",
                "autoscaling:DescribeAutoScalingGroups",
                "backup:DescribeBackupVault",
                "backup:GetBackupPlan",
                "backup:GetBackupSelection",
                "backup:ListBackupPlans",
                "backup:ListBackupSelections",
                "cloudformation:DescribeStacks",
                "cloudformation:ListStackResources",
                "cloudformation:ValidateTemplate",
                "cloudwatch:DescribeAlarms",
                "cloudwatch:GetMetricData",
                "cloudwatch:GetMetricStatistics",
                "datasync:DescribeTask",
                "datasync:ListLocations",
                "datasync:ListTasks",
                "devops-guru:ListMonitoredResources",
                "dlm:GetLifecyclePolicies",
                "dlm:GetLifecyclePolicy",
                "docdb-elastic:GetCluster",
                "docdb-elastic:GetClusterSnapshot",
                "docdb-elastic:ListClusterSnapshots",
                "docdb-elastic:ListTagsForResource",
                "drs:DescribeJobs",
                "drs:DescribeSourceServers",
                "drs:GetReplicationConfiguration",
                "ds:DescribeDirectories",
                "dynamodb:DescribeContinuousBackups",
```

```
                "dynamodb:DescribeGlobalTable",
                "dynamodb:DescribeLimits",
                "dynamodb:DescribeTable",
                "dynamodb:ListGlobalTables",
                "dynamodb:ListTagsOfResource",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeFastSnapshotRestores",
                "ec2:DescribeFleets",
                "ec2:DescribeHosts",
                "ec2:DescribeInstances",
                "ec2:DescribeNatGateways",
                "ec2:DescribePlacementGroups",
                "ec2:DescribeRegions",
                "ec2:DescribeSnapshots",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeVolumes",
                "ec2:DescribeVpcEndpoints",
                "ecr:DescribeRegistry",
                "ecs:DescribeCapacityProviders",
                "ecs:DescribeClusters",
                "ecs:DescribeContainerInstances",
                "ecs:DescribeServices",
                "ecs:DescribeTaskDefinition",
                "ecs:ListContainerInstances",
                "ecs:ListServices",
                "eks:DescribeCluster",
                "eks:DescribeFargateProfile",
                "eks:DescribeNodegroup",
                "eks:ListFargateProfiles",
                "eks:ListNodegroups",
                "elasticache:DescribeCacheClusters",
                "elasticache:DescribeGlobalReplicationGroups",
                "elasticache:DescribeReplicationGroups",
                "elasticache:DescribeServerlessCaches",
                "elasticahce:DescribeServerlessCacheSnapshots",
                "elasticache:DescribeSnapshots",
                "elasticfilesystem:DescribeFileSystems",
                "elasticfilesystem:DescribeLifecycleConfiguration",
                "elasticfilesystem:DescribeMountTargets",
                "elasticfilesystem:DescribeReplicationConfigurations",
                "elasticloadbalancing:DescribeListeners",
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticloadbalancing:DescribeTargetGroups",
```

```
                "elasticloadbalancing:DescribeTargetHealth",
                "fis:GetExperiment",
                "fis:GetExperimentTemplate",
                "fis:ListExperiments",
                "fis:ListExperimentResolvedTargets",
                "fis:ListExperimentTemplates",
                "fsx:DescribeFileSystems",
                "lambda:GetFunctionConcurrency",
                "lambda:GetFunctionConfiguration",
                "lambda:ListAliases",
                "lambda:ListEventSourceMappings",
                "lambda:ListFunctionEventInvokeConfigs",
                "lambda:ListVersionsByFunction",
                "rds:DescribeDBClusterSnapshots",
                "rds:DescribeDBClusters",
                "rds:DescribeDBInstanceAutomatedBackups",
                "rds:DescribeDBInstances",
                "rds:DescribeDBProxies",
                "rds:DescribeDBProxyTargets",
                "rds:DescribeDBSnapshots",
                "rds:DescribeGlobalClusters",
                "rds:ListTagsForResource",
                "resource-groups:GetGroup",
                "resource-groups:ListGroupResources",
                "route53-recovery-control-config:ListClusters",
                "route53-recovery-control-config:ListControlPanels",
                "route53-recovery-control-config:ListRoutingControls",
                "route53-recovery-readiness:GetReadinessCheckStatus",
                "route53-recovery-readiness:GetResourceSet",
                "route53-recovery-readiness:ListReadinessChecks",
                "route53:GetHealthCheck",
                "route53:ListHealthChecks",
                "route53:ListHostedZones",
                "route53:ListResourceRecordSets",
                "route53resolver:ListResolverEndpoints",
                "route53resolver:ListResolverEndpointIpAddresses",
                "s3:ListBucket",
                "servicecatalog:GetApplication",
                "servicecatalog:ListAssociatedResources",
                "sns:GetSubscriptionAttributes",
                "sns:GetTopicAttributes",
                "sns:ListSubscriptionsByTopic",
                "sqs:GetQueueAttributes",
                "sqs:GetQueueUrl",
```

```
                "ssm:DescribeAutomationExecutions",
                "states:DescribeStateMachine",
                "states:ListStateMachineVersions",
                "states:ListStateMachineAliases",
                "tag:GetResources"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AWSResilienceHubApiGatewayStatement",
            "Effect": "Allow",
            "Action": [
                "apigateway:GET"
            ],
            "Resource": [
                "arn:aws:apigateway:*::/apis/*",
                "arn:aws:apigateway:*::/restapis/*",
                "arn:aws:apigateway:*::/usageplans"
            ]
        },
        {
            "Sid": "AWSResilienceHubS3ArtifactStatement",
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:PutObject",
                "s3:GetObject"
            ],
            "Resource": "arn:aws:s3:::aws-resilience-hub-artifacts-*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
        },
        {
            "Sid": "AWSResilienceHubS3AccessStatement",
            "Effect": "Allow",
            "Action": [
                "s3:GetBucketLocation",
                "s3:GetBucketLogging",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketTagging",
```

```
                "s3:GetBucketVersioning",
                "s3:GetMultiRegionAccessPointRoutes",
                "s3:GetReplicationConfiguration",
                "s3:ListAllMyBuckets",
                "s3:ListMultiRegionAccessPoints"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
        },
        {
            "Sid": "AWSResilienceHubCloudWatchStatement",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": "ResilienceHub"
                }
            }
        },
        {
            "Sid": "AWSResilienceHubSSMStatement",
            "Effect": "Allow",
            "Action": [
                "ssm:GetParametersByPath"
            ],
            "Resource": "arn:aws:ssm:*:*:parameter/ResilienceHub/*"
        }
    ]
}
```

AWS Resilience Hub mises à jour des politiques AWS gérées

Consultez les détails des mises à jour des politiques AWS gérées AWS Resilience Hub 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 Historique du AWS Resilience Hub document.

Modification	Description	Date
AWSResilienceHubAssessmentExecutionPolicy—Modification	AWS Resilience Hub a mis à jour le `AWSResilienceHubAsssessmentExecutionPolicy` to grant `List` et `Get` les autorisations pour vous permettre d'accéder aux expériences AWS FIS lors de l'exécution des évaluations.	17 décembre 2024
AWSResilienceHubAssessmentExecutionPolicy—Modification	AWS Resilience Hub a mis `AWSResilienceHubAssessmentExecutionPolicy` à jour le pour accorder `Describe` des autorisations vous permettant d'accéder aux ressources et aux configurations sur Amazon ElastiCache (Redis OSS) Serverless lors de l'exécution d'évaluations.	25 septembre 2024
AWSResilienceHubAssessmentExecutionPolicy—Modification	AWS Resilience Hub a mis `AWSResilienceHubAssessmentExecutionPolicy` à jour le pour vous accorder `Describe` des autorisations vous permettant d'accéder aux ressources et aux configurations sur Amazon DocumentDB, Elastic Load Balancing et AWS	01 août 2024

Modification	Description	Date
	Lambda lors de l'exécution d'évaluations.	
AWSResilienceHubAssessmentExecutionPolicy—Modification	AWS Resilience Hub a mis `AWSResilienceHubAssessmentExecutionPolicy` à jour le pour accorder `Describe` des autorisations afin de vous permettre de lire la configuration du serveur de fichiers Amazon FSx pour Windows lors de l'exécution d'évaluations.	26 mars 2024
AWSResilienceHubAssessmentExecutionPolicy—Modification	AWS Resilience Hub a mis `AWSResilienceHubAssessmentExecutionPolicy` à jour le pour accorder `Describe` des autorisations vous permettant de lire la AWS Step Functions configuration lors de l'exécution des évaluations.	30 octobre 2023
AWSResilienceHubAssessmentExecutionPolicy—Modification	AWS Resilience Hub a mis `AWSResilienceHubAssessmentExecutionPolicy` à jour le pour accorder `Describe` des autorisations vous permettant d'accéder aux ressources sur Amazon RDS lors de l'exécution d'évaluations.	5 octobre 2023

Modification	Description	Date
AWSResilienceHubAssessmentExecutionPolicy—Nouveau	Cette AWS Resilience Hub politique donne accès à d'autres AWS services pour exécuter des évaluations.	26 juin 2023
AWS Resilience Hub a commencé à suivre les modifications	AWS Resilience Hub a commencé à suivre les modifications apportées AWS à ses politiques gérées.	15 juin 2023

AWS Resilience Hub référence aux personas et aux autorisations IAM

Vous pouvez accorder les autorisations IAM aux personnes avec lesquelles vous devez travailler AWS Resilience Hub en utilisant une politique `AWSResilienceHubAsssessmentExecutionPolicy` AWS gérée et l'une des politiques spécifiques aux personnes suivantes. Pour plus d'informations sur les politiques AWS gérées, consultezthe section called "AWSResilienceHubAsssessmentExecutionPolicy".

Politiques relatives aux personnes suggérées par AWS Resilience Hub :

- Autorisations IAM pour le responsable des applications d'infrastructure persona
- Permissions IAM pour le responsable de la continuité des activités
- Autorisations IAM pour le propriétaire de l'application
- Autorisations IAM pour accorder un accès en lecture seule

Autorisations IAM pour le responsable des applications d'infrastructure persona

La politique suivante accorde les autorisations nécessaires requises pour le personnage du gestionnaire d'applications d'infrastructure.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "InfrastructureApplicationManager",
      "Effect": "Allow",
```

```
      "Action": [
        "resiliencehub:AddDraftAppVersionResourceMappings",
        "resiliencehub:CreateAppVersionAppComponent",
        "resiliencehub:CreateAppVersionResource",
        "resiliencehub:CreateRecommendationTemplate",
        "resiliencehub:DeleteAppAssessment",
        "resiliencehub:DeleteAppInputSource",
        "resiliencehub:DeleteAppVersionAppComponent",
        "resiliencehub:DeleteAppVersionResource",
        "resiliencehub:DeleteRecommendationTemplate",
        "resiliencehub:Describe*",
        "resiliencehub:List*",
        "resiliencehub:PublishAppVersion",
        "resiliencehub:PutDraftAppVersionTemplate",
        "resiliencehub:RemoveDraftAppVersionResourceMappings",
        "resiliencehub:ResolveAppVersionResources",
        "resiliencehub:StartAppAssessment",
        "resiliencehub:TagResource",
        "resiliencehub:UntagResource",
        "resiliencehub:UpdateAppVersion",
        "resiliencehub:UpdateAppVersionAppComponent",
        "resiliencehub:UpdateAppVersionResource"
      ],
      "Resource": "*"
    }
  ]
}
```

Permissions IAM pour le responsable de la continuité des activités

La politique suivante accorde les autorisations nécessaires requises pour le personnage du responsable de la continuité des activités.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "BusinessContinuityManager",
      "Effect": "Allow",
      "Action": [
        "resiliencehub:CreateResiliencyPolicy",
        "resiliencehub:DeleteResiliencyPolicy",
        "resiliencehub:Describe*",
```

```
        "resiliencehub:List*",
        "resiliencehub:ResolveAppVersionResources",
        "resiliencehub:TagResource",
        "resiliencehub:UntagResource",
        "resiliencehub:UpdateAppVersion",
        "resiliencehub:UpdateAppVersionAppComponent",
        "resiliencehub:UpdateAppVersionResource",
        "resiliencehub:UpdateResiliencyPolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

Autorisations IAM pour le propriétaire de l'application

La politique suivante accorde les autorisations nécessaires requises pour le personnage du propriétaire de l'application.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ApplicationOwner",
      "Effect": "Allow",
      "Action": [
        "resiliencehub:AddDraftAppVersionResourceMappings",
        "resiliencehub:BatchUpdateRecommendationStatus",
        "resiliencehub:CreateApp",
        "resiliencehub:CreateAppVersionAppComponent",
        "resiliencehub:CreateAppVersionResource",
        "resiliencehub:CreateRecommendationTemplate",
        "resiliencehub:CreateResiliencyPolicy",
        "resiliencehub:DeleteApp",
        "resiliencehub:DeleteAppAssessment",
        "resiliencehub:DeleteAppInputSource",
        "resiliencehub:DeleteAppVersionAppComponent",
        "resiliencehub:DeleteAppVersionResource",
        "resiliencehub:DeleteRecommendationTemplate",
        "resiliencehub:DeleteResiliencyPolicy",
        "resiliencehub:Describe*",
        "resiliencehub:ImportResourcesToDraftAppVersion",
        "resiliencehub:List*",
```

```
        "resiliencehub:PublishAppVersion",
        "resiliencehub:PutDraftAppVersionTemplate",
        "resiliencehub:RemoveDraftAppVersionResourceMappings",
        "resiliencehub:ResolveAppVersionResources",
        "resiliencehub:StartAppAssessment",
        "resiliencehub:TagResource",
        "resiliencehub:UntagResource",
        "resiliencehub:UpdateApp",
        "resiliencehub:UpdateAppVersion",
        "resiliencehub:UpdateAppVersionAppComponent",
        "resiliencehub:UpdateAppVersionResource",
        "resiliencehub:UpdateResiliencyPolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

Autorisations IAM pour accorder un accès en lecture seule

La politique suivante accorde les autorisations nécessaires pour l'accès en lecture seule.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ReadOnly",
      "Effect": "Allow",
      "Action": [
        "resiliencehub:Describe*",
        "resiliencehub:List*",
        "resiliencehub:ResolveAppVersionResources"
      ],
      "Resource": "*"
    }
  ]
}
```

Importation du fichier d'état Terraform dans AWS Resilience Hub

AWS Resilience Hub prend en charge l'importation de fichiers d'état Terraform chiffrés à l'aide du chiffrement côté serveur (SSE) avec des clés gérées par Amazon Simple Storage Service (SSE-

S3) ou des clés gérées (SSE-KMS). AWS Key Management Service Si vos fichiers d'état Terraform sont chiffrés à l'aide de clés de chiffrement fournies par le client (SSE-C), vous ne pourrez pas les importer à l'aide de. AWS Resilience Hub

L'importation de fichiers d'état Terraform dans AWS Resilience Hub un environnement nécessite les politiques IAM suivantes en fonction de l'emplacement de votre fichier d'état.

Importation de fichiers d'état Terraform à partir d'un compartiment Amazon S3 situé dans le compte principal

La politique de compartiment Amazon S3 et la politique IAM suivantes sont requises pour autoriser l'accès en AWS Resilience Hub lecture à vos fichiers d'état Terraform situés dans un compartiment Amazon S3 sur le compte principal.

- Politique de compartiment : politique de compartiment sur le compartiment Amazon S3 cible, situé dans le compte principal. Pour plus d'informations, consultez l'exemple suivant.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<primary-account>:role/<invoker-role-or-current-iam-
role>"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::<s3-bucket-name>/<path-to-state-file>"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<primary-account>:role/<invoker-role-or-current-iam-
role>"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::<s3-bucket-name>"
    }
  ]
}
```

- Politique d'identité : politique d'identité associée au rôle Invoker défini pour cette application, ou au rôle IAM AWS actuel AWS Resilience Hub sur le compte principal AWS . Pour plus d'informations, consultez l'exemple suivant.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::<s3-bucket-name>/<path-to-state-file>"
    },
    {
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::<s3-bucket-name>"
    }
  ]
}
```

> **Note**
>
> Si vous utilisez la politique `AWSResilienceHubAsssessmentExecutionPolicy` gérée, aucune `ListBucket` autorisation n'est requise.

> **Note**
>
> Si vos fichiers d'état Terraform sont chiffrés à l'aide de KMS, vous devez ajouter l'autorisation suivante`kms:Decrypt`.
>
> ```
> {
>  "Effect": "Allow",
>  "Action": [
>  "kms:Decrypt",
>  ],
>  "Resource": "<arn_of_kms_key>"
> }
> ```

Importation de fichiers d'état Terraform à partir d'un compartiment Amazon S3 situé dans un compte secondaire

- Politique de compartiment : politique de compartiment sur le compartiment Amazon S3 cible, situé dans l'un des comptes secondaires. Pour plus d'informations, consultez l'exemple suivant.

```
 {
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<primary-account>:role/<invoker-role-or-current-iam-
role>"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::<bucket-with-statefile-in-secondary-account>/<path-
to-state-file>"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<primary-account>:role/<invoker-role-or-current-iam-
role>"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::<bucket-with-statefile-in-secondary-account>"
    }
  ]
}
```

- Politique d'identité : politique d'identité associée au rôle de AWS compte, qui s'exécute AWS Resilience Hub sur le AWS compte principal. Pour plus d'informations, consultez l'exemple suivant.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<primary-account>:role/<invoker-role-or-current-iam-
role>"
```

```
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::<bucket-with-statefile-in-secondary-account>/<path-
to-state-file>"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<primary-account>:role/<invoker-role-or-current-iam-
role>"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::<bucket-with-statefile-in-secondary-account>"
    }
  ]
}
```

> **Note**
>
> Si vous utilisez la politique `AWSResilienceHubAsssessmentExecutionPolicy` gérée, aucune `ListBucket` autorisation n'est requise.

> **Note**
>
> Si vos fichiers d'état Terraform sont chiffrés à l'aide de KMS, vous devez ajouter l'autorisation suivante`kms:Decrypt`.
>
> ```
> {
>  "Effect": "Allow",
>  "Action": [
>  "kms:Decrypt",
>  ],
>  "Resource": "<arn_of_kms_key>"
> }
> ```

Permettre AWS Resilience Hub l'accès à votre cluster Amazon Elastic Kubernetes Service

AWS Resilience Hub évalue la résilience d'un cluster Amazon Elastic Kubernetes Service (Amazon EKS) en analysant l'infrastructure de votre cluster Amazon EKS. AWS Resilience Hub utilise la configuration du contrôle d'accès basé sur les rôles (RBAC) Kubernetes pour évaluer les autres charges de travail Kubernetes (K8s), qui sont déployées dans le cadre du cluster Amazon EKS. AWS Resilience Hub Pour interroger votre cluster Amazon EKS afin d'analyser et d'évaluer la charge de travail, vous devez effectuer les opérations suivantes :

- Créez ou utilisez un rôle AWS Identity and Access Management (IAM) existant dans le même compte que le cluster Amazon EKS.
- Activez l'accès des utilisateurs et des rôles IAM à votre cluster Amazon EKS et accordez des autorisations supplémentaires en lecture seule aux ressources K8s au sein du cluster Amazon EKS. Pour plus d'informations sur l'activation de l'accès des utilisateurs et des rôles IAM à votre cluster Amazon EKS, consultez Activation de l'accès des utilisateurs et des rôles IAM à votre cluster - Amazon EKS.

L'accès à votre cluster Amazon EKS à l'aide d'entités IAM est activé par l'authentificateur AWS IAM pour Kubernetes, qui s'exécute sur le plan de contrôle Amazon EKS. L'authentificateur obtient les informations de configuration auprès de. `aws-auth ConfigMap`

> **Note**
>
> - Pour plus d'informations sur tous les `aws-auth ConfigMap` paramètres, voir Format de configuration complet sur GitHub.
> - Pour plus d'informations sur les différentes identités IAM, consultez la section Identités (utilisateurs, groupes et rôles) dans le guide de l'utilisateur IAM.
> - Pour plus d'informations sur la configuration du contrôle d'accès basé sur les rôles (RBAC) de Kubernetes, consultez la section Utilisation de l'autorisation RBAC.

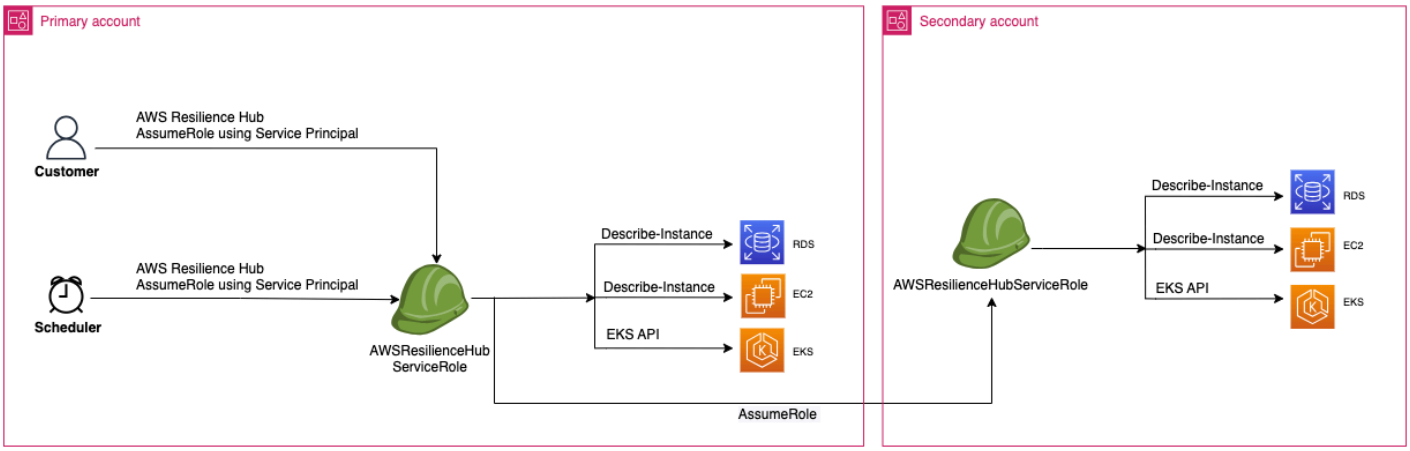
AWS Resilience Hub interroge les ressources de votre cluster Amazon EKS à l'aide d'un rôle IAM dans votre compte. Pour accéder AWS Resilience Hub aux ressources de votre cluster Amazon EKS, le rôle IAM utilisé par AWS Resilience Hub doit être mappé à un groupe Kubernetes disposant

d'autorisations en lecture seule suffisantes pour accéder aux ressources de votre cluster Amazon EKS.

AWS Resilience Hub permet d'accéder aux ressources de votre cluster Amazon EKS en utilisant l'une des options de rôle IAM suivantes :

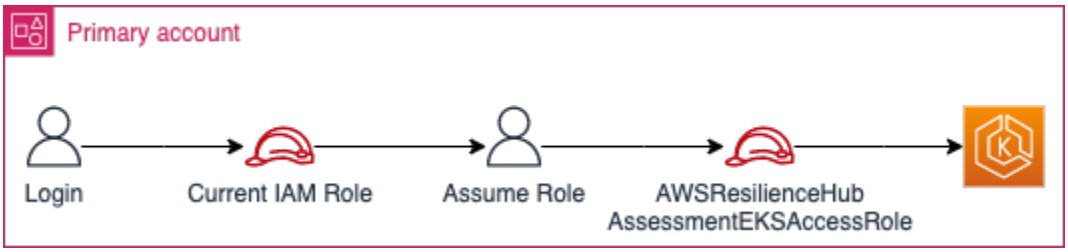
- Si votre application est configurée pour utiliser un accès basé sur les rôles pour accéder aux ressources, le rôle d'invocateur ou le rôle de compte secondaire transmis AWS Resilience Hub lors de la création d'une application sera utilisé pour accéder à votre cluster Amazon EKS lors de l'évaluation.

  Le schéma conceptuel suivant montre comment AWS Resilience Hub accéder aux clusters Amazon EKS lorsque l'application est configurée en tant qu'application basée sur des rôles.

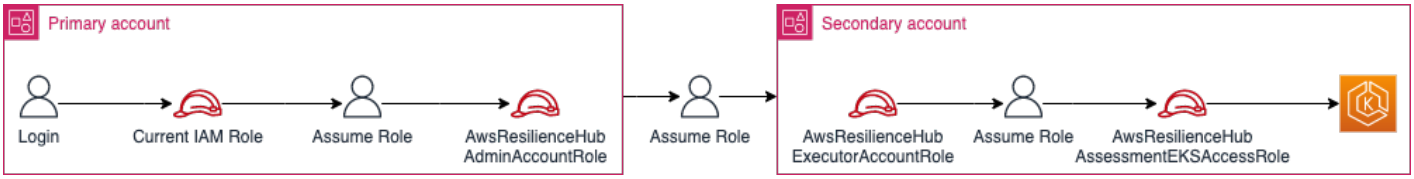


- Si votre application est configurée pour utiliser l'utilisateur IAM actuel pour accéder aux ressources, vous devez créer un nouveau rôle IAM dont le nom figure `AwsResilienceHubAssessmentEKSAccessRole` dans le même compte que celui du cluster Amazon EKS. Ce rôle IAM sera ensuite utilisé pour accéder à votre cluster Amazon EKS.

  Le schéma conceptuel suivant montre comment AWS Resilience Hub accéder aux clusters Amazon EKS déployés dans votre compte principal lorsque l'application est configurée pour utiliser les autorisations utilisateur IAM actuelles.



Le schéma conceptuel suivant montre comment AWS Resilience Hub accéder aux clusters Amazon EKS déployés sur un compte secondaire lorsque l'application est configurée pour utiliser les autorisations utilisateur IAM actuelles.



Octroi de l' AWS Resilience Hub accès aux ressources de votre cluster Amazon EKS

AWS Resilience Hub vous permet d'accéder aux ressources situées sur les clusters Amazon EKS à condition que vous ayez configuré les autorisations requises.

Pour accorder les autorisations nécessaires à la découverte et AWS Resilience Hub à l'évaluation des ressources au sein du cluster Amazon EKS

1. Configurez un rôle IAM pour accéder au cluster Amazon EKS.

   Si vous avez configuré votre application à l'aide d'un accès basé sur les rôles, vous pouvez ignorer cette étape et passer à l'étape 2 et utiliser le rôle que vous avez utilisé pour créer l'application. Pour plus d'informations sur l' AWS Resilience Hub utilisation des rôles IAM, consultezthe section called "Comment AWS Resilience Hub fonctionne avec IAM".

   Si vous avez configuré votre application à l'aide des autorisations utilisateur IAM actuelles, vous devez créer le rôle `AwsResilienceHubAssessmentEKSAccessRole` IAM dans le même compte que celui du cluster Amazon EKS. Ce rôle IAM sera ensuite utilisé lors de l'accès à votre cluster Amazon EKS.

   Lors de l'importation et de l'évaluation de votre application, AWS Resilience Hub utilise un rôle IAM pour accéder aux ressources de votre cluster Amazon EKS. Ce rôle doit être créé dans le même compte que votre cluster Amazon EKS et il sera mappé à un groupe Kubernetes incluant les autorisations requises pour AWS Resilience Hub évaluer votre cluster Amazon EKS.

   Si votre cluster Amazon EKS se trouve sur le même compte que le compte d' AWS Resilience Hub appel, le rôle doit être créé selon la politique de confiance IAM suivante. Dans cette politique de confiance IAM, `caller_IAM_role` il est utilisé dans le compte courant pour appeler le APIs for AWS Resilience Hub.

> **Note**
>
> `caller_IAM_role`Il s'agit du rôle associé à votre compte AWS utilisateur.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::eks_cluster_account_id:role/caller_IAM_role"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Si votre cluster Amazon EKS se trouve sur un compte croisé (un compte différent du compte d' AWS Resilience Hub appel), vous devez créer le rôle `AwsResilienceHubAssessmentEKSAccessRole` IAM en appliquant la politique de confiance IAM suivante :

> **Note**
>
> Comme condition préalable, pour accéder au cluster Amazon EKS déployé dans un compte différent de celui de l' AWS Resilience Hub utilisateur, vous devez configurer l'accès multicompte. Pour plus d'informations, veuillez consulter la rubrique

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::eks_cluster_account_id:role/
AwsResilienceHubExecutorRole"
      },
```

```
      "Action": "sts:AssumeRole"
    }
  ]
}
```

2. Créez `ClusterRole` et/ou des `ClusterRoleBinding` rôles pour AWS Resilience Hub l'application. `RoleBinding`

   Création `ClusterRole` et `ClusterRoleBinding` octroi des autorisations de lecture seule requises AWS Resilience Hub pour analyser et évaluer les ressources faisant partie de certains espaces de noms de votre cluster Amazon EKS.

   AWS Resilience Hub vous permet de limiter son accès à vos espaces de noms pour générer des évaluations de résilience en effectuant l'une des opérations suivantes :

   a. Accordez un accès en lecture à tous les espaces de noms à AWS Resilience Hub l'application.

      AWS Resilience Hub Pour évaluer la résilience des ressources dans tous les espaces de noms d'un cluster Amazon EKS, vous devez créer les éléments suivants `ClusterRole` et. `ClusterRoleBinding`

      - `resilience-hub-eks-access-cluster-role`(`ClusterRole`) — Définit les autorisations requises AWS Resilience Hub pour évaluer votre cluster Amazon EKS.
      - `resilience-hub-eks-access-cluster-role-binding`(`ClusterRoleBinding`) — Définit un groupe nommé `resilience-hub-eks-access-group` dans votre cluster Amazon EKS qui accorde à ses utilisateurs les autorisations requises pour effectuer des évaluations de résilience dans AWS Resilience Hub.

      Le modèle permettant d'accorder un accès en lecture à tous les espaces de noms à AWS Resilience Hub l'application est le suivant :

```
cat << EOF | kubectl apply -f -
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: resilience-hub-eks-access-cluster-role
rules:
- apiGroups:
```

```
    - ""
  resources:
    - pods
    - replicationcontrollers
    - nodes
  verbs:
    - get
    - list
- apiGroups:
    - apps
  resources:
    - deployments
    - replicasets
  verbs:
    - get
    - list
- apiGroups:
    - policy
  resources:
    - poddisruptionbudgets
  verbs:
    - get
    - list
- apiGroups:
    - autoscaling.k8s.io
  resources:
    - verticalpodautoscalers
  verbs:
    - get
    - list
- apiGroups:
    - autoscaling
  resources:
    - horizontalpodautoscalers
  verbs:
    - get
    - list
- apiGroups:
    - karpenter.sh
  resources:
    - provisioners
    - nodepools
  verbs:
    - get
```

```
    - list
- apiGroups:
    - karpenter.k8s.aws
  resources:
    - awsnodetemplates
    - ec2nodeclasses
  verbs:
    - get
    - list
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: resilience-hub-eks-access-cluster-role-binding
subjects:
  - kind: Group
    name: resilience-hub-eks-access-group
    apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
  name: resilience-hub-eks-access-cluster-role
  apiGroup: rbac.authorization.k8s.io
---
EOF
```

b. Octroi AWS Resilience Hub de l'accès à la lecture d'espaces de noms spécifiques.

Vous pouvez limiter AWS Resilience Hub l'accès aux ressources au sein d'un ensemble spécifique d'espaces de noms en utilisant`RoleBinding`. Pour ce faire, vous devez créer les rôles suivants :

- `ClusterRole`— Pour accéder AWS Resilience Hub aux ressources dans des espaces de noms spécifiques au sein d'un cluster Amazon EKS et évaluer sa résilience, vous devez créer les rôles suivants`ClusterRole`.
  - `resilience-hub-eks-access-cluster-role`— Spécifie les autorisations nécessaires pour évaluer les ressources au sein d'espaces de noms spécifiques.
  - `resilience-hub-eks-access-global-cluster-role`— Spécifie les autorisations nécessaires pour évaluer les ressources délimitées au cluster, qui ne sont pas associées à un espace de noms spécifique, au sein de vos clusters Amazon EKS. AWS Resilience Hub nécessite des autorisations pour accéder aux ressources

délimitées au cluster (telles que les nœuds) sur votre cluster Amazon EKS afin d'évaluer la résilience de votre application.

Le modèle pour créer un `ClusterRole` rôle est le suivant :

```
cat << EOF | kubectl apply -f -
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: resilience-hub-eks-access-cluster-role
rules:
  - apiGroups:
      - ""
    resources:
      - pods
      - replicationcontrollers
    verbs:
      - get
      - list
  - apiGroups:
      - apps
    resources:
      - deployments
      - replicasets
    verbs:
      - get
      - list
  - apiGroups:
      - policy
    resources:
      - poddisruptionbudgets
    verbs:
      - get
      - list
  - apiGroups:
      - autoscaling.k8s.io
    resources:
      - verticalpodautoscalers
    verbs:
      - get
      - list
  - apiGroups:
```

```
      - autoscaling
    resources:
      - horizontalpodautoscalers
    verbs:
      - get
      - list

---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: resilience-hub-eks-access-global-cluster-role
rules:
  - apiGroups:
      - ""
    resources:
      - nodes
    verbs:
      - get
      - list
  - apiGroups:
      - karpenter.sh
    resources:
      - provisioners
      - nodepools
    verbs:
      - get
      - list
  - apiGroups:
      - karpenter.k8s.aws
    resources:
      - awsnodetemplates
      - ec2nodeclasses
    verbs:
      - get
      - list

---
EOF
```

- `RoleBinding`rôle — Ce rôle accorde les autorisations requises pour accéder AWS Resilience Hub aux ressources dans des espaces de noms spécifiques. En d'autres

termes, vous devez créer un `RoleBinding` rôle dans chaque espace de noms pour permettre d'accéder AWS Resilience Hub aux ressources de l'espace de noms donné.

> **Note**
>
> Si vous utilisez `ClusterAutoscaler` pour la mise à l'échelle automatique, vous devez également créer `RoleBinding` dans le`kube-system`. Cela est nécessaire pour évaluer votre`ClusterAutoscaler`, qui fait partie de l'espace de `kube-system` noms.
> Ce faisant, vous accorderez AWS Resilience Hub les autorisations requises pour évaluer les ressources au sein de l'espace de `kube-system` noms lors de l'évaluation de votre cluster Amazon EKS.

Le modèle pour créer un `RoleBinding` rôle est le suivant :

```
cat << EOF | kubectl apply -f -
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  name: resilience-hub-eks-access-cluster-role-binding
  namespace: <namespace>
subjects:
  - kind: Group
    name: resilience-hub-eks-access-group
    apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
  name: resilience-hub-eks-access-cluster-role
  apiGroup: rbac.authorization.k8s.io

---
EOF
```

- `ClusterRoleBinding`rôle — Ce rôle accorde les autorisations requises pour accéder AWS Resilience Hub aux ressources délimitées au cluster.

  Le modèle pour créer un `ClusterRoleBinding` rôle est le suivant :

```
cat << EOF | kubectl apply -f -
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: resilience-hub-eks-access-global-cluster-role-binding
subjects:
  - kind: Group
    name: resilience-hub-eks-access-group
    apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
  name: resilience-hub-eks-access-global-cluster-role
  apiGroup: rbac.authorization.k8s.io

---
EOF
```

3. Mettez à jour le `aws-auth ConfigMap` pour le mapper `resilience-hub-eks-access-group` avec le rôle IAM utilisé pour accéder au cluster Amazon EKS.

   Cette étape crée un mappage entre le rôle IAM utilisé à l'étape 1 et le groupe Kubernetes créé à l'étape 2. Ce mappage accorde des autorisations aux rôles IAM pour accéder aux ressources du cluster Amazon EKS.

   > **Note**
   >
   > - `ROLE-NAME`fait référence au rôle IAM utilisé pour accéder au cluster Amazon EKS.
   > - Si votre application est configurée pour utiliser l'accès basé sur les rôles, le rôle doit être soit le rôle d'invocateur, soit le rôle de compte secondaire transmis AWS Resilience Hub lors de la création de l'application.
   > - Si votre application est configurée pour utiliser l'utilisateur IAM actuel pour accéder aux ressources, il doit s'agir du`AwsResilienceHubAssessmentEKSAccessRole`.
   >
   > - `ACCOUNT-ID`doit être l'ID de AWS compte du cluster Amazon EKS.

Vous pouvez créer le `aws-auth ConfigMap` en utilisant l'une des méthodes suivantes :

- Utiliser `eksctl`

  Utilisez la commande suivante pour mettre à jour `aws-auth ConfigMap` :

  ```
  eksctl create iamidentitymapping \
   --cluster <cluster-name> \
   --region=<region-code> \
   --arn arn:aws:iam::<ACCOUNT-ID>:role/<ROLE-NAME>\
   --group resilience-hub-eks-access-group \
   --username AwsResilienceHubAssessmentEKSAccessRole
  ```

- Vous pouvez les modifier manuellement `aws-auth ConfigMap` en ajoutant les détails du rôle IAM dans la `mapRoles ConfigMap` section des données sous-jacentes. Utilisez la commande suivante pour modifier le `aws-authConfigMap`.

  ```
  kubectl edit -n kube-system configmap/aws-auth
  ```

  `mapRolescette` section comprend les paramètres suivants :

  - `rolearn`— Le nom de ressource Amazon (ARN) du rôle IAM à ajouter.
    - Syntaxe ARN —`arn:aws:iam::<ACCOUNT-ID>:role/<ROLE-NAME>`.
  - `username`— Le nom d'utilisateur dans Kubernetes à associer au rôle IAM (). `AwsResilienceHubAssessmentEKSAccessRole`
  - `groups`— Les noms des groupes doivent correspondre aux noms des groupes créés à l'étape 2 (`resilience-hub-eks-access-group`).

  > **Note**
  >
  > Si `mapRoles` la section n'existe pas, vous devez l'ajouter manuellement.

  Utilisez le modèle suivant pour ajouter les détails du rôle IAM à la `mapRoles ConfigMap` section des données sous-jacentes.

  ```
    - groups:
      - resilience-hub-eks-access-group
      rolearn: arn:aws:iam::<ACCOUNT-ID>:role/<ROLE-NAME>
  ```

```
        username: AwsResilienceHubAssessmentEKSAccessRole
```

Activation AWS Resilience Hub de la publication de sujets sur votre Amazon Simple Notification Service

Cette section explique comment activer la publication AWS Resilience Hub de notifications concernant l'application sur vos rubriques Amazon Simple Notification Service (Amazon SNS). Pour envoyer des notifications à une rubrique Amazon SNS, assurez-vous que vous disposez des éléments suivants :

- Une AWS Resilience Hub application active.
- Rubrique Amazon SNS existante à laquelle vous AWS Resilience Hub devez envoyer des notifications. Pour plus d'informations sur la création d'une rubrique Amazon SNS, consultez Création d'une rubrique Amazon SNS.

AWS Resilience Hub Pour permettre de publier des notifications sur votre rubrique Amazon SNS, vous devez mettre à jour la politique d'accès de la rubrique Amazon SNS avec les éléments suivants :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowResilienceHubPublish",
      "Effect": "Allow",
      "Principal": {
        "Service": "resiliencehub.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:account-id:topic-name"
    }
  ]
}
```

> **Note**
>
> Lorsque vous publiez des messages provenant de régions facultatives vers des sujets situés dans des régions activées par défaut, vous devez modifier la politique de

ressources créée pour le sujet Amazon SNS. AWS Resilience Hub Modifiez la valeur du principal de `resiliencehub.amazonaws.com` à`resiliencehub.<opt-in-region>.amazonaws.com`.

Si vous utilisez une rubrique Amazon SNS chiffrée côté serveur (SSE), vous devez vous assurer qu' AWS Resilience Hub elle dispose de l'accès `Decrypt` et `GenerateDataKey` * à la clé de chiffrement Amazon SNS.

Pour fournir la politique d'autorisation d'`GenerateDataKey*`accès suivante `Decrypt` et y accéder AWS Resilience Hub, vous devez inclure les autorisations d' AWS Key Management Service accès suivantes.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowResilienceHubDecrypt",
      "Effect": "Allow",
      "Principal": {
        "Service": "resiliencehub.amazonaws.com"
      },
      "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
      ],
      "Resource": "arn:aws:kms:region:account-id:key/key-id"
    }
  ]
}
```

Limiter les autorisations pour inclure ou exclure AWS Resilience Hub des recommandations

AWS Resilience Hub vous permet de restreindre les autorisations permettant d'inclure ou d'exclure des recommandations par application. Vous pouvez restreindre les autorisations pour inclure ou exclure des recommandations par application en utilisant la politique de confiance IAM suivante. Dans cette politique de confiance IAM, `caller_IAM_role` (associée à votre compte AWS utilisateur) est utilisée dans le compte courant pour appeler le APIs for AWS Resilience Hub.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "resiliencehub:BatchUpdateRecommendationStatus",
      "Resource": "arn:aws:resiliencehub:us-west-2:12345678900:app/0e6237b7-23ba-4103-
adb2-91811326b703"
    }
  ]
}
```

Sécurité de l'infrastructure dans AWS Resilience Hub

En tant que service géré, AWS Resilience Hub il est protégé par les procédures de sécurité du réseau AWS mondial décrites dans le white paper Amazon Web Services : Overview of Security Processes.

Vous utilisez des appels d'API AWS publiés pour accéder AWS Resilience Hub via le réseau. Les clients doivent prendre en charge le protocole TLS (Transport Layer Security) 1.2 ou version ultérieure. Nous recommandons TLS 1.3 ou version ultérieure. Les clients doivent aussi prendre en charge les suites de chiffrement PFS (Perfect Forward Secrecy) comme Ephemeral Diffie-Hellman (DHE) ou Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un principal IAM. Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

Contrôles de résilience pour les AWS services

Ce chapitre fournit les détails des différents contrôles de résilience effectués par AWS Resilience Hub les AWS services pris en charge afin de garantir que les postures de résilience des applications ne sont pas affectées. Ces contrôles estiment l'objectif de temps de restauration (RTO) et l'objectif du point de reprise (RPO) par rapport aux valeurs définies dans la politique de résilience pour chaque composant d'application (AppComponent). Les évaluations portent sur différents types de perturbations, à savoir les défaillances d'applications, d'infrastructure, les pannes d'AZ et les défaillances régionales. Toutefois, pour exécuter ces vérifications, vous devez fournir les autorisations IAM pertinentes AWS Resilience Hub pour lui permettre d'accéder à vos ressources. Pour en savoir plus sur les autorisations IAM requises pour accéder AWS Resilience Hub à vos ressources et effectuer les contrôles de résilience décrits dans ce chapitre, consultezAWS politiques gérées pour AWS Resilience Hub.

AWS services

- Amazon Elastic File System
- Amazon Relational Database Service et Amazon Aurora
- Amazon Simple Storage Service
- Amazon DynamoDB
- Amazon Elastic Compute Cloud
- Amazon EBS
- AWS Lambda
- Amazon Elastic Kubernetes Service
- Amazon Simple Notification Service
- Amazon Simple Queue Service
- Amazon Elastic Container Service
- Elastic Load Balancing
- Amazon API Gateway
- Amazon DocumentDB
- Passerelle NAT
- Amazon Route 53

- Contrôleur Amazon Application Recovery (ARC)
- Serveur FSx de fichiers Amazon pour Windows
- AWS Step Functions
- Amazon ElastiCache (Redis OSS)

Amazon Elastic File System

Cette section répertorie tous les contrôles de résilience et les recommandations spécifiques à Amazon Elastic File System. Pour plus d'informations sur Amazon Elastic File System, consultez la documentation Amazon Elastic File System.

Type de système de fichiers

AWS Resilience Hub vérifie le type de système de fichiers : régional ou zone unique. Le type de système de fichiers affecte sa résilience en cas de perturbations de l'infrastructure ou de l'AZ. Pour plus d'informations sur les types de systèmes de fichiers, consultez Disponibilité et durabilité des systèmes de fichiers Amazon EFS.

Backup du système de fichiers

AWS Resilience Hub vérifie si un AWS Backup plan est défini pour le système de fichiers déployé. En outre, il vérifie si l'option de `Cross-Region` sauvegarde est activée, garantissant ainsi une couverture en cas de perturbations au niveau régional si votre police l'exige.

Réplication des données

AWS Resilience Hub vérifie si une réplication de données Amazon EFS régionale ou interrégionale est définie pour le système de fichiers déployé. La réplication des données Amazon EFS contribue à améliorer le RTO estimé et le RPO estimé au niveau de l'application, de l'infrastructure, de l'AZ et de la région. En outre, AWS Resilience Hub vérifie s'il est associé à un système intégré AWS Backup à la région pour permettre la résilience du système de fichiers en cas d'interruption de l'application.

Amazon Relational Database Service et Amazon Aurora

Cette section répertorie tous les contrôles de résilience et les recommandations spécifiques à Amazon Relational Database Service et Amazon Aurora. Pour plus d'informations sur Amazon

Relational Database Service et Amazon Aurora, consultez la documentation Amazon Relational Database Service.

Déploiement mono-AZ

AWS Resilience Hub vérifie si la base de données est déployée en tant qu'instance unique et, si elle est déterminée, elle indique qu'elle ne prend pas en charge l'instance secondaire et ne lit pas la réplique.

déploiement multi-AZ

AWS Resilience Hub vérifie si la base de données est déployée soit avec une instance secondaire, soit avec des répliques en lecture. Si la base de données est déployée avec une réplique en lecture, AWS Resilience Hub valide si elle est déployée dans une autre zone de disponibilité afin de permettre le basculement en cas d'interruption de la zone AZ.

Sauvegarde

AWS Resilience Hub vérifie si les fonctionnalités de sauvegarde suivantes sont appliquées sur une instance de base de données déployée.

- AWS Backup plan avec option de sauvegarde automatique
- AWS Backup plan avec copie de sauvegarde interrégionale si cela est requis par votre politique
- Instantanés manuels pour systèmes de sauvegarde tiers

Basculement entre régions

AWS Resilience Hub vérifie les objectifs RTO et RPO définis dans la politique de résilience pour se remettre des perturbations régionales. En outre, AWS Resilience Hub peut identifier les architectures interrégionales suivantes pour couvrir les perturbations régionales :

- Une sauvegarde régionale avec une copie d'un instantané interrégional
- Une réplique lue dans une autre région
- Une base de données globale Amazon Aurora avec un cluster secondaire dans une autre région
- Une base de données globale Amazon Aurora avec un cluster secondaire sans tête dans une autre région

Basculement régional plus rapide

AWS Resilience Hub vérifie les objectifs RTO et RPO définis dans la politique de résilience lors de perturbations de l'infrastructure ou de l'AZ. En outre, AWS Resilience Hub peut identifier les architectures régionales suivantes pour couvrir les perturbations liées aux applications, à l'infrastructure et à l'AZ :

- Une sauvegarde régionale
- Une réplique lue dans un AZ différent
- Un cluster Aurora avec une réplique en lecture dans un autre AZ
- Une instance multi-AZ d'Amazon Relational Database Service (Amazon RDS)
- Un cluster multi-AZ Amazon RDS
- Une instance unique d'Amazon RDS avec une réplique en lecture dans un autre AZ

Amazon Simple Storage Service

Cette section répertorie tous les contrôles de résilience et les recommandations spécifiques à Amazon Simple Storage Service (Amazon S3). Pour plus d'informations sur Amazon S3, consultez la documentation Amazon S3.

Gestion des versions

AWS Resilience Hub vérifie si un compartiment Amazon S3 est configuré avec le contrôle de version activé.

Sauvegarde planifiée

AWS Resilience Hub vérifie si un AWS Backup plan est défini pour le bucket Amazon Simple Storage Service (Amazon S3) déployé. En outre, il vérifie également si l'option de sauvegarde interrégionale est activée si votre police exige une couverture pour les perturbations au niveau régional.

Point-in-time rétablissement

AWS Resilience Hub vérifie si point-in-time la restauration (PITR) est requise par l'objectif RPO de votre politique de résilience. Cependant, la sauvegarde entre régions n'est pas prise en charge pour le PITR. Par conséquent, vous utilisez un AWS Backup plan planifié existant avec l'option de sauvegarde interrégionale activée, ou vous en créez un nouveau.

Réplication des données

AWS Resilience Hub vérifie si une réplication entre régions (SRR) et une réplication entre régions (CRR) sont définies pour le compartiment Amazon S3 déployé. La réplication des données Amazon S3 améliore le RTO estimé de la charge de travail et le RPO de charge de travail estimé au niveau de l'application, de l'infrastructure, de l'AZ et de la région. En outre, il protège également contre la suppression physique d'un objet, car la suppression d'une version d'objet n'est pas répliquée dans le compartiment Amazon S3 cible. En outre, en fonction des cibles RTO définies dans votre politique de résilience, AWS Resilience Hub vérifie si Amazon S3 Replication Time Control (S3 RTC) doit être activé ou non. Cette fonctionnalité facturable reproduit 99,99 % des objets du compartiment source en 15 minutes.

- AWS Backup plan avec option de sauvegarde automatique
- AWS Backup plan avec copie de sauvegarde interrégionale si cela est requis par votre politique
- Instantanés manuels pour systèmes de sauvegarde tiers

Amazon DynamoDB

Cette section répertorie tous les contrôles de résilience et les recommandations spécifiques à Amazon DynamoDB. Pour plus d'informations sur Amazon DynamoDB, consultez la documentation Amazon DynamoDB.

Sauvegarde planifiée

AWS Resilience Hub vérifie si une sauvegarde est déjà définie pour la table déployée. En outre, il vérifie également si la sauvegarde interrégionale doit être configurée conformément à votre politique si elle nécessite une couverture pour les perturbations au niveau régional.

Point-in-time rétablissement

AWS Resilience Hub vérifie si une point-in-time restauration (PITR) est requise conformément à l'objectif de RPO de votre politique de résilience. Cependant, la sauvegarde entre régions n'est pas prise en charge pour le PITR. Par conséquent, vous utilisez un AWS Backup plan planifié existant avec l'option de sauvegarde interrégionale activée, ou vous en créez un nouveau.

Tableau global

AWS Resilience Hub vérifie si la table Amazon DynamoDB déployée est définie comme une table globale avec une ou plusieurs répliques dans d'autres régions. La configuration de Global Table améliore le RTO estimé de la charge de travail et le RPO de charge de travail estimé au niveau de la région, et permet également de travailler en mode multirégional actif-actif ou actif-passif. AWS Backup ou Amazon DynamoDB PITR peut être utilisé dans l'une des régions pour gérer les interruptions d'application.

Amazon Elastic Compute Cloud

Cette section répertorie tous les contrôles de résilience et les recommandations spécifiques à Amazon Elastic Compute Cloud. Pour plus d'informations sur Amazon Elastic Compute Cloud, consultez la documentation Amazon Elastic Compute Cloud.

Instance dynamique

AWS Resilience Hub identifie une EC2 instance Amazon en tant qu'instance dynamique si l'un des critères suivants est rempli :

- Si `DeleteOnTermination` l'attribut est défini sur false pour au moins un volume Amazon Elastic Block Store (Amazon EBS) attaché à cette instance.
- Si Amazon Data Lifecycle Manager ou un AWS Backup plan est associé à l' EC2 instance Amazon ou à au moins un volume Amazon EBS.
- Il AWS Elastic Disaster Recovery est utilisé pour répliquer les volumes de stockage de vos EC2 instances Amazon.

> **Note**
>
> Si une EC2 instance Amazon ne répond à aucun des critères ci-dessus, AWS Resilience Hub traitez-la comme une EC2 instance Amazon apatride.

Groupes Auto Scaling

AWS Resilience Hub vérifie la présence d'un groupe d' EC2 instances Amazon apatrides. En cas de découverte, il est recommandé de l'orchestrer à l'aide de groupes Auto Scaling (ASG) avec une

configuration multi-AZ. Si un ASG existant est identifié, ARH vérifiera s'il est configuré sur plusieurs zones de disponibilité. Si l'ASG est également défini à l'aide d' EC2instances Amazon ponctuelles uniquement, il est recommandé d'augmenter sa capacité avec des EC2 instances Amazon à la demande afin d'améliorer la résilience lorsque les EC2 instances Amazon ponctuelles ne sont pas disponibles.

EC2 Flotte Amazon

AWS Resilience Hub identifie Amazon EC2 Fleet et vérifie s'il est défini comme un déploiement multi-AZ et s'il utilise uniquement des EC2 instances Amazon ponctuelles. La définition d'un déploiement multi-AZ d'Amazon EC2 Fleet améliorera sa résilience en cas d'interruption de service. L'ajout d'instances à la demande à un Amazon EC2 Fleet améliorera sa résilience lorsque les instances ponctuelles ne sont pas disponibles.

Amazon EBS

Cette section répertorie tous les contrôles de résilience et les recommandations spécifiques à Amazon EBS. Pour plus d'informations sur Amazon EBS, consultez la documentation Amazon EBS.

Sauvegarde planifiée

AWS Resilience Hub vérifie si l'un des éléments suivants ou les deux sont définis pour vos volumes Amazon EBS.

- Règle de sauvegarde pour un volume Amazon EBS spécifique attaché à votre EC2 instance Amazon.
- Règle de sauvegarde permettant de créer une AMI basée sur Amazon EBS sur votre instance Amazon. EC2
- Instantanés manuels pour les systèmes de sauvegarde tiers.

En outre, si votre police exige une couverture pour les perturbations au niveau régional, AWS Resilience Hub vérifiez si l'option de sauvegarde entre régions est activée dans votre règle de sauvegarde.

Sauvegarde et réplication des données

AWS Resilience Hub identifie un volume Amazon EBS et est considéré comme un volume dynamique si l'un des critères suivants est rempli :

- Si `DeleteOnTermination` l'attribut est défini sur false pour ce volume Amazon EBS.
- Si Amazon Data Lifecycle Manager ou un AWS Backup plan est associé à ce volume Amazon EBS ou à l' EC2 instance Amazon à laquelle il est attaché.
- Il AWS Elastic Disaster Recovery est utilisé pour répliquer les volumes de stockage de vos EC2 instances Amazon.

AWS Lambda

Cette section répertorie tous les contrôles de résilience et les recommandations spécifiques à AWS Lambda. Pour plus d'informations AWS Lambda, consultez AWS Lambda la documentation.

Client : Amazon VPC Access

AWS Resilience Hub identifie une AWS Lambda fonction connectée au VPC. La connexion AWS Lambda à des sous-réseaux situés dans différents AZs de votre Amazon VPC permet de garantir la résilience des fonctions en cas d'interruption de l'AZ.

File d'attente de lettres mortes

AWS Resilience Hub vérifie si une AWS Lambda fonction est associée à une file d'attente de lettres mortes (DLQ) pour stocker les demandes ayant échoué. L'attachement d'un DLQ au AWS Lambda fonctionnement permet d'éviter la perte de données des demandes et de réessayer de traiter les demandes ayant échoué ultérieurement.

Amazon Elastic Kubernetes Service

Cette section répertorie tous les contrôles de résilience et les recommandations spécifiques à Amazon Elastic Kubernetes Service (Amazon EKS). Pour plus d'informations sur Amazon EKS, consultez la documentation Amazon EKS.

déploiement multi-AZ

AWS Resilience Hub identifie si le déploiement du pod s'exécute sur plusieurs nœuds de travail AZs. Un cluster Amazon EKS supplémentaire dans une autre région est requis si votre politique de résilience exige une couverture en cas de perturbation régionale. Ce cluster Amazon EKS supplémentaire est également vérifié pour les déploiements de pods répartis entre plusieurs nœuds de travail. AZs

Déploiement vs. ReplicaSet

AWS Resilience Hub vérifie si vous utilisez des objets ReplicaSets ou des pods au lieu de les déployer. Le remplacement ReplicaSets des objets du module par le déploiement simplifie les mises à jour du module vers une nouvelle version du logiciel et inclut d'autres fonctionnalités utiles.

Maintenance du déploiement

AWS Resilience Hub vérifie si les meilleures pratiques suivantes sont utilisées pour le déploiement :

- Utilisation du budget de perturbation des pods (PDB) — L'utilisation du PDB permet d'améliorer la disponibilité en limitant le nombre de pods dans la charge de travail qui peuvent être interrompus à un moment donné.
- Remplacement des groupes de nœuds autogérés par des groupes de nœuds gérés par Amazon EKS : ce remplacement simplifie les mises à jour des images des nœuds de travail pendant la maintenance.
- Prise en charge des demandes dynamiques de processeur et de mémoire par déploiement : ces demandes aident Kubernetes à sélectionner un nœud adapté aux besoins d'un pod.
- Configuration des sondes de réactivité et de disponibilité pour tous les conteneurs — La configuration des sondes de réactivité permet d'améliorer la résilience en redémarrant les pods non fonctionnels. La configuration des sondes de disponibilité permet d'améliorer la disponibilité en détournant le trafic des modules bondés.
- Configuration de Karpenter, Cluster Autoscaler ou AWS Fargate — Ces configurations permettent à l'infrastructure du cluster Amazon EKS de se développer et de répondre aux demandes de charge de travail.
- Configuration de Horizontal Pod Autoscaler : cette configuration permet au cluster Amazon EKS de redimensionner automatiquement la charge de travail pour répondre à la demande de traitement des demandes.

Amazon Simple Notification Service

Cette section répertorie tous les contrôles de résilience et les recommandations spécifiques à Amazon Simple Notification Service (Amazon SNS). Pour plus d'informations sur Amazon SNS, consultez la documentation Amazon SNS.

Abonnements thématiques

AWS Resilience Hub vérifie si au moins un abonnement est associé à une rubrique Amazon SNS afin de s'assurer que les messages entrants ne sont pas perdus.

Amazon Simple Queue Service

Cette section répertorie tous les contrôles de résilience et les recommandations spécifiques à Amazon Simple Queue Service (Amazon SQS). Pour plus d'informations sur Amazon SQS, consultez la documentation Amazon SQS.

File d'attente de lettres mortes

AWS Resilience Hub vérifie si une DLQ est associée à la file d'attente Amazon SQS afin de gérer les messages qui ne peuvent pas être remis aux abonnés avec succès.

Amazon Elastic Container Service

Cette section répertorie tous les contrôles de résilience et les recommandations spécifiques à Amazon Elastic Container Service (Amazon ECS). Pour plus d'informations sur Amazon ECS, consultez la documentation Amazon ECS.

déploiement multi-AZ

AWS Resilience Hub vérifie si les tâches ou les services Amazon ECS s'exécutent en plusieurs en AZs fonction d'Amazon EC2 ou des types de AWS Fargate lancement. Un cluster Amazon ECS supplémentaire dans une autre région est requis si votre police nécessite une couverture en cas de perturbation régionale. Le cluster supplémentaire est également vérifié pour l'exécution de tâches ou de services en plusieurs fois AZs.

Elastic Load Balancing

Cette section répertorie tous les contrôles de résilience et les recommandations spécifiques à Elastic Load Balancing. Pour plus d'informations sur Elastic Load Balancing, consultez la documentation d'Elastic Load Balancing.

déploiement multi-AZ

AWS Resilience Hub vérifie si Elastic Load Balancing fonctionne en mode multiple AZs.

Un Elastic Load Balancing supplémentaire dans une autre région est requis si votre police nécessite une couverture en cas de perturbation régionale. L'Elastic Load Balancing supplémentaire, situé dans une autre région, est également vérifié pour son déploiement dans plusieurs régions AZs.

Amazon API Gateway

Cette section répertorie tous les contrôles de résilience et les recommandations spécifiques à Amazon API Gateway. Pour plus d'informations sur Amazon API Gateway, consultez la documentation Amazon API Gateway.

Déploiement entre régions

Si votre politique doit prendre en compte les perturbations régionales, AWS Resilience Hub nous vérifierons s'il existe un déploiement supplémentaire de la ressource API Amazon API Gateway dans une autre région.

Déploiement multi-AZ d'API privées

AWS Resilience Hub vérifie si votre API est définie comme privée dans Amazon API Gateway. Private APIs doit recevoir du trafic via le point de terminaison de l'interface Amazon VPC qui est déployé sur plusieurs. AZs

Amazon DocumentDB

Cette section répertorie toutes les vérifications et recommandations spécifiques à Amazon DocumentDB. Pour plus d'informations sur Amazon DocumentDB, consultez la documentation Amazon DocumentDB.

déploiement multi-AZ

AWS Resilience Hub vérifie si le cluster Amazon DocumentDB est déployé en plusieurs. AZs Un cluster Amazon DocumentDB secondaire supplémentaire est requis dans une autre région si votre contrat prévoit une couverture en cas de perturbations régionales. Le cluster Amazon DocumentDB supplémentaire, situé dans une autre région, est également vérifié pour son exécution en plusieurs. AZs

Déploiement en cluster élastique et multi-AZ

AWS Resilience Hub vérifie si les partitions du cluster Elastic Amazon DocumentDB utilisent des répliques de lecture déployées dans des environnements différents. AZs

Cluster élastique et instantanés manuels

AWS Resilience Hub vérifie si des instantanés manuels sont régulièrement créés pour un cluster Amazon DocumentDB Elastic. Les instantanés manuels permettent une plus longue persistance et offrent la flexibilité de définir la fréquence des instantanés en fonction des besoins de votre entreprise.

Passerelle NAT

Cette section répertorie toutes les vérifications et recommandations spécifiques à NAT Gateway. Pour plus d'informations sur les passerelles NAT, consultez Passerelles NAT.

déploiement multi-AZ

AWS Resilience Hub vérifie si la passerelle NAT est déployée en plusieurs AZs. Un déploiement de passerelle NAT supplémentaire est requis dans une autre région si votre police d'assurance prévoit une couverture en cas de perturbation régionale. La passerelle NAT supplémentaire, située dans une région différente, est également vérifiée pour son déploiement dans plusieurs régions AZs.

Amazon Route 53

Cette section répertorie toutes les vérifications et recommandations spécifiques à Amazon Route 53. Pour plus d'informations sur Amazon Route 53, consultez la documentation Amazon Route 53.

déploiement multi-AZ

AWS Resilience Hub vérifie si l'enregistrement de zone hébergée Amazon Route 53 est défini avec plusieurs cibles dans la même région et si ces cibles sont déployées dans plusieurs AZs. Si votre police prévoit une couverture en cas de perturbations régionales AWS Resilience Hub , vérifiez si l'enregistrement de zone hébergée Amazon Route 53 est défini dans plusieurs régions avec plusieurs cibles par région, et si ces cibles sont déployées dans plusieurs régions AZs.

Contrôleur Amazon Application Recovery (ARC)

Cette section répertorie toutes les vérifications et recommandations spécifiques à Amazon Application Recovery Controller (ARC) (ARC). Pour plus d'informations sur ARC, consultez la documentation ARC.

déploiement multi-AZ

AWS Resilience Hub vérifie si des ressources similaires sont déployées dans plusieurs régions et recommande, comme bonne pratique, de définir des contrôles de préparation de l'ARC afin d'accroître leur disponibilité et leur préparation en cas de perturbation régionale. Vous serez informé que des frais horaires supplémentaires vous seront facturés.

Serveur FSx de fichiers Amazon pour Windows

Cette section répertorie toutes les vérifications et recommandations spécifiques à Amazon FSx pour Windows File Server. Pour plus d'informations sur le serveur de fichiers Amazon FSx pour Windows, consultez la documentation du serveur de fichiers Amazon FSx pour Windows.

Type de système de fichiers

AWS Resilience Hub vérifie le type de système de fichiers : `Regional` ou`One Zone`. Le type de système de fichiers affecte sa résilience en cas de perturbations de l'infrastructure ou de l'AZ. Pour plus d'informations sur les types de systèmes de fichiers, consultez Amazon EFS.

Backup du système de fichiers

AWS Resilience Hub vérifie si un AWS Backup est défini pour le système de fichiers déployé. En outre, il vérifie également si l'`cross-Region backup`option est activée si votre police exige une couverture pour les perturbations au niveau de la région.

Réplication des données

AWS Resilience Hub vérifie si une tâche de réplication de AWS DataSync données planifiée au niveau régional ou interrégional est définie pour le système de fichiers déployé.

AWS DataSync une tâche de réplication de données planifiée peut améliorer le RTO estimé de la charge de travail et le RPO de charge de travail estimé au niveau de l'infrastructure, de l'AZ et de la

région. En outre, il peut être associé à un système intégré AWS Backup à la région pour effectuer une restauration en cas d'interruption de l'application.

AWS Step Functions

Cette section répertorie tous les contrôles et recommandations spécifiques à AWS Step Functions. Pour plus d'informations AWS Step Functions, consultez AWS Step Functions la documentation.

Gestion des versions et alias

AWS Resilience Hub vérifie si le AWS Step Functions flux de travail utilise le versionnement et les alias pour améliorer le temps de redéploiement.

Déploiement entre régions

AWS Resilience Hub vérifie si un AWS Step Functions flux de travail du même type est déployé dans une région différente pour être rétabli en cas de perturbation régionale.

Amazon ElastiCache (Redis OSS)

Cette section répertorie toutes les vérifications et recommandations spécifiques à Amazon ElastiCache (Redis OSS).

Pour plus d'informations sur Amazon ElastiCache (Redis OSS), consultez ElastiCache la documentation Amazon.

Déploiement mono-AZ

AWS Resilience Hub vérifie si le cluster Amazon ElastiCache (Redis OSS) est déployé en tant que nœud unique ou avec tous ses nœuds dans une seule zone de disponibilité.

Déploiement mono-AZ

AWS Resilience Hub valide si le cluster Amazon ElastiCache (Redis OSS) est déployé en tant que groupe de réplication (pour les clusters activés en mode cluster et pour les clusters désactivés en mode cluster) sur plusieurs zones de disponibilité afin de permettre le basculement en cas d'interruption de la zone de disponibilité.

Basculement entre régions

AWS Resilience Hub vérifie les objectifs RTO et RPO définis dans la politique de résilience pour se remettre d'une interruption régionale. En outre, AWS Resilience Hub peut identifier les clusters de banques de données mondiaux Amazon ElastiCache (Redis OSS) déployés dans plusieurs régions.

Sauvegarde

AWS Resilience Hub vérifie si les fonctionnalités de sauvegarde suivantes sont appliquées sur un Amazon déployé ElastiCache (Redis OSS) ou sur un cluster auto-conçu :

- Sauvegarde automatique
- Sauvegarde manuelle pour les systèmes de sauvegarde tiers

AWS Resilience Hub ne recommandera pas la sauvegarde comme méthode de restauration si vous n'utilisez pas la sauvegarde. Cependant, vous pouvez réinitialiser la couche de cache en cas d'incohérence des données et recréer les données à partir du stockage principal.

Basculement régional plus rapide

AWS Resilience Hub vérifie les objectifs RTO et RPO définis dans la politique de résilience lors de perturbations de l'infrastructure ou de l'AZ. En outre, AWS Resilience Hub vous pouvez identifier les architectures régionales suivantes pour vous remettre en cas de perturbations liées à l'infrastructure et à l'AZ :

- Instance de nœud de secours secondaire dans une zone de disponibilité différente pour le type de cluster Amazon ElastiCache (Redis OSS) désactivé en mode cluster.
- Instance de nœud de secours secondaire dans une zone de disponibilité différente pour chaque partition pour le type de cluster Amazon ElastiCache (Redis OSS) activé en mode cluster.

Utilisation d'autres services

Cette section décrit les AWS services qui interagissent avec AWS Resilience Hub.

Rubriques

- AWS CloudFormation
- AWS CloudTrail
- AWS Systems Manager
- AWS Trusted Advisor

AWS CloudFormation

AWS Resilience Hub est intégré à AWS CloudFormation un service qui vous aide à modéliser et à configurer vos AWS ressources afin que vous puissiez passer moins de temps à créer et à gérer vos ressources et votre infrastructure. Vous créez un modèle qui décrit toutes les AWS ressources que vous souhaitez (telles que AWS::ResilienceHub:::ResiliencyPolicy et AWS::ResilienceHub:::App), et qui AWS CloudFormation fournit et configure ces ressources pour vous.

Lorsque vous l'utilisez AWS CloudFormation, vous pouvez réutiliser votre modèle pour configurer vos AWS Resilience Hub ressources de manière cohérente et répétée. Décrivez vos ressources une seule fois, puis fournissez les mêmes ressources à plusieurs reprises dans plusieurs AWS comptes et régions.

AWS Resilience Hub et AWS CloudFormation modèles

Pour fournir et configurer des ressources AWS Resilience Hub et des services associés, vous devez comprendre les AWS CloudFormation modèles. Les modèles sont des fichiers texte formatés en JSON ou YAML. Ces modèles décrivent les ressources que vous souhaitez mettre à disposition dans vos AWS CloudFormation piles. Si vous n'êtes pas familiarisé avec JSON ou YAML, vous pouvez utiliser AWS CloudFormation Designer pour vous aider à démarrer avec les AWS CloudFormation modèles. Pour plus d'informations, consultez Qu'est-ce que AWS CloudFormation Designer ? dans le AWS CloudFormation Guide de l'utilisateur.

AWS Resilience Hub prend en charge la création AWS::ResilienceHub:::ResiliencyPolicy et AWS::ResilienceHub:::App l'entrée AWS CloudFormation. Pour plus d'informations, notamment des exemples de modèles JSON et YAML pour AWS::ResilienceHub:::ResiliencyPolicy et

AWS::ResilienceHub:::App, consultez la référence au type de AWS Resilience Hub ressource dans le guide de l'AWS CloudFormation utilisateur.

Vous pouvez utiliser des AWS CloudFormation piles pour définir des AWS Resilience Hub applications. Une pile vous permet de gérer les ressources connexes comme une seule unité. Une pile peut contenir toutes les ressources dont vous avez besoin pour exécuter une application Web, telles qu'un serveur Web ou des règles réseau.

En savoir plus sur AWS CloudFormation

Pour plus d'informations AWS CloudFormation, consultez les ressources suivantes :

- AWS CloudFormation
- AWS CloudFormation Guide de l'utilisateur
- AWS CloudFormation API Reference
- Guide de l'utilisateur de l'interface de ligne de commande AWS CloudFormation

AWS CloudTrail

AWS Resilience Hub est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans AWS Resilience Hub. CloudTrail capture tous les appels d'API AWS Resilience Hub sous forme d'événements. Les appels capturés incluent les appels provenant de la AWS Resilience Hub console et les appels de code vers les opérations de l' AWS Resilience Hub API. Si vous créez un suivi, vous pouvez activer la diffusion continue d' CloudTrail événements vers un compartiment Amazon S3, y compris les événements pour AWS Resilience Hub. 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 AWS Resilience Hub, 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 plus d'informations CloudTrail, consultez le guide de AWS CloudTrail l'utilisateur.

AWS Systems Manager

AWS Resilience Hub travaille avec Systems Manager pour automatiser vos étapes SOPs en fournissant un certain nombre de documents SSM que vous pouvez utiliser comme base pour celles-ci SOPs.

AWS Resilience Hub vous fournit des AWS CloudFormation modèles contenant les rôles IAM nécessaires pour exécuter différents documents de Systems Manager, un rôle par document avec les autorisations requises pour le document en question. Après avoir créé une pile avec le AWS CloudFormation modèle, celui-ci configurera les rôles IAM et enregistrera les métadonnées dans le paramètre Systems Manager pour que le document d'automatisation de Systems Manager soit exécuté pour différentes procédures de restauration.

Pour plus d'informations sur l'utilisation SOPs, consultezGestion des procédures opérationnelles standard.

AWS Trusted Advisor

AWS Trusted Advisor est une base centralisée de recommandations de bonnes AWS pratiques qui vous aide à identifier, hiérarchiser et optimiser votre déploiement sur AWS. AWS Trusted Advisor inspecte votre AWS environnement, puis formule des recommandations par le biais de contrôles lorsque des opportunités existent pour économiser de l'argent, améliorer la disponibilité et les performances du système ou contribuer à combler les failles de sécurité. Ces contrôles sont divisés en plusieurs catégories en fonction de leur objectif. Pour plus d'informations sur les différentes catégories d'enregistrements AWS Trusted Advisor, consultez le guide de AWS Supportl'utilisateur.

AWS Trusted Advisor fournit plusieurs recommandations de résilience de haut niveau par le biais de contrôles de résilience pour chaque application AWS Resilience Hub relevant de la catégorie de tolérance aux pannes. La catégorie de tolérance aux pannes répertorie tous les contrôles qui testent vos applications pour déterminer leur résilience et leur fiabilité. Ces contrôles vous alertent en cas de AppComponent défaillances et de violations des politiques susceptibles d'entraîner des risques de résilience et d'affecter la disponibilité des applications pour la continuité des activités. Il fournit également des recommandations de résilience qui amélioreront les chances de réduire ces risques dans la section Actions recommandées, qui doit être abordée dans AWS Resilience Hub. Pour plus d'informations sur les recommandations relatives à chaque application du AWS Trusted Advisor, nous vous recommandons de consulter les recommandations détaillées fournies dans le AWS Resilience Hub.

AWS Trusted Advisor fournit les vérifications suivantes pour chaque application dans AWS Resilience Hub :

- AWS Resilience Hub scores de résilience des applications — Vérifie le score de résilience de vos applications à partir de leur dernière évaluation AWS Resilience Hub et vous avertit si leurs scores de résilience sont inférieurs à une valeur spécifique.

Critères d'alerte

- Vert — Indique que le score de résilience de votre application est supérieur ou égal à 70.
- Jaune — Indique que le score de résilience de votre application est compris entre 40 et 69.
- Rouge — Indique que le score de résilience de votre application est inférieur à 40.

Action recommandée

Pour améliorer la posture de résilience et obtenir le meilleur score de résilience possible pour votre application, effectuez une évaluation avec la version la plus récente des ressources de votre application et, le cas échéant, mettez en œuvre les recommandations opérationnelles suggérées. Pour plus d'informations sur l'exécution, la révision et la mise en œuvre des évaluations, la révision et l'inclusion/exclusion des recommandations opérationnelles, ainsi que sur leur mise en œuvre, consultez les rubriques suivantes :

- the section called "Exécution d'évaluations de résilience dans AWS Resilience Hub"
- the section called "Révision des rapports d'évaluation"
- the section called "Révision des recommandations en matière de résilience"
- the section called "Y compris ou excluant les recommandations opérationnelles"

- AWS Resilience Hub violation de la politique d'application — Vérifie si les AWS Resilience Hub applications atteignent les objectifs RTO et RPO que vous avez définis pour une application et vous alerte si l'application n'atteint pas les objectifs RTO et RPO.

  Critères d'alerte

  - Vert — Indique que l'application dispose d'une politique et que le RTO de charge de travail estimé et le RPO de charge de travail estimé répondent aux objectifs de RTO et de RPO.
  - Jaune — Indique que l'application possède une politique et n'a pas été évaluée.
  - Rouge — Indique que l'application dispose d'une politique et que le RTO de charge de travail estimé et le RPO de charge de travail estimé ne répondent pas aux objectifs de RTO et de RPO.

  Action recommandée

  Pour vous assurer que le RTO de charge de travail estimé et le RPO de charge de travail estimé de votre application répondent toujours aux objectifs de RTO et de RPO définis, effectuez régulièrement des évaluations avec la dernière version mise à jour des ressources de votre application. En outre, si vous souhaitez vous assurer que la politique de résilience de votre application n'est pas violée, nous vous recommandons de consulter le rapport d'évaluation et

de mettre en œuvre les recommandations de résilience suggérées. Pour plus d'informations sur l'activation AWS Resilience Hub de l'exécution quotidienne d'évaluations en votre nom, l'exécution d'évaluations, l'examen des recommandations de résilience et leur mise en œuvre, consultez les rubriques suivantes :

- the section called "Modification des ressources de l'application"(AWS Resilience Hub Pour permettre d'exécuter des évaluations quotidiennement en votre nom, suivez les étapes de la section Pour modifier les paramètres de notification de dérive de votre procédure de candidature pour sélectionner la case à cocher Évaluer automatiquement chaque jour.)
- the section called "Exécution d'évaluations de résilience dans AWS Resilience Hub"
- the section called "Révision des rapports d'évaluation"
- the section called "Révision des recommandations en matière de résilience"
- the section called "Y compris ou excluant les recommandations opérationnelles"

- AWS Resilience Hub âge d'évaluation des candidatures — Vérifie la dernière fois que vous avez effectué une évaluation pour chacune de vos candidatures dans AWS Resilience Hub. Il vous avertit si vous n'avez pas effectué d'évaluation pendant le nombre de jours spécifié.

  Critères d'alerte

  - Vert — Indique que vous avez effectué une évaluation de votre candidature au cours des 30 derniers jours.
  - Jaune : indique que vous n'avez pas évalué votre candidature au cours des 30 derniers jours.

  Action recommandée

  Réalisez régulièrement des évaluations pour gérer et améliorer la résilience de vos applications sur AWS. Si vous AWS Resilience Hub souhaitez évaluer votre candidature quotidiennement en votre nom, vous pouvez l'activer en cochant la case à cocher Évaluer automatiquement cette application quotidiennement dans la notification de AWS Resilience Hub dérive. Pour sélectionner la case à cocher Évaluer automatiquement cette application tous les jours, complétez la procédure Pour modifier la notification de dérive de votre candidature dans???.

  > **Note**
  >
  > Cette vérification détermine l'âge d'évaluation uniquement des candidatures qui ont été évaluées au moins une fois. AWS Resilience Hub

- AWS Resilience Hub vérification des composants de l'application — Vérifie si un composant d'application (AppComponent) de votre application est irrécupérable. En d'autres termes, si cela AppComponent ne se rétablit pas en cas d'interruption, vous risquez de subir une perte de données inconnue et une interruption du système. Si le critère d'alerte est défini sur Rouge, cela indique qu'il AppComponent est irrécupérable.

  Action recommandée

  Pour vous assurer que vous AppComponent êtes récupérable, passez en revue et mettez en œuvre les recommandations de résilience, puis effectuez une nouvelle évaluation. Pour plus d'informations sur la révision des recommandations en matière de résilience, consultezthe section called "Révision des recommandations en matière de résilience".

Pour plus d'informations sur l'utilisation AWS Trusted Advisor, consultez le guide de AWS Support l'utilisateur.

Historique du document pour le guide de AWS Resilience Hub l'utilisateur

Le tableau suivant décrit la documentation de cette version de AWS Resilience Hub.

- Version de l'API : dernière en date
- Dernière mise à jour de la documentation : 17 décembre 2024

Modification	Description	Date
AWS Resilience Hub intègre les CloudWatch alarmes Amazon déjà implémentées	AWS Resilience Hub détecte et intègre désormais automatiquement les CloudWatch alarmes Amazon déjà configurées dans ses évaluations de résilience, fournissant ainsi une vue plus complète de la posture de résilience de votre application. Cette nouvelle fonctionnalité associe AWS Resilience Hub des recommandations à votre configuration de surveillance actuelle afin de rationaliser la gestion des alarmes et d'améliorer la précision des évaluations. Pour de plus amples informations, veuillez consulter Gérer les alarmes.	17 décembre 2024
AWS Resilience Hub a activé des fonctionnalités supplémentaires pour fournir des tests	AWS Resilience Hub prend désormais en charge une intégration améliorée avec	17 décembre 2024

de résilience simplifiés avec AWS Fault Injection Service des expériences personnalisées	AWS Fault Injection Service (AWS FIS) pour proposer des recommandations personnalisées à l'aide d' AWS FIS actions et de scénarios basés sur le contexte spécifique de l'application afin d'améliorer la posture de résilience. L'exécution des expériences recommandées ou de vos propres tests améliorera votre score de résilience, ce qui vous permettra de suivre les changements au fil du temps. Pour plus d'informations, consultez les rubriques suivantes : • AWSResilienceHubAssessmentExecutionPolicy • Gestion des AWS Fault Injection Service expériences • AWS Resilience Hub — Tests de résilience

AWS Resilience Hub introduit une vue récapitulative	AWS Resilience Hub de la nouvelle vue récapitulative offre une représentation visuelle de haut niveau de la résilience des applications sous forme de tableaux et de graphiques clairs, vous permettant de visualiser l'état de votre portefeuille d'applications et de gérer et d'améliorer efficacement la capacité de vos applications à résister aux perturbations et à s'en remettre. Outre la nouvelle vue récapitulative, vous pouvez exporter les données qui alimentent la vue récapitulative afin de créer des rapports personnalisés pour la communication avec les parties prenantes. Pour de plus amples informati ons, veuillez consulter the section called "AWS Resilienc e Hub résumé".	21 novembre 2024

AWS Resilience Hub introduit le widget Resiliency dans le tableau de bord MyApplications	Le nouveau widget Resiliency du tableau de bord MyApplications rationalise l'évaluation et le suivi de la posture de résilience de vos applications. Il vous permet d'évaluer rapidement la résilience des applications définies dans MyApplications sans avoir à les répliquer manuellement dans le. AWS Resilience Hub Pour plus d'informations, consultez les rubriques suivantes : • the section called "AWS Resilience Hub et MyApplications" • the section called "Gestion des évaluations de résilience à partir du widget Resiliency"	22 octobre 2024

AWS Resilience Hub étend le support pour Amazon ElastiCache (Redis OSS) Serverless	AWS Resilience Hub évalue désormais les applications qui utilisent Amazon ElastiCache (Redis OSS), notamment Amazon ElastiCache (Redis OSS) Serverless et Global Datastores, et fournit des recommandations de résilience améliorées. Il s'agit notamment des directives pour les configurations régionales et multirégionales, ainsi que des stratégies pour les déploiements multi-AZ, le regroupement des ressources et la sauvegarde. En outre, afin de mieux contrôler la posture de résilience des applications, AWS Resilience Hub propose des CloudWatch alarmes Amazon adaptées à Amazon ElastiCache (Redis OSS). Pour plus d'informations, consultez les rubriques suivantes : • the section called "Gestion des composants de l'application" • the section called " AWS Resilience Hub Ressources prises en charge"	25 septembre 2024

- the section called "AWSResilienceHubAsssessmentExecutionPolicy"

AWS Resilience Hub introduit des recommandations de regroupement	AWS Resilience Hub introduit une nouvelle option de regroupement intelligent pour regrouper les ressource s dans les composants de l'application (AppComponents) lors de l'intégration de vos applications. Lorsque vous effectuez des évaluations de résilience AWS Resilience Hub, il est important que vos ressources soient regroupée s avec précision par catégorie appropriée AppCompon ents afin de recevoir des recommandations optimisée s et exploitables. Cette option est idéale pour les applicati ons complexes ou interrégi onales afin de réduire le temps nécessaire à l'intégration de vos applications, et elle complète le flux de travail d'intégration des applications existant qui est disponible aujourd'hui. Pour plus d'informations, consultez les rubriques suivantes : • the section called "Gestion des composants de l'applica tion" • the section called "AWS Resilience Hub recommand	1er août 2024

	ations de regroupement de ressources"	
AWS Resilience Hub introduit un nouveau widget de synthèse des évaluations	AWS Resilience Hub introduit un nouveau widget de synthèse des évaluatio ns qui utilise les fonctionn alités d'intelligence artificie lle générative d'Amazon Bedrock pour transformer des données de résilienc e complexes en informati ons hautement exploitables. Ces résumés d'évaluation extraient les résultats critiques , hiérarchisent les risques et recommandent des mesures pour améliorer la résilience. En vous concentrant sur les éléments les plus important s, vous pouvez comprendr e les évaluations beaucoup plus facilement, ce qui vous permet de disposer d'informa tions à fort impact axées sur les éléments les plus critiques de votre posture de résilience. Pour de plus amples informati ons, veuillez consulter the section called "Résumé de l'évaluation".	1er août 2024

AWS Resilience Hub étend la prise en charge d'Amazon DocumentDB	Cette AWS Resilience Hub politique vous permet d'accorder `Describe` des autorisations vous permettant d'accéder aux ressources et aux configurations sur Amazon DocumentDB, Elastic Load Balancing et AWS Lambda lors de l'exécution d'évaluations. Pour plus d'informations sur la politique AWS gérée, consultezthe section called "AWSResilienceHubAsssessmentExecutionPolicy".	1er août 2024

AWS Resilience Hub étend les capacités de détection des dérives en matière de résilience des applications	AWS Resilience Hub a étendu ses capacités de détection de dérive en introduisant un nouveau type de détection de dérive : la dérive des ressources des applications. Cette amélioration détecte les modifications, telles que l'ajout ou la suppression de ressources dans les sources d'entrée de l'application. Vous pouvez activer les services d'évaluation AWS Resilience Hub planifiée et de notification de dérive et être averti chaque fois qu'une dérive se produit. La dernière évaluation de la résilience identifie les dérives et présente des mesures correctives pour remettre l'application en conformité avec votre politique de résilience. Pour plus d'informations, consultez les rubriques suivantes : • the section called "Détection des écarts" • the section called "Configuration de l'évaluation planifiée et de la notification de dérive"	8 mai 2024

AWS Trusted Advisor améliorations	AWS Resilience Hub a étendu le support AWS Trusted Advisor en ajoutant une vérification pour identifier les composants d'application irrécupérables (). AppComponents Pour de plus amples informations, veuillez consulter the section called "AWS Trusted Advisor".	28 mars 2024
AWS Resilience Hub étend la prise en charge des alarmes recommandées	AWS Resilience Hub a mis à jour le fichier `README.md` modèle avec des valeurs qui vous permettent de créer des alarmes recommandées par l' AWS Resilience Hub intérieur AWS (Amazon, par exemple CloudWatch) ou par l'extérieur AWS. Pour de plus amples informations, veuillez consulter the section called "Gérer les alarmes".	26 mars 2024

AWS Resilience Hub étend la prise en charge d'Amazon FSx pour Windows File Server	AWS Resilience Hub étend le support d'évaluation pour les ressources du serveur de fichiers Amazon FSx pour Windows tout en évaluant la résilience de votre application. Pour les applications utilisant Amazon FSx pour Windows File Server, AWS Resilienc e Hub fournit un nouvel ensemble de recommand ations en matière de résilienc e, couvrant les déploiements en zone de disponibilité (AZ) et multi-AZ, ainsi que les plans de sauvegarde, ainsi que la réplication des données. AWS Resilience Hub prend en charge le serveur de fichiers Amazon FSx pour Windows, y compris la dépendance du système de fichiers à Microsoft Active Directory, pour les déploiements régionaux et interrégionaux. Pour plus d'informations, consultez les rubriques suivantes : • the section called " AWS Resilience Hub Ressources prises en charge" • the section called "AWSResilienceHubA sssessmentExecutionPolicy"	26 mars 2024

	• the section called "Regroupement de ressources dans un composant d'application"	
AWS Resilience Hub fournit des informations supplémentaires sur le score de résilience	AWS Resilience Hub a mis à jour le score de résilience de l'expérience utilisateur pour vous aider à naviguer facilement et à comprendre les actions nécessaires pour améliorer la résilience de vos applications. Pour de plus amples informations, veuillez consulter the section called "Comprendre les scores de résilience".	9 novembre 2023
AWS Resilience Hub étend le support aux applications qui incluent des ressources Amazon Elastic Kubernetes Service (Amazon EKS)	AWS Resilience Hub étend le support aux applications qui incluent des ressources Amazon EKS afin d'inclure de nouvelles recommandations opérationnelles. Lors de l'exécution d'une évaluation qui inclut les ressources des clusters Amazon EKS, nous allons maintenant recommander des tests et des alarmes à exécuter pour améliorer la résilience des applications. Pour de plus amples informations, veuillez consulter the section called "Gestion des AWS Fault Injection Service expériences".	9 novembre 2023

AWS Resilience Hub fournit des informations supplémentaires au niveau de l'application	AWS Resilience Hub fournit des informations supplémentaires au niveau de l'application sur le RTO de charge de travail estimé et le RPO de charge de travail estimé. Ces informations supplémentaires indiquent le RTO de charge de travail estimé maximal et le RPO de charge de travail estimé de votre application sur la base de la dernière évaluation réussie. Cette valeur correspond au RTO de charge de travail maximal estimé et au RPO de charge de travail estimé pour tous les types de perturbations. Pour de plus amples informations, veuillez consulter the section called "Gestion d'applications".	30 octobre 2023

AWS Resilience Hub étend le soutien à l'évaluation pour les AWS Step Functions ressources	AWS Resilience Hub étend le support à l'évaluation des AWS Step Functions ressources tout en évaluant la résilience de votre application. AWS Resilience Hub analyse la AWS Step Functions configuration, y compris le type de machine à états (flux de travail Standard ou Express). En outre, AWS Resilience Hub fournira également des recommand ations qui vous aideront à atteindre les objectifs de temps de reprise (RTO) estimés de la charge de travail et les objectifs du point de reprise de la charge de travail (RPO) estimés. Pour évaluer les applications, y compris les AWS Step Functions ressources, vous devez configurer les autorisations nécessaires, soit en utilisant une politique AWS gérée, soit en ajoutant manuellement l'autorisation spécifique AWS Resilience Hub permettant de lire la AWS Step Functions configuration. Pour plus d'informations sur les autorisations associées , consultezthe section called	30 octobre 2023

"AWSResilienceHubAsssessmentExecutionPolicy".

AWS Resilience Hub permet d'exclure les recommandations opérationnelles	AWS Resilience Hub vous permet d'exclure les recommandations opérationnelles, notamment les alarmes, les procédures opérationnelles standard (SOPs) et les tests AWS Fault Injection Service (AWS FIS). Lors de l'exécution d'une évaluation AWS Resilience Hub, vous recevez des estimations des temps de restauration et des recommandations sur les moyens d'accroître la résilience de l'application évaluée. À l'aide du flux de travail d'exclusion des recommandations, vous pouvez désormais exclure les alarmes recommandées et les AWS FIS tests qui ne les concernent pas. SOPs Le flux de travail d'exclusion est avantageux si vous utilisez une plate-forme autre que celle suggérée ou si vous avez déjà mis en œuvre la recommandation dans une autre méthode. Pour plus d'informations, consultez les rubriques suivantes : • the section called "Y compris ou excluant les	9 août 2023

	recommandations opération nelles” • the section called “Limiter les autorisations pour inclure ou exclure AWS Resilience Hub des recommandations”	
Améliorer la conception des autorisations pour AWS Resilience Hub	AWS Resilience Hub introduit une nouvelle conception d'autorisations pour apporter de la flexibilité lors de la configuration des rôles AWS Identity and Access Management (IAM) pour AWS Resilience Hub. Il consolide également les autorisations en un seul rôle, avec la possibili té de créer des noms de rôles personnalisés qui sont significatifs pour vous et vos équipes. Une nouvelle politique gérée vous AWS Resilience Hub permettra de disposer des autorisations appropriées pour les services pris en charge. Si vous êtes à l'aise avec la méthode actuelle de définition des autorisations, nous continuerons à prendre en charge la configuration manuelle. Pour plus d'informations sur la politique AWS gérée, consultezthe section called “AWSResilienceHubA sssessmentExecutionPolicy”.	02/08/2023

Détection de la dérive de résilience des applications avec AWS Resilience Hub	AWS Resilience Hub vous permet de détecter et de comprendre de manière proactive les actions nécessaires pour améliorer la résilience des applications. Permettre à Amazon Simple Notification Service (Amazon SNS) de recevoir des notifications lorsque l'objectif de temps de rétablissement de la charge de travail estimé (RTO) ou l'objectif du point de reprise de charge de travail estimé (RPO) est passé de l'objectif à celui de ne plus répondre aux objectifs commerciaux de votre entreprise. Le fait de passer de la détection réactive des problèmes de résilience lors de l'exécution manuelle d'une évaluation à une notification proactive via les rubriques Amazon SNS vous permettra d'anticiper les perturbations potentielles à un stade plus précoce et de renforcer la certitude que les objectifs de reprise seront atteints. Pour plus d'informations, consultez les rubriques suivantes : • the section called "Configuration de l'évaluation	02/08/2023

planifiée et de la notification de dérive"

- the section called "Modification des ressources de l'application"

AWS Resilience Hub améliore le support pour Amazon Relational Database Service et Amazon Aurora	AWS Resilience Hub étend le support d'évaluation pour le proxy Amazon Relational Database Service et les configurations de base de données Headless et Amazon Aurora DB. En outre, lors de l'évaluation des applications qui incluent Amazon RDS, nous allons maintenant faire la distinction entre les différents moteurs de base de données afin de fournir des estimations plus précises des objectifs de temps de restauration de la charge de travail (RTOs). AWS Resilience Hub fournira également des actions supplémentaires pour mettre en œuvre les meilleures pratiques de résilience au sein de votre AWS environnement. Les meilleures pratiques peuvent inclure des informations sur les performances avec DevOps Guru pour Amazon RDS, une surveillance améliorée et une automatisation du déploiement bleu/vert sur les moteurs de base de données pris en charge. Pour en savoir plus sur les autorisations requises AWS Resilience Hub pour inclure les ressources de tous les	02/08/2023

	services pris en charge dans votre évaluation, consultez the section called "AWSResilienceHubAsssessmentExecutionPolicy".	
AWS Resilience Hub étend la prise en charge des instantanés Amazon Elastic Block Store	AWS Resilience Hub étend le support d'évaluation pour Amazon Elastic Block Store (Amazon EBS) afin de reconnaître les instantanés Amazon EBS, qui sont pris dans la même région Amazon EBS à l'aide de la technologie Direct. APIs Le support étendu vient s'ajouter au support actuel pour les clients utilisant Amazon Data Lifecycle Manager (Amazon Data Lifecycle Manager) ou AWS Backup. Pour plus d'informations, consultez Amazon Elastic Block Store (Amazon EBS).	02/08/2023

Améliorations apportées à Amazon Elastic Compute Cloud	AWS Resilience Hub a étendu la prise en charge d'Amazon Elastic Compute Cloud (Amazon EC2). Pour les applications de différent es tailles, AWS permet EC2 à ses clients utilisant Amazon de sélectionner la configuration adaptée à leur cas d'utilisation. AWS Resilience Hub prend en charge l'évaluation sur les EC2 configurations Amazon suivantes : • Instances à la demande. • Sauvegarde des instances par AWS Backup et AWS Elastic Disaster Recovery. • Support pour l'auto-scaling des groupes avec Amazon Application Recovery Controller (ARC) (ARC) À l'avenir, le support d'évaluat ion s'étendra aux instances ponctuelles, aux hôtes dédiés, aux instances dédiées, aux groupes de placement et aux flottes. Pour de plus amples informati ons, veuillez consulter the section called "AWS Resilienc e Hub référence des autorisat ions d'accès".	27 juin 2023

AWS mises à jour des politiques gérées	Ajout d'une nouvelle politique qui donne accès à d'autres AWS services pour exécuter des évaluations. Pour de plus amples informations, veuillez consulter the section called "AWSResilienceHubAsssessmentExecutionPolicy".	26 juin 2023
Nouvelles alarmes de recommandation opérationnelle Amazon DynamoDB	Pour les applications utilisant Amazon DynamoDB AWS Resilience Hub , il fournit désormais un nouvel ensemble d'alarmes qui vous avertissent des risques de résilience liés aux modes de capacité à la demande et provisionnée et aux tables globales. Pour accéder aux nouvelles alarmes, vous devrez peut-être mettre à jour la politique AWS Identity and Access Management (IAM) du rôle que vous utilisez. Pour de plus amples informations, veuillez consulter the section called "AWS Resilience Hub référence des autorisations d'accès".	2 mai 2023

AWS Trusted Advisor améliorations	AWS Resilience Hub a étendu le support AWS Trusted Advisor et les applications utilisant Amazon DynamoDB. Lorsque vous utilisez AWS Trusted Advisor avec AWS Resilience Hub, vous pouvez désormais recevoir une notification lorsqu'une demande n'a pas été évaluée au cours des 30 derniers jours. Cette notification vous invite à réévaluer l'application afin de déterminer si des modificat ions pourraient avoir un impact sur sa résilience. Pour plus d'informations sur la vérification de AWS Resilience Hub l'âge lors de l'évaluation, consultezthe section called "AWS Trusted Advisor".	2 mai 2023

Support supplémentaire pour Amazon Simple Storage Service	Outre la prise en charge actuelle de la réplication interrégionale (Amazon S3) et de la réplication entre régions (Amazon S3 CRR) /Amazon S3 dans la même région (SRR), le versionnement et la AWS sauvegarde permettent désormais d'évaluer Amazon S3 en termes de point d'accès multirégional, AWS Resilienc e Hub de contrôle du temps de réplication (Amazon S3 RTC) et de restauration des sauvegardes (PITR). AWS point-in-time Pour plus d'informations, consultez les rubriques suivantes : • the section called "AWS Resilience Hub référence des autorisations d'accès" • Gestion de votre stockage Amazon S3	21 mars 2023

Support supplémentaire pour Amazon Elastic Kubernetes Service	AWS Resilience Hub a ajouté le cluster Amazon EKS en tant que ressource prise en charge pour définir, valider et suivre la résilience des applications. Les clients peuvent ajouter des clusters Amazon EKS à des applications nouvelles ou existantes, et recevoir des évaluations et des recommandations pour améliorer la résilience. Les clients peuvent ajouter des ressources d'application à AWS CloudFormation l'aide de Terraform et AWS Resource Groups MyApplications. En outre, les clients peuvent ajouter un ou plusieurs clusters Amazon EKS directement dans une ou plusieurs régions avec un ou plusieurs espaces de noms dans chaque cluster. Cela permet AWS Resilience Hub de fournir des évaluations et des recommandations uniques et interrégionales. En plus d'examiner les déploiements, les réplicas et les pods ReplicationControllers, AWS Resilience Hub nous analyserons la résilience globale du cluster. AWS Resilience Hub prend en charge les charges de travail	21 mars 2023

du cluster Amazon EKS sans état. Les nouvelles fonctionnalités sont disponibles dans toutes les AWS régions où elles AWS Resilience Hub sont prises en charge.

Pour plus d'informations, consultez les rubriques suivantes :

- the section called "Gérez les ressources de votre application"
- the section called "Ajouter des clusters EKS"
- the section called "AWS Resilience Hub référence des autorisations d'accès"
- AWS Services régionaux

Support supplémentaire pour Amazon Elastic File System	Outre le support actuel pour la sauvegarde Amazon Elastic File System (Amazon EFS), AWS Resilience Hub nous allons maintenant évaluer Amazon EFS pour la réplication Amazon EFS et la configuration AZ. Pour plus d'informations, consultez les rubriques suivantes : • the section called " AWS Resilience Hub Ressources prises en charge" • Qu'est ce qu'Amazon Elastic File System ?	21 mars 2023
Support pour les sources d'entrée des applications	AWS Resilience Hub fournit désormais de la transpare nce sur les sources de vos applications. Il vous permet d'ajouter, de supprimer et de réimporter les sources d'entrée de votre application, ainsi que de publier une nouvelle version de l'application. Pour de plus amples informati ons, veuillez consulter the section called "Modification des ressources de l'applica tion".	21 février 2023

Support pour les paramètres de configuration des applications	AWS Resilience Hub fournit désormais un mécanisme de saisie pour recueillir des informations supplémentaires sur les ressources associées à vos applications. Ces informations AWS Resilience Hub vous permettront de mieux comprendre vos ressources et de fournir de meilleures recommandations en matière de résilience. Pour plus d'informations, consultez les rubriques suivantes : • the section called "Paramètres de configuration de l'application" • the section called "Configuration des paramètres de configuration de l'application" • the section called "Mise à jour des paramètres de configuration des applications"	21 février 2023

Support supplémentaire pour Amazon Elastic Block Store	Outre le support actuel des volumes Amazon Elastic Block Store (Amazon EBS) AWS Resilience Hub , nous allons désormais évaluer les instantanés Amazon EBS par Amazon Data Lifecycle Manager et Amazon EBS fast snapshot restore (FSR). Pour plus d'informations, consultez les rubriques suivantes : • the section called "AWS Resilience Hub référence des autorisations d'accès" • Amazon Elastic Block Store (Amazon EBS)	21 février 2023

Intégration avec AWS Trusted Advisor	AWS Trusted Advisor les utilisateurs pourront consulter les applications associées à leur compte qui ont été évaluées par AWS Resilienc e Hub. AWS Trusted Advisor affiche le dernier score de résilience et fournit un statut indiquant si la politique de résilience ciblée (RTO et RPO) a été respectée ou non. Chaque fois qu'une évaluatio n est exécutée, elle est AWS Resilience Hub mise à jour AWS Trusted Advisor avec les derniers résultats. AWS Trusted Advisor est un service qui analyse en permanence vos AWS comptes et fournit des recommandations pour vous aider à suivre les AWS meilleures pratiques et les directives de AWS Well-Arch itected. Pour de plus amples informati ons, veuillez consulter the section called "AWS Trusted Advisor".	18 novembre 2022

Support pour Amazon Simple Notification Service (Amazon SNS)	AWS Resilience Hub évalue désormais les applications utilisant Amazon SNS en analysant la configuration d'Amazon SNS, y compris les abonnés, et fournit des recommandations pour atteindre les objectifs de reprise de charge de travail estimés de l'organisation (RTO de charge de travail estimé et RPO de charge de travail estimé) pour les applicati ons. Amazon SNS est un service géré qui transmet les messages des éditeurs (producteurs) aux abonnés (consommateurs). Pour plus d'informations, consultez les rubriques suivantes : • the section called " AWS Resilience Hub Ressources prises en charge" • the section called "Gestion de l'identité et des accès" • the section called "Regroupe ment de ressources dans un composant d'application"	16 novembre 2022

Support supplémentaire pour Amazon Application Recovery Controller (ARC) (Amazon ARC)	AWS Resilience Hub évalue désormais Amazon ARC pour Elastic Load Balancing et Amazon Relational Database Service (Amazon RDS), notamment en indiquant dans quels cas Amazon ARC serait bénéfique. Extension AWS Resilienc e Hub du support d'évaluat ion d'Amazon ARC au-delà d' AWS Auto Scaling Group (AWS ASG) et d'Amazon DynamoDB. Amazon ARC fournit une haute disponibi lité à votre application, ce qui vous permet de basculer rapidement l'ensemble de votre application vers une région de basculement. Pour plus d'informations, consultez les rubriques suivantes : • the section called " AWS Resilience Hub Ressources prises en charge" • the section called "Gestion de l'identité et des accès"	16 novembre 2022

Support supplémentaire pour AWS Backup	AWS Resilience Hub évalue désormais Amazon ARC pour Elastic Load Balancing et Amazon Relational Database Service (Amazon RDS), notamment en indiquant dans quels cas Amazon ARC serait bénéfique. Extension AWS Resilienc e Hub du support d'évaluat ion d'Amazon ARC au-delà d' AWS Auto Scaling Group (AWS ASG) et d'Amazon DynamoDB. Amazon ARC fournit une haute disponibi lité à votre application, ce qui vous permet de basculer rapidement l'ensemble de votre application vers une région de basculement. Pour plus d'informations, consultez les rubriques suivantes : • the section called " AWS Resilience Hub Ressources prises en charge" • the section called "Gestion de l'identité et des accès"	16 novembre 2022
Contenu mis à jour : ajout de nouvelles ressources sur les composants d'application	Route53 et AWS Backup ont été ajoutés à la liste des ressources de composant s d'application prises en charge dans la section de AppComponent regroupement.	1et juillet 2022

Nouveau contenu : concept de statut de conformité des applications	Le type d'état Modifications détectées a été ajouté.	2 juin 2022
Présentant AWS Resilience Hub	AWS Resilience Hub est désormais disponible. Ce guide explique comment analyser votre infrastructure, obtenir des recommandations pour améliorer la résilienc e de vos AWS applications, examiner les scores de résilience, etc. AWS Resilienc e Hub	10 novembre 2021

AWS Glossaire

Pour la AWS terminologie la plus récente, consultez le AWS glossaire dans la Glossaire AWS référence.

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.