AWS Hub de Résilience

Guide de l’utilisateur

AWS Hub de Résilience: Guide de l’utilisateur

Table of Contents

Qu'est-ce que AWS Resilience Hub ?

AWS Resilience Hubvous offre un emplacement central pour définir, valider et suivre la résilience de votreAWSapplication. Resilience Hub vous aide à protéger vos applications contre les perturbations et à réduire les coûts de récupération afin d'optimiser la continuité de l'activité afin de répondre aux exigences réglementaires et de conformité. Utilisez Resilience Hub pour effectuer les opérations suivantes :

- Analysez votre infrastructure et obtenez des recommandations pour améliorer la résilience de vos applications. Outre les conseils architecturaux pour améliorer la résilience de vos applications, les recommandations fournissent un code permettant de respecter votre stratégie de résilience, de mettre en œuvre des tests, des alarmes et des procédures d'exploitation standard (SOP) que vous pouvez déployer et exécuter avec votre application dans votre intégration et livraison (CI/CD) pipeline.
- Validez les cibles de temps de récupération (RTO) et de point de récupération (RPO) dans différentes conditions.
- Optimisez la continuité des activités tout en réduisant les coûts de récupération
- Identifiez et résolvez les problèmes avant qu'ils n'apparaissent en production.

Une fois que vous avez déployé une application en production, vous pouvez ajouter Resilience Hub à votre pipeline CI/CD pour valider chaque build avant sa mise en production.

Décrire

Décrivez vos applications à l'aideAWS CloudFormationavec des piles inter-régions et inter-comptes. Vous pouvez également utiliserAWSFichiers d'état Terraform. Les applications peuvent également être décrites à l'aide de groupes de ressources, ou vous pouvez choisir parmi des applications déjà définies dansAWS Service Catalog AppRegistry.

Définir

Définissez les politiques de résilience de vos applications. Ces stratégies incluent les cibles RTO et RPO pour les perturbations des applications, de l'infrastructure, de la zone de disponibilité et de la région.

Évaluer

L'évaluation du Resilience Hub utilise les meilleures pratiques duAWSFramework Well-Architected pour analyser les composants d'une application et découvrir les faiblesses potentielles de résilience. Ces faiblesses peuvent être causées par une configuration incomplète de l'infrastructure, une mauvaise configuration ou des situations où des améliorations supplémentaires de la configuration sont nécessaires.

Valider

Une fois l'application et les procédures d'exploitation standard (SOP) mises à jour pour intégrer les recommandations issues de l'évaluation de la résilience, vous pouvez utiliser Resilience Hub pour tester et vérifier votre application afin de vérifier si elle atteint ses objectifs de résilience avant de la mettre en production. Resilience Hub fonctionne avecAWS Fault Injection Simulator(AWS FIS), un service d'ingénierie du chaos, pour fournir des simulations d'injection de pannes réelles telles que des erreurs réseau ou un trop grand nombre de connexions ouvertes à une base de données, afin de valider les restaurations de l'application dans les cibles de résilience que vous avez définies. Resilience Hub fournit également des opérations API pour que vous puissiez intégrer son évaluation et ses tests de résilience dans vos pipelines CI/CD pour une validation continue de la résilience. L'inclusion de la validation de la résilience dans les pipelines CI/CD permet de s'assurer que les modifications apportées à l'infrastructure sous-jacente de l'application ne compromettent pas la résilience.

Afficher et suivre

Resilience Hub offre une vue complète de l'état global de la résilience de votre portefeuille d'applications via son tableau de bord. Pour vous aider à suivre la résilience des applications, Resilience Hub agrège et organise les événements de résilience (tels que la base de données indisponible ou la validation de la résilience échouée), les alertes et les informations provenant de services tels qu'Amazon CloudWatch, Amazon Route 53 Application Recovery Controller etAWS FIS). Resilience Hub génère également un score de résilience, une échelle qui indique le niveau d'implémentation des tests de résilience recommandés, des alarmes et des SOP de récupération. Ce score est utilisé pour mesurer l'amélioration de la résilience au fil du temps.

Concepts Resilience Hub

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

Résilience

La capacité de maintenir la disponibilité et de récupérer après une perturbation logicielle et opérationnelle dans un laps de temps déterminé.

Objectif de point de récupération (RPO)

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

Objectif de temps de récupération (RTO)

Le délai maximal acceptable entre l'interruption du service et la restauration du service. Cela détermine ce qui est considéré comme une fenêtre horaire acceptable lorsque le service n'est pas disponible.

Application

UnAWS Resilience Hubest une collection deAWSressources utilisées pour détecter et prévenir les interruptions et les pannes d'applications. Il aide également les systèmes à se rétablir automatiquement après des perturbations.

Composant d'application

Un groupe de personnes apparentéesAWSressources qui fonctionnent et échouent en tant qu'unité unique. Par exemple, si vous possédez une base de données principale et une base de données réplica, les deux bases de données appartiennent au même composant d'application.

AWS Resilience Hubdétermine lequelAWSles ressources peuvent appartenir à quel type de composant d'application. Par exemple, un`DBInstance`ne peut pas appartenir à`AWS::ResilienceHub::ComputeAppComponent`calcul.

Statut de conformité des applications

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

Politique respectée

L'application répond à ses objectifs RTO et RPO définis dans la politique. Tous ses composants répondent aux objectifs stratégiques définis. Par exemple, vous avez sélectionné un RTO et un RPO de 24 heures pour les perturbations entreAWSRégions.AWS Resilience Hubpeut voir que vos sauvegardes sont copiées dans votre région de secours. Vous devez toujours maintenir une restauration à partir d'une procédure d'exploitation standard (SOP) de sauvegarde, ainsi que la tester et la chronomiser. Cela se trouve dans les recommandations opérationnelles et fait partie de votre score de résilience global.

La politique a été violée

L'application ne répondait pas aux objectifs de RTO et de RPO définis dans la politique. Un ou plusieurs de ses composants d'application ne répondent pas aux objectifs de la politique. Par exemple, vous avez sélectionné un RTO et un RPO de 24 heures pour les perturbations entreAWSLes régions, mais la configuration de votre base de données n'inclut aucune méthode de récupération entre régions, telle qu'une réplication globale et des copies de sauvegarde.

Non évalué

L'application 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.

Évaluation de Résilience

Resilience Hub utilise une liste de lacunes et de remèdes potentiels pour mesurer l'efficacité d'une politique sélectionnée pour se rétablir et continuer après une catastrophe. Il évalue l'état de conformité de chaque composant d'application ou de chaque application avec la stratégie. Ce rapport inclut des recommandations d'optimisation des coûts et des références à des problèmes potentiels.

Score de résilience

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 d'exploitation standard (SOP) et les tests de l'application.

Type de perturbation

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

Application RTO et RPO

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

Infrastructure Cloud RTO et RPO

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.

Panne Cloud Infrastructure AZ

Une ou plusieurs zones de disponibilité ne sont pas disponibles. Ce type de pannes peut être résolu en basculant vers une zone de disponibilité différente.

Panne de la région Cloud Infrastructure

Une ou plusieurs régions ne sont pas disponibles. Ce type de panne peut être résolu en basculant vers une autre région.

Expériences d'injection de pannes

Resilience Hub recommande des tests pour vérifier la résilience des applications contre différents types de pannes. Ces pannes incluent les pannes d'application, d'infrastructure, de zones de disponibilité (AZ) ou de régions des composants d'application.

Ces tests vous permettent d'effectuer les tâches suivantes :

- Injectez un échec.
- Vérifiez que les alarmes peuvent détecter une panne.
- Vérifiez que les procédures de récupération, ou procédures d'exploitation standard (SOP), fonctionnent correctement pour récupérer l'application après la panne.

Les tests des SOP mesurent le RTO et le RPO. Vous pouvez tester différentes configurations d'applications et mesurer si le RTO et le RPO en sortie répondent aux objectifs définis dans votre stratégie.

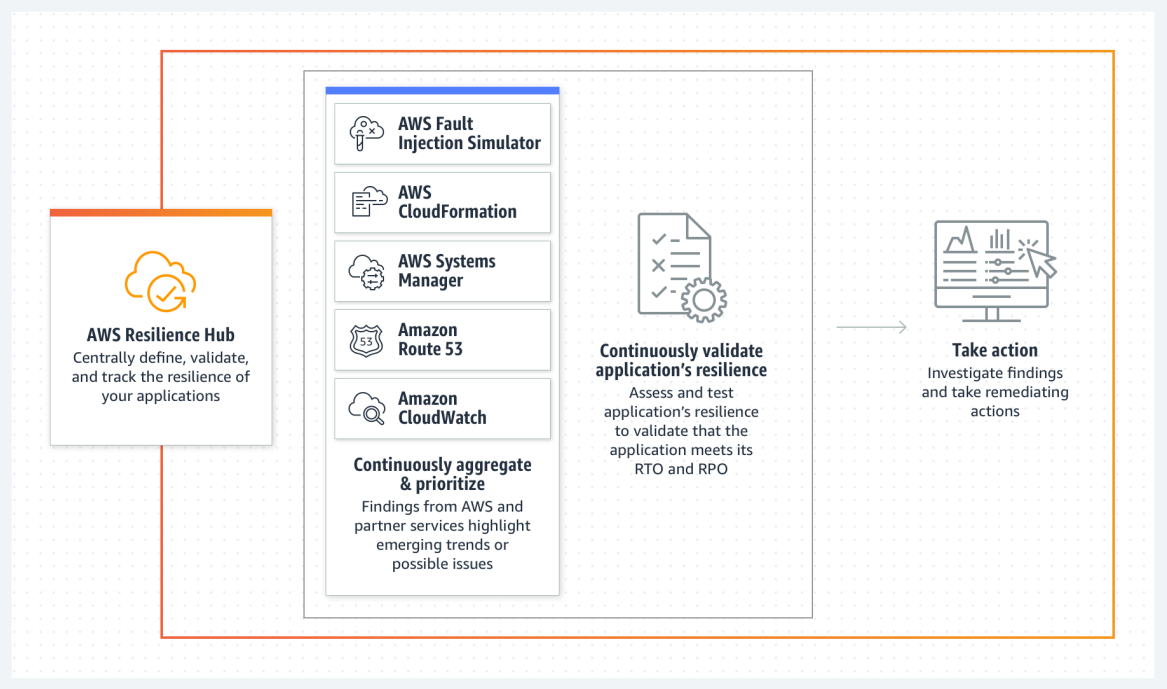
SOP

Le SOP (Standard Operating Procedure) gère les procédures de récupération basées sur le type de panne et les composants de l'application.

Fonctionnement de Resilience Hub

Resilience Hub vous aide à préparer et à protéger de manière proactive votreAWSles applications provenant de perturbation. Le Resilience Hub offre une évaluation et une validation de la résilience qui s'intègrent dans le cycle de vie de votre développement logiciel pour découvrir les faiblesses de résilience. Resilience Hub vous aide à vous assurer que l'objectif de temps de récupération (RTO) et l'objectif de point de récupération (RPO) de vos applications peuvent être atteints et aide à résoudre les problèmes avant qu'ils ne soient mis en production.

Une fois que vous avez déployé unAWSen production, vous pouvez utiliser Resilience Hub pour continuer à suivre la posture de résilience de votre application. En cas de panne, Resilience Hub envoie une notification à l'opérateur pour lancer le processus de récupération associé.



Les étapes suivantes fournissent un aperçu général du fonctionnement de Resilience Hub.

1. Décrivez l'existantAWSque vous souhaitez protéger contre les perturbations en tant qu'application Resilience Hub, puis définissez des objectifs de résilience pour l'application.

   Lorsque vous décrivez l'application, vous importez des ressources depuisAWS CloudFormationpiles, fichiers d'état Terraform, groupes de ressources ou AppRegistry pour former la base structurelle d'une application dans Resilience Hub. Vous pouvez utiliser une application existante pour créer une structure existante à partir d'une structure existante. Vous attachez ensuite une stratégie de résilience à l'application.

   Une stratégie de résilience Resilience Hub contient les informations et les objectifs utilisés pour évaluer si votre application peut récupérer après un type de perturbation, comme une perturbation logicielle ou matérielle. Lorsque vous créez une stratégie de résilience, vous définissez RTO et RPO pour les types de perturbations. Ces objectifs sont utilisés pour déterminer si l'application répond à la politique de résilience.

2. Évaluez l'application pour savoir si elle répond à vos objectifs.

   Après avoir décrit votre application et y avoir attaché une stratégie de résilience, exécutez une évaluation de résilience. L'évaluation évalue la configuration de votre application par rapport à la stratégie de résilience attachée à l'application et génère un rapport. Le rapport montre comment votre application est mesurée par rapport aux objectifs de votre politique de résilience.

3. Recevez des recommandations pour améliorer la résilience.

   Pour améliorer la résilience, mettez à jour votre application et votre stratégie de résilience conformément aux recommandations du rapport d'évaluation. Les recommandations incluent la configuration des composants, des alarmes, des tests et des SOP de récupération. Vous pouvez ensuite exécuter une autre évaluation et comparer les résultats avec le rapport précédent pour voir à quel point la résilience s'améliore. Réitérez ce processus jusqu'à ce que vous atteigniez vos objectifs en matière de RTO et de RPO.

4. Validez les objectifs et les procédures de reprise après sinistre

   Exécutez des tests pour mesurer la résilience de votreAWSet le temps que cela prend pour récupérer à partir d'une application, d'une infrastructure, d'une zone de disponibilité etRégion AWSpannes. Pour mesurer la résilience, ces tests simulent les pannes de votreAWSAWS. Des exemples de pannes incluent les erreurs réseau indisponibles, les basculements, les processus arrêtés, la récupération de démarrage Amazon RDS et les problèmes liés à votre zone de disponibilité.

   Lorsque le test est terminé, vous pouvez déterminer si une application peut récupérer à partir des types de panne définis dans le RTO dans la stratégie de résilience.
5. Affichez et suivez la résilience de vos applications au fil du temps.

   Une fois que vous avez déployé unAWSen production, vous pouvez utiliser Resilience Hub pour continuer à suivre la posture de résilience de l'application. En cas de panne, l'opérateur peut voir la panne dans Resilience Hub et lancer le processus de récupération associé.
6. Commencez la récupération en cas de perturbation.

   En cas de perturbation d'application, Resilience Hub aide à identifier le type de perturbation et alerte l'opérateur. L'opérateur peut ensuite lancer le SOP associé à des fins de récupération.

AWS Resilience Hubressources prises en charge

Les ressources qui affectent RTO et RPO sont entièrement prises en charge parAWS Resilience Hubdes ressources de premier niveau telles que`AWS::RDS::DBInstance`et`AWS::RDS::DBCluster`. Consultez la liste complète des ressources prises en charge dans le tableau suivant des ressources des composants d'application.

Resilience Hub ignore les types de ressources suivants :

- Ressources qui n'affectent pas RTO ou RPO— Des ressources telles que`AWS::RDS::DBParameterGroup`, qui n'affecte jamais le RTO ou le RPO et est toujours ignoré par Resilience Hub.
- Ressources hors niveau supérieur— Resilience Hub n'importe que des ressources de premier niveau, car elles peuvent dériver d'autres propriétés en interrogeant les propriétés des ressources de premier niveau. Par exemple,`AWS::ApiGateway::RestApi`et`AWS::ApiGatewayV2::Api`sont des ressources prises en charge pour Amazon API Gateway. Cependant,`AWS::ApiGatewayV2::Stage`n'est pas une ressource de premier niveau. Par conséquent, il n'est pas importé par Resilience Hub. Cela ne signifie pas que Resilience Hub ignore ces ressources.

  Note

  Ressources non prises en charge
  Ces ressources peuvent affecter RTO et RPO, mais elles ne sont pas entièrement prises en charge parAWS Resilience Hubà l'heure actuelle.AWS Resilience Hubs'efforce d'avertir les utilisateurs des ressources non prises en charge si l'application est soutenue par un CloudFormation pile, fichier d'état Terraform, groupe de ressources ou AppRegistry application.

Regroupement de composants d'application

AppComponent est un groupe deAWSressources qui fonctionnent et échouent en tant qu'unité unique. Par exemple, si vous possédez une base de données principale et une base de données réplica, les deux bases de données appartiennent au même composant d'application.AWS Resilience Huba des

règles qui régissentAWSles ressources peuvent appartenir à quel type de composant d'application. Par exemple, un`DBInstance`peut appartenir à`AWS::ResilienceHub::DatabaseAppComponent`mais pas pour`AWS::ResilienceHub::ComputeAppComponent`calcul.

Lorsqu'un CloudFormation pile, fichier d'état Terraform, groupe de ressources ou AppRegistry est importée dans Resilience Hub, elle fait de son mieux pour regrouper les ressources associées dans le même composant d'application, mais peut ne pas toujours être précise à 100 %. Vous connaissez le mieux l'architecture de votre application. Vous devez donc regrouper ces ressources si nécessaire. Par exemple, si vous avez trois instances EC2 dans unAWS CloudFormation, Resilience Hub crée un seul composant d'application par instance EC2, mais les trois instances EC2 peuvent exécuter le même logiciel d'application. Dans ce cas, le bon choix consiste à regrouper les trois instances EC2 en une seule instance`ComputeAppComponent`.

Voici des exemples de regroupements corrects :

- Regroupez les bases de données principales et les réplicas sous un seul composant d'application.
- Regroupez un compartiment S3 et sa réplication sous un seul composant d'application.
- Regroupez les instances EC2 qui exécutent la même application sous un seul composant d'application.
- Regroupez une file d'attente SQS et sa file d'attente de lettres mortes sous un seul composant d'application.

> **Note**
>
> Resilience Hub nécessite le regroupement approprié pour pouvoir calculer correctement le RTO et le RPO et donner des recommandations correctes.

Chaque composant d'application peut contenir certains types de ressources tels que définis dans le tableau suivant :

Ressources pour les composants d'application

Type de ressource	Type de composant AppComposant
`AWS::EC2::Volume`	`AWS::ResilienceHub::StorageAppComponent`
`AWS::EC2::NatGateway`	`AWS::ResilienceHub::NetworkingAppComponent`
`AWS::DynamoDB::Table`	`AWS::ResilienceHub::DatabaseAppComponent`
`AWS::RDS::DBInstance`	`AWS::ResilienceHub::DatabaseAppComponent`
`AWS::SQS::Queue`	`AWS::ResilienceHub::QueueAppComponent`
`AWS::AutoScaling::AutoScalingGroup`	`AWS::ResilienceHub::ComputeAppComponent`
`AWS::ECS::Service`	`AWS::ResilienceHub::ComputeAppComponent`
`AWS::S3::Bucket`	`AWS::ResilienceHub::StorageAppComponent`
`AWS::ApiGatewayV2::Api`	`AWS::ResilienceHub::ComputeAppComponent`
`AWS::EFS::FileSystem`	`AWS::ResilienceHub::StorageAppComponent`
`AWS::RDS::DBCluster`	`AWS::ResilienceHub::DatabaseAppComponent`
`AWS::ApiGateway::RestApi`	`AWS::ResilienceHub::ComputeAppComponent`

Type de ressource	Type de composant AppComposant
`AWS::Lambda::Function`	`AWS::ResilienceHub::ComputeAppComponent`
`AWS::DocDB::DBCluster`	`AWS::ResilienceHub::DatabaseAppComponent`
`AWS::EC2::Instance`	`AWS::ResilienceHub::ComputeAppComponent`

Démarrer

Cette section décrit comment commencer à utiliserAWS Resilience Hub. Cela inclut la créationAWS Identity and Access Management(IAM) pour un compte.

Prérequis

Pour pouvoir utiliser Resilience Hub, vous devez configurer :

- Une ou plusieurs AWScomptes.
- AWS Identity and Access Managementautorisations (IAM).

Création des rôles IAM pour un compte

Resilience Hub s'intègre avecAWS Identity and Access Management(IAM) afin que vous puissiez accorder aux utilisateurs de Resilience Hub les autorisations d'accès, de test et de surveillance des applications afin d'éviter les perturbations et de mettre en œuvre la reprise après sinistre.

Les autorisations pour Resilience Hub dépendent du type de ressources qui composent vos applications et des fonctionnalités spécifiques de Resilience Hub qu'elles utilisent. Par exemple, si une application est constituée de la base de données RDS, vous devez`rds:DescribeDBInstances`autorisation.

Pour obtenir des instructions d'utilisation des rôles et stratégies, consultezFonctionnement de AWS Resilience Hub avec IAM (p. 52).

Ajout d'une application dansAWS Resilience Hub

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

- Découverte des faiblesses de la résilience.
- Vérifier que vos objectifs de durée de récupération (RPO) peuvent être atteints.
- Résolution des problèmes avant leur mise en production.

Cette section vous guide dans l'ajout d'une application. Vous collectez des ressources à partir d'une application existante,AWS CloudFormationpiles, groupes de ressources ou AppRegistry et créer une politique de résilience appropriée. Après avoir décrit une application, vous pouvez la publier dans Resilience Hub et générer un rapport d'évaluation sur la résilience de votre application. Vous pouvez ensuite utiliser les recommandations de l'évaluation pour améliorer la résilience. Vous pouvez exécuter une autre évaluation, comparer les résultats, puis effectuer une itération jusqu'à ce que vous atteigniez vos objectifs en matière de RTO et de RPO.

Rubriques

Commencez par ajouter une application

Démarrer avecAWS Resilience Huben décrivant les détails de votreAWSet en exécutant un rapport pour évaluer la résilience.

Mise en route

- Dans la pageAWS Resilience HubPage d'accueil sousMise en route, choisissezAjouter une application.

Suivant

Suivant (p. 10)

Étape 1 : Découvrez la structure et décrivez votre application Resilience Hub

Cette section traite des méthodes suivantes que vous utilisez pour fFormez la base de votre structure d'application :

- Stacks CloudFormation
- Resource Groups
- AppRegistry
- Fichiers d'état Terraform
- Une version existanteAWS Resilience Hubcandidature

CloudFormation

Vous pouvez utiliser jusqu'à cinq CloudFormation piles.

Cliquez sur l'onglet CloudFormation piles contenant les ressources que vous souhaitez utiliser dans l'application que vous décrivez. Les piles peuvent provenir duCompte AWSque vous utilisez pour décrire l'application, ou ils peuvent provenir de différents comptes ou de différentes régions.

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

1. Tâche de sélectionCommencez par CloudFormation pilespour découvrir vos ressources basées sur la pile.
2. Choisissez des piles parmiSélectionner des pilesqui sont associés à votreCompte AWSet la région.

   Pour utiliser des piles qui se trouvent dans une autreCompte AWSou une autre région, entrez l'Amazon Resource Name (ARN) de la pile dans l'ARN Stack, puis choisissezARN Stack. Pour en

savoir plus sur les ARN, consultez la section Amazon Resource Names (ARN) dans les Références générales AWS.

3. Entrez un nom pour chaque pile que vous ajoutez.
4. Choisissez Next (Suivant).

Terraform

Vous pouvez utiliser jusqu'à cinq fichiers d'état Terraform.

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

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

1. Tâche de sélectionCommencez par les fichiers d'état Terraformpour découvrir vos ressources de compartiment S3.
2. ChoisissezParcourir S3pour accéder à l'emplacement de votreAWSFichier d'état Terraform.

   Pour utiliserAWSLes fichiers d'état Terraform situés dans une région différente fournissent le lien vers l'emplacement du fichier d'état dans leURL S3.

   > Note
   >
   > La limite pour les fichiers d'état Terraform est de 4 mégaoctets (Mo).
3. Sélectionnez vos compartiments S3 dans leFichier d'état Terraform s3écran et choisissezChoisissez.
4. Choisissez Next (Suivant).

Groupes de ressources

Choisissez les groupes de ressources qui contiennent les ressources que vous souhaitez utiliser dans l'application que vous décrivez. Vous pouvez utiliser jusqu'à cinq groupes de ressources.

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

1. Tâche de sélectionDémarrez avec Resource Groupspour découvrir votreRessources basées sur un groupe.
2. Choisissez des ressources parmiSélectionner des groupes de ressources. Vous pouvez également ajouterARN du groupe de ressources.
3. Choisissez Next (Suivant).

AppRegistry

Cliquez sur l'onglet AppRegistry les applications qui contiennent les ressources que vous souhaitez utiliser dans l'application que vous décrivez. Vous ne pouvez ajouter qu'une seule AppRegistry application à la fois.

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

1. Tâche de sélectionCommencez par AppRegistrypour le sélectionner dans une liste d'applications créées dans AppRegistry.
2. Choisissez des applications parmiSélectionner une applicationqui ont été créés dans AppRegistry.

3. Choisissez Next (Suivant).

Application existante

Pour commencer, utilisez une application existante.

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

1. Tâche de sélectionDémarrez avec une application existantepour construire une structure existante.
2. Choisissez Next (Suivant).

Étape suivante

Étape 2 : Décrivez les détails de votre application dans Resilience Hub (p. 12)

Étape 2 : Décrivez les détails de votre application dans Resilience Hub

Cette section vous montre comment décrire les détails de votre ordinateur existant.AWSapplication dansAWS Resilience Hub.

Pour décrire les détails de votre application

1. Entrez un nom pour l'application.
2. (Facultatif) Entrez une description de l'application.
3. Assurez-vous que votre nom et votre description sont ce que vous voulez.

   Choisissez Next (Suivant).

Étape suivante

Étape suivante (p. 12)

Étape 3 : Évaluation du calendrier

Laissez Resilience Hub exécuter une évaluation quotidienne de votre application ou désactivez ce paramètre et exécutez manuellement l'évaluation selon votre propre calendrier. Lorsque cette option est activée, le calendrier d'évaluation quotidien ne commence qu'une fois que l'application a été évaluée manuellement avec succès pour la première fois et si le`AwsResilienceHubPeriodicAssessmentRole`Le rôle IAM est créé. Pour plus d'informations, consultez Exemples de stratégies AWS Resilience Hub (p. 47).

> **Note**
>
> Les évaluations quotidiennes peuvent avoir un impact sur votre quota pour les essais. Pour de plus amples informations sur les quotas, consultez.AWS Resilience HubPoints de terminaison et quotasdans leAWSRéférence générale.

Pour empêcher votre application d'exécuter des évaluations quotidiennes

- (Facultatif) Utilisez le bouton pour désactiver le calendrier d'évaluation quotidien recommandé pour votre application.

Étape suivante

Étape suivante (p. 13)

Étape 4 : Ajout de balises

Attribuer une étiquette ou une étiquette à unAWSResource pour rechercher et filtrer vos ressources ou suivre vos coûts AWS.

Pour ajouter des balises à votre application

- (Facultatif) ChoisissezAjouter une nouvelle balisesi vous souhaitez associer une ou plusieurs balises à l'application. Pour de plus amples informations sur les balises, consultez.Balisage des ressourcesdans leAWSRéférence générale.

Étape suivante

Étape suivante (p. 13)

Étape 5 : Consultez les ressources de votre application Resilience Hub

Vous devez identifier les ressources de votre application pour vous assurer qu'elles contiennent celles que vous souhaitez. Vous pouvez ajouter des ressources manquantes ou supprimer des ressources dont vous n'avez pas besoin. Les rapports d'évaluation, la validation et les recommandations sont basés sur les ressources répertoriées.

Les ressources sont regroupées en composants d'application logiques. Vous pouvez modifier les composants de l'application pour mieux refléter la structure de votre application. La modification des ressources modifie uniquement la référence Resilience Hub de votre application. Aucune modification n'est apportée à vos ressources réelles, l'AWS CloudFormationles piles, ou leAWSFichiers d'état Terraform contenant les ressources.

Pour identifier les ressources d'application

1. Les ressources du CloudFormation les piles, les applications ajoutées manuellement, le Registre d'applications ou les groupes de ressources que vous avez choisis pour la description de votre application sont répertoriés sousRessources. Vous pouvez les identifier par les éléments suivants :

   - ID logique— Un identifiant logique est un nom utilisé pour identifier les ressources de votre CloudFormation pile, fichier d'état Terraform, application, AppRegistry ou groupes de ressources ajoutés manuellement.

     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 qui portent le même nom.
   - État— Si la ressource a été identifiée comme étant prise en charge par Resilience Hub, le statut estInclude,Exclude, ou estNon pris en charge.
     - Include- Cela indique que Resilience Hub évaluera la résilience de votre ressource.
     - Exclude- Cela indique que Resilience Hub n'évaluera pas la résilience de votre ressource.
     - Non pris en charge- Cela indique que Resilience Hub ne prend pas actuellement en charge votre ressource et ne peut pas évaluer sa résilience.

- Type de ressource— Le type de ressource identifie la ressource de composant de votre application. Par exemple,`AWS::EC2::Instance`déclare un EC2exemple. Pour de plus amples informations sur les ressources des composants d'application, consultez.AWS Resilience Hubressources prises en charge (p. 1).
- Nom: nom de la ressource que vous pouvez ajouter et modifier.
- Nom du composant: nom du composant utilisé pour identifier les composants.
- ID physique— Identificateur réel affecté à cette ressource (par exemple, un ID d'instance EC2 ou un nom de compartiment S3).
- Pile CloudFormation— Le CloudFormation pile qui contient la ressource. Cette colonne dépend du type de structure d'application que vous avez sélectionné.

2. Pour trouver une ressource qui n'est pas répertoriée sousRessources, entrez l'ID logique de la ressource dans la zone de recherche.
3. Pour supprimer une ressource de votre application, sélectionnez la ressource, puis choisissezExclude ressource.

   À l'invite, choisissezExclurepour supprimer la ressource de votre application.

   Pour afficher la liste des ressources exclues, choisissez l'optionExclude ressourcesonglet.

   > **Note**
   >
   > Vous ne pouvez pas importer une ressource exclue tant que l'exclusion de la ressource n'est pas supprimée.

4. Choisissez Next (Suivant).

Étape suivante

Étape suivante (p. 14)

Étape 6 : Sélectionnez une stratégie pour votre application

Une stratégie de résilience Resilience Hub contient des informations et des objectifs utilisés pour évaluer si votre application peut se rétablir après une perturbation, telle qu'une interruption d'application ou d'infrastructure. Lorsque vous créez une stratégie de résilience, vous définissez l'objectif de temps de récupération (RTO) et l'objectif de point de récupération (RPO) pour les types de perturbations. Ces objectifs déterminent si l'application répond à la politique de résilience.

Lorsque vous créez une nouvelle stratégie ou que vous sélectionnez une stratégie de résilience Resilience Hub existante, tenez compte de vos objectifs de résilience et de perturbations potentielles. Par exemple, considérez l'impact commercial de l'application, ainsi que les objectifs RTO et RPO que vous souhaitez que votre application respecte. Identifiez également les perturbations les plus préoccupantes que votre application peut rencontrer car vous pouvez définir des objectifs RTO et RPO pour chaque type de perturbation.

Utilisez une stratégie suggérée ou créez une nouvelle stratégie pour commencer.

Pour créer une stratégie de résilience

1. Tâche de sélectionCréer une stratégie.
2. Entrez le nom de la politique.
3. (Facultatif) Entrez une description de la stratégie.
4. Choisissez l'une des options suivantesPalier :

- Les principaux services informatiques de base
- Mission critique
- Critical (Critique)
- Important
- Non critique

5. UNDERApplication client RTO et RPO, entrez une valeur numérique dans la zone, puis choisissez l'unité de temps que la valeur représente, pour les deuxTOetRPO.

   Répétez ces entrées sousInfrastructure RTO et RPOpourInfrastructureetZone de disponibilité.
6. (Facultatif) Si vous disposez d'une application multi-régions, vous pouvez définir un RTO et un RPO de région.

   UNDERRégion - Facultatifentrez une valeur numérique dans la zone, puis choisissez l'unité de temps que la valeur représente, pour les deuxTOetRPO.
7. (Facultatif) Si vous souhaitez ajouter des balises, vous pouvez le faire ultérieurement pendant que vous continuez à créer votre stratégie. Pour de plus amples informations sur les balises, consultez.Balisage des ressourcesdans leAWSRéférence générale.
8. Pour créer la stratégie, choisissezCréer.
9. Vérifiez que votre stratégie nouvellement créée est sélectionnée par défaut dans la liste des stratégies sousStratégies de résilience, et choisissezSuivant.

Pour utiliser une stratégie de résilience suggérée

1. Entrez le nom de la stratégie de résilience.
2. (Facultatif) Entrez une description de la stratégie.
3. UNDERMesures de résilience suggérées, affichez et choisissez l'un des niveaux de stratégie de résilience prédéterminés suivants :

   - Application non critique
   - Application importante
   - Application critique
   - Application critique globale
   - Application critique
   - Application stratégique globale
   - Service de base
4. Pour créer la stratégie de résilience, choisissezCréer une stratégie.
5. Vérifiez que votre stratégie nouvellement créée est sélectionnée par défaut dans la liste des stratégies sousStratégies de résilience, et choisissezSuivant.

Étape suivante

Étape suivante (p. 15)

Étape 7 : Consultez et publiez votre application Resilience Hub

Après avoir configuré votre application, identifié vos ressources et sélectionné votre stratégie de résilience, vous pouvez consulter et publier votreAWS Resilience Hubapplication.

Pour vérifier et publier votre application

1. Vérifiez toutes les informations que vous avez saisies lors des étapes précédentes.

   Si vous voyez des informations que vous devez modifier ou si vous souhaitez activer ou désactiver la fonction d'évaluation planifiée, choisissezModifier. Une fois que vous avez effectué une modification, choisissezSuivantpour chaque étape jusqu'à ce que vous reveniez à l'étape 7 : Vérifier et publier.
2. Une fois que vous avez terminé votre évaluation, choisissezPublier.

Étape suivante

Étape suivante (p. 16)

Étape 8 : Exécutez une évaluation de votre application Resilience Hub

L'application que vous avez publiée est répertoriée sur leRécapitulatif.

Une fois que vous avez publié votreAWS Resilience Hub, vous êtes redirigé vers la page récapitulative de l'application où vous pouvez exécuter une évaluation de résilience. L'évaluation évalue la configuration de votre application par rapport à la stratégie de résilience attachée à votre application. Un rapport d'évaluation est généré qui montre comment votre application est mesurée par rapport aux objectifs de votre politique de résilience.

Pour effectuer une évaluation de la résilience

1. Dans la pageRésumé des demandes, choisissezÉvaluer la résilience.
2. UNDERNom du rapport, entrez un nom unique pour le rapport ou utilisez le nom généré.
3. Cliquez sur Run (Exécuter).
4. Une fois que vous avez été informé que le rapport d'évaluation a été généré, choisissez l'optionÉvaluationet votre évaluation pour afficher le rapport.
5. Cliquez sur l'ongletVérificationdans le rapport d'évaluation de votre application.

Étape suivante

Étape suivante (p. 16)

Étape 9 : Consultez l'application et les recommandations opérationnelles de votre application Resilience Hub

Consultez la résilience et les recommandations opérationnelles de l'application que vous avez publiée à partir duVérification. Cette page affiche la présentation de l'évaluation des applications, le résumé du RTO et du RPO, ainsi que les détails du type de perturbation, comme suit :

- Présentation- La section Vue d'ensemble contient des informations telles que le nom de l'application, le nom de la stratégie attachée, l'ARN d'évaluation et la date de création de l'évaluation.
- Résumé du RTO- Le récapitulatif RTO affiche le temps RTO ciblé par rapport au temps estimé évalué.

- Résumé du RPO- Le résumé du RPO affiche le temps de RPO ciblé par rapport au temps estimé évalué.
- Détails- La section Détails répertorie le type de perturbation, le composant d'application et les temps réels de RTO et de RPO testés par rapport aux configurations de stratégie attachées.

Pour améliorer la résilience, vous pouvez mettre à jour votre application et votre stratégie de résilience conformément aux recommandations du rapport. Ensuite, exécutez une autre évaluation, comparez les résultats et réitérez le processus jusqu'à ce que vous atteigniez vos objectifs de temps de récupération (RTO) et d'objectif de point de récupération (RPO).

Pour afficher les recommandations d'application

1. Dans la pageVérification, choisissezRecommandations d'application.
2. Dans la pageRecommandations d'application, choisissez un composant dans l'ongletComposantspour afficher les recommandations des applications.

LeRecommandations d'applicationaffiche des informations de recommandation pour optimiser le RTO et le RPO (AZ), le coût et les modifications minimales.

- Optimiser pour RTO et RPO (AZ)- Cette section fournit des informations sur les recommandations sur l'obtention des temps de RTO et de RPO les plus bas pour chaque type de perturbation. Ces informations comprennent la description des recommandations, le coût estimé de la mise en œuvre de la recommandation, le type d'architecture, les modifications recommandées et le temps estimé de RTO et de RPO.
- Optimiser le coût- Cette section fournit des informations de recommandation pour atteindre les heures de RTO et de RPO de votre police au coût le plus bas. Ces informations comprennent la description des recommandations, le coût estimé de la mise en œuvre de la recommandation, le type d'architecture, les modifications recommandées et le temps estimé de RTO et de RPO.
- Optimiser pour des changements minimaux- Cette section fournit des informations de recommandation sur l'atteinte des délais RTO et RPO de votre stratégie avec les modifications minimales de l'infrastructure. Ces informations comprennent la description des recommandations, le coût estimé de la mise en œuvre de la recommandation, le type d'architecture, les modifications recommandées et le temps estimé de RTO et de RPO.

Pour examiner les recommandations opérationnelles

1. Dans la pageVérification, choisissezRecommandations opérationnelles.
2. Dans la pageRecommandations opérationnelles, choisissez un composant dans l'ongletComposantspour afficher les recommandations des applications.

   LeRecommandations opérationnellesaffiche des informations de recommandation pour optimiser le RTO et le RPO, le coût et les modifications minimales.

   - Optimiser pour RTO et RPO (AZ)- Cette section fournit des informations sur les recommandations sur l'obtention des temps de RTO et de RPO les plus bas pour chaque type de perturbation. Ces informations comprennent la description des recommandations, le coût estimé de la mise en œuvre de la recommandation, le type d'architecture, les modifications recommandées et le temps estimé de RTO et de RPO.
   - Optimiser le coût- Cette section fournit des informations de recommandation pour atteindre les heures de RTO et de RPO de votre police au coût le plus bas. Ces informations comprennent la description des recommandations, le coût estimé de la mise en œuvre de la recommandation, le type d'architecture, les modifications recommandées et le temps estimé de RTO et de RPO.

- Optimiser pour des changements minimaux- Cette section fournit des informations de recommandation sur l'atteinte des délais RTO et RPO de votre stratégie avec les modifications minimales de l'infrastructure. Ces informations comprennent la description des recommandations, le coût estimé de la mise en œuvre de la recommandation, le type d'architecture, les modifications recommandées et le temps estimé de RTO et de RPO.

Pour plus d'informations sur la description des applications, la modification des ressources, la création de stratégies de résilience, l'exécution d'évaluations, etc., reportez-vous à la sectionUtiliser Resilience Hub (p. 19).

Utiliser Resilience Hub

AWS Resilience Hubvous aide à améliorer la résilience de vos applications surAWSet réduisez le temps de récupération en cas de panne d'application.

Pour utiliser Resilience Hub, vous devez :

- Décrire vosAWSapplications dans Resilience Hub.
- Gérez vosAWSressources dans Resilience Hub.
- Créez des politiques de résilience efficaces.
- Gérez les évaluations qui indiquent la résilience de vos applications.
- Gérez les alarmes, les procédures d'exploitation standard (SOP) et les tests pour vos applications.

Description et gestion des applications Resilience Hub

UnAWS Resilience Hubest une collection deAWSressources structurées pour prévenir et récupérerAWSInterruptions des applications.

Pour décrire une application Resilience Hub, vous fournissez un nom d'application, des ressources d'une ou plusieurs (jusqu'à cinq)AWS CloudFormationet une politique de résilience appropriée. Vous pouvez également utiliser n'importe quelle application Resilience Hub existante comme modèle pour décrire votre application.

Une fois que vous avez décrit une application Resilience Hub, vous la publiez afin de pouvoir exécuter une évaluation de résilience sur celle-ci. Vous pouvez ensuite utiliser les recommandations de l'évaluation pour améliorer la résilience en exécutant une autre évaluation, en comparant les résultats, puis en répétant le processus jusqu'à ce que vous atteigniez vos objectifs de temps de récupération (RTO) et d'objectif de point de récupération (RPO).

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

Rubriques

Modification des ressources applicatives Resilience Hub

Pour recevoir des évaluations de résilience précises et utiles, assurez-vous que la description de votre application est à jour et correspond à votre description réelle.AWSapplication et ressources. Les rapports d'évaluation, de validation et de recommandations sont basés sur les ressources répertoriées. Si vous

ajoutez ou supprimez des ressources d'unAWS, alors vous devez refléter ces changements exactement dansAWS Resilience Hub.

Vous pouvez identifier et modifier les ressources de votre application. La modification des ressources modifie uniquement le paramètreAWS Resilience Hubréférence de votre application. Aucune modification n'est apportée à vos ressources réelles ouAWS CloudFormationpiles.

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

Ajoutez ou mettez à jour vos ressources applicatives Resilience Hub en modifiant une version préliminaire de votre application. Apportez des modifications à la version brouillon, puis publiez une nouvelle version (version de publication), qui est la version évaluée lorsque vous exécutez des évaluations de résilience.

Pour modifier les ressources d'application

1. Dans le volet de navigation, choisissez Applications.
2. Dans la pageApplications, choisissez le nom de l'application que vous souhaitez modifier.
3. Cliquez sur l'ongletVersions d'onglet.
4. UNDERVersions d', sélectionnezébauche, si cette option n'est pas déjà sélectionnée.
5. Les ressources de l'application que vous avez choisi d'utiliser comme modèle pour la description de votre application sont répertoriées sous leRessourcesonglet. Vous pouvez identifier les ressources en procédant comme suit :

   - ID logique— Un identifiant logique est un nom utilisé pour identifier les ressources de votre CloudFormation pile, fichier d'état Terraform, application, AppRegistry ou groupes de ressources ajoutés manuellement.

     Note

     AWSTerraform 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 qui portent le même nom.
   - pile source— Le CloudFormation pile qui contient la ressource. Cette colonne dépend du type de structure d'application que vous avez sélectionnée.
   - État— Si la ressource a été identifiée comme étant prise en charge par Resilience Hub, le statut estInclude,Exclude, ou estNon pris en charge.
     - Include- Resilience Hub évalue la résilience de votre ressource.
     - Exclude- Resilience Hub n'évalue pas la résilience de votre ressource.
     - Non pris en charge- Resilience Hub ne prend actuellement pas en charge votre ressource et ne peut pas évaluer sa résilience.
   - Type de ressource— Le type de ressource identifie la ressource de composant de votre application. Par exemple,`AWS::EC2::Instance`déclare un EC2exemple. Pour plus d'informations sur les ressources de composants d'application, consultez Groupement AppComponent, consultezRegroupement de composants d'application (p. 1).
   - Nom du composant: nom du composant utilisé pour identifier les composants.
   - ID physique— Identificateur réel affecté à cette ressource (par exemple, un ID d'instance EC2 ou un nom de compartiment S3).
6. Pour trouver une ressource qui n'est pas répertoriée, entrez l'ID logique de la ressource dans la zone de recherche.
7. Pour supprimer une ressource de votre application, sélectionnez la ressource, puis choisissezExclureà partir deModifier.

   Pour afficher la liste des ressources exclues, choisissez l'optionRessources excludesonglet.

8. Pour ajouter une ressource à votre application, depuisActions, choisissezAjout d'une ressource.
9. Pour résoudre les ressources de votre application, depuisActions, choisissezRésolution des ressources.
10. Pour mettre à jour les piles de votre application, depuisActions, choisissezMettre à jour les piles.
11. Si un CloudFormation pile associée aux modifications apportées à votre application, vous pouvez réimporter la pile. Toutes les nouvelles ressources de la pile sont importées, à l'exception des ressources actuellement exclues de Resilience Hub.

    Pour réimporter CloudFormation piles, choisissezMettre à jour les piles.

    a. DansSélectionner les piles, sélectionnez les piles qui sont associées à votreAWScompte et région.

       Pour utiliser des piles qui se trouvent dans une autreAWS, saisissez l'Amazon Resource Name (ARN) de la pile dans leARN Stackpuis choisissezAjouter un ARN de pile. Pour en savoir plus sur les ARN, consultez la section Amazon Resource Names (ARN) dans les Références générales AWS.

    b. Sélectionnez Update (Mettre à jour).
12. Si un fichier d'état Terraform associé à votre application a changé, vous pouvez réimporter le compartiment S3. Toutes les nouvelles ressources du fichier d'état sont importées, à l'exception des ressources actuellement exclues de Resilience Hub.

    Pour réimporter des fichiers d'état Terraform, choisissezMettre à jour les piles.

    a. ChoisissezParcourir S3pour accéder à l'emplacement de votreAWSFichier d'état Terraform.

       Pour utiliserAWSLes fichiers d'état Terraform situés dans une région différente fournissent le lien vers l'emplacement du fichier d'état dans leURL S3.

       > **Note**
       >
       > La limite des fichiers d'état Terraform est de 4 mégaoctets (Mo).

    b. Sélectionnez vos compartiments S3 à partir duFichier d'état Terraform s3écran.
    c. Sélectionnez Update (Mettre à jour).
13. Pour afficher les composants logiques dans lesquels les ressources sont regroupées, choisissez l'optionComposantsonglet.

    SousComposants, vous pouvez ajouter de nouveaux composants, renommer un composant ou supprimer un composant à l'aide duActionsmenu.

Une fois que vous avez apporté des modifications à votre liste de ressources, vous recevez 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 publication d'une nouvelle version, consultezPublication d'une nouvelle version d'application Resilience Hub (p. 23).

Affichage d'un résumé d'application Resilience Hub

La page récapitulatif des applications dans leAWS Resilience HubFournit une vue d'ensemble des informations sur l'application et l'état de la résilience.

Pour afficher un résumé d'une application

1. Dans le volet de navigation, choisissez Applications.
2. Dans la pageApplicationsChoisissez le nom de l'application.

La page récapitulatif des applications comporte les sections suivantes.

Rubriques

Détails

Résumé de l'applicationDétailsRécapitulatif des sélections pour l'application.

- Politique de résilience- Affiche le nom de la stratégie de résilience attachée à votre application. Pour de plus amples informations sur les stratégies de résilience, veuillez consulterGestion des stratégies de résilience (p. 24).
- Description— Description de l'application.
- État— Indique si la stratégie est active ou inactive.
- Heure de création— Date et heure de création de l'application.
- Version— Indique si l'application est publiée ou en version brouillon.
- Évaluation planifiée- Indique si l'évaluation quotidienne est active ou inactive.

Pour mettre à jour l'évaluation planifiée

1. Pour mettre à jour l'évaluation planifiée sur votre application, depuisActions, choisissezMise à jour de l'évaluation.
2. DansÉvaluation planifiéeUtilisez le bouton bascule pour activer ou désactiver le calendrier d'évaluation quotidien recommandé.
3. Sélectionnez Enregistrer les modifications.

> **Note**
>
> Pour activer des évaluations planifiées sur des applications existantes, vous devez exécuter manuellement une évaluation après avoir activé la fonction d'évaluations planifiées pour la première fois. Pour de plus amples informations sur l'exécution des évaluations, consultezExécution d'évaluations de résilience (p. 28).

Résilience des applications

Les mesures affichées sur leRésilience des applicationsproviennent de l'évaluation la plus récente de la résilience de l'application.

Score de résilience

Le score de résilience vous aide à quantifier votre capacité à gérer une perturbation potentielle. Ce score reflète dans quelle mesure votre application a suivi les recommandations du Resilience Hub pour respecter la politique de résilience, les alarmes, les procédures d'exploitation standard (SOP) et les 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. Il indique que les tests déclenchent l'alarme correcte et que l'alarme déclenche le bon SOP.

Supposons, par exemple, que Resilience Hub recommande un test avec une alarme et un SOP. Lorsque le test est exécuté, l'alarme déclenche le SOP associé, puis s'exécute correctement. Pour de plus amples informations sur le score de résilience, consultezComprendre les scores de résilience (p. 32).

Score de résilience dans le temps

Avec le score de résilience dans le temps, vous pouvez afficher 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, Resilience Hub affiche uniquement un graphique de quatre applications à la fois. Pour de plus amples informations sur les évaluations planifiées, veuillez consulterÉtape suivante (p. 9).

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

Resilience Hub utilise également Amazon CloudWatch pour générer ces graphiques. ChoisissezAfficher les métriques dans CloudWatchpour créer et afficher des informations plus granulaires sur la résilience de votre application dans votre CloudWatch tableau de bord Pour de plus amples informations sur CloudWatch, consultezUtilisation des tableaux de bordans leAmazon CloudWatch Guide de l'utilisateur.

Alarmes

Résumé de l'applicationAlarmesrépertorie les alarmes que vous avez configurées dans Amazon CloudWatch pour surveiller l'application. Pour de plus amples informations sur les alarmes, veuillez consulterGérer les alarmes (p. 40).

Expériences

Résumé de l'applicationExpériences d'injection de pannesaffiche la liste des expériences d'injection de défauts. Pour de plus amples informations sur les expériences d'injection d'erreurs, consultezExpériences d'injection de pannes (p. 37).

Publication d'une nouvelle version d'application Resilience Hub

Une fois que vous avez apporté des modifications à votreAWS Resilience Hubressources applicatives telles que décrites dansModification des ressources applicatives Resilience Hub (p. 19), vous devez publier une nouvelle version de votre application pour effectuer 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 alarmes, SOP et tests recommandés à votre application.

Pour publier une nouvelle version d'une application

1. Dans le volet de navigation, choisissez Applications.
2. Dans la pageApplications, choisissez le nom de l'application.
3. Cliquez sur l'ongletVersions d'onglet.
4. Sélectionnez l'onglet Ressources.

5. Choisissez Publish new version (Publier une nouvelle version). Lorsque vous publiez une nouvelle version de votre application, elle devient la version évaluée lorsque vous exécutez des évaluations de résilience.
6. Choisissez Publish.

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 respecte toujours votre stratégie de résilience. Pour de plus amples informations sur l'exécution d'une évaluation, veuillez consulterExécution et gestion des évaluations de résilience Hub (p. 28).

Suppression d'unAWS Resilience Hubcandidature

Une fois que vous avez atteint le maximum de dix limites d'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. Dans la pageApplications, sélectionnez l'application que vous souhaitez supprimer.
3. Choisissez Actions, puis Supprimer.
4. Pour confirmer la suppression, saisissezSupprimer.

Gestion des stratégies de résilience

Cette section décrit comment créer des stratégies de résilience pour vos applications. La définition correcte de stratégies de résilience vous permet de comprendre la posture de résilience de vos applications. Une stratégie de résilience contient des informations et des objectifs que vous utilisez pour déterminer si votre application peut récupérer à partir d'un type de perturbation, tel que logiciel, matériel, zone de disponibilité ouAWSRégion . Les politiques de résilience sont des lignes directrices qui mesurent vos objectifs. Ces stratégies ne modifient pas ou n'affectent pas une application réelle. Plusieurs applications peuvent avoir la même stratégie de résilience.

Lorsque vous créez une stratégie de résilience, vous définissez les objectifs suivants : Objectif de temps de récupération (RTO) et objectif de point de récupération (RPO). Les objectifs déterminent si l'application répond à la politique de résilience. Liez la stratégie à votre application et exécutez une évaluation de résilience. Vous pouvez créer différentes stratégies 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 mensuelle.

L'évaluation évalue la configuration de votre application par rapport à la stratégie de résilience attachée. À la fin du processus,AWS Resilience Hubfournit une évaluation de la façon dont votre application mesure par rapport aux objectifs de votre politique de résilience.

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

AWS Resilience Hubutilise vos objectifs RTO et RPO pour mesurer la résilience face à ces types potentiels de perturbations :

- Application— Perte d'un service ou d'un processus logiciel requis.
- Infrastructure cloud— Perte de matériel, comme les instances EC2.
- Zone de disponibilité de l'infrastructure cloud— Une ou plusieurs zones de disponibilité ne sont pas disponibles.

- Région Infrastructure cloud— Une ou plusieurs régions ne sont pas disponibles.

AWS Resilience Hubvous permet de créer des politiques de résilience personnalisées ou d'utiliser nos politiques de résilience standard ouvertes recommandées. Lorsque vous créez des stratégies personnalisées, nommez et décrivez votre stratégie et choisissez le niveau ou le niveau approprié qui définit votre stratégie. Ces niveaux sont les suivants : Services principaux informatiques fondamentaux, critiques, importants et non critiques.

Choisissez le niveau qui convient à votre classe d'application. Par exemple, vous pouvez classer un système de trading en temps réel comme critique pour la mission, tandis que vous pouvez classer une application de reporting mensuel comme non critique. Lorsque vous utilisez nos stratégies standard, vous pouvez choisir une stratégie de résilience avec un niveau et des valeurs préconfigurés pour les objectifs RTO et RPO par type de perturbation. Vous pouvez, le cas échéant, modifier les valeurs de niveau, ainsi que les valeurs RTO et RPO.

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

Création de stratégies de résilience

DansAWS Resilience Hub, vous pouvez créer une stratégie de résilience. Une stratégie de résilience contient des informations et des objectifs que vous utilisez pour déterminer si votre application peut récupérer à partir d'un type de perturbation, tel que logiciel, matériel, zone de disponibilité ou région AWS. Les politiques de résilience sont des lignes directrices qui mesurent vos objectifs. Ces stratégies ne modifient pas ou n'affectent pas une application réelle. Plusieurs applications peuvent avoir la même stratégie de résilience.

Lorsque vous créez une stratégie de résilience, vous définissez les objectifs suivants : Objectif de temps de récupération (RTO) et objectif de point de récupération (RPO). Les objectifs déterminent si l'application répond à la politique de résilience. Liez la stratégie à votre application et exécutez une évaluation de résilience.

L'évaluation évalue la configuration de votre application par rapport à la stratégie de résilience attachée. À la fin du processus,AWS Resilience Hubfournit une évaluation de la façon dont votre application mesure par rapport aux objectifs de votre politique de résilience.

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

Pour créer des stratégies de résilience dans Applications

1. Dans le menu de navigation de gauche, choisissezApplications.
2. DansApplications, choisissezAjouter une application. Choisissez ensuite l'une des optionsDémarrage rapideouProcédure pas à pas(instructions guidées). En fonction de votre sélection, passez à l'étape 3 ou à l'étape 4.
3. Si vous choisissezDémarrage rapide, entrez un nom, ainsi qu'une description si vous le souhaitez, puis choisissezAddition. Vous pouvez ajouter des ressources et des stratégies de résilience ultérieurement.
4. Si vous choisissezProcédure pas à pas :
   - DansDescription des détails de l'application, entrez le nom et une description si vous le souhaitez. Choisissez Next (Suivant).
   - Spécifiez comment votre application découvre des ressources provenant d'applications existantes, ouAWS CloudFormationpiles.
   - DansPolitiques Résilience, choisissezCréer une stratégie.

- Si vous savez comment vous souhaitez configurer votre stratégie résilience, choisissezCréer une stratégie.
  - Nommez et décrivez la stratégie, puis sélectionnez le niveau qui définit la stratégie.
  - Entrez les valeurs RTO et RPO pour la perturbation matérielle, la perturbation logicielle, la perturbation de la zone de disponibilité et la perturbation de la région (la région est facultative).
  - ChoisissezCréerpour terminer le processus.
- Si vous avez besoin de recommandations pour configurer votre politique de résilience, choisissezSélectionnez une stratégie parmi les suggestions.
  - Nommez et décrivez la stratégie.
  - Choisissez l'une des stratégies de résilience suivantes. Vous pouvez obtenir plus de détails sur la politique ultérieurement.

    Application non critique, niveau applicatif important, niveau d'application critique, niveau d'application critique global, niveau d'application critique, niveau d'application critique, niveau d'application critique global et niveau de service principal. Vous pouvez obtenir plus d'informations sur la stratégie ultérieurement.
  - ChoisissezCréerpour terminer le processus.

Pour créer des stratégies de résilience dans des stratégies de résilience

1. Dans le menu de navigation de gauche, choisissezPolitiques Résilience.
2. DansPolitiques Résilience, choisissezCréer une stratégie.
   - Nommez et décrivez la stratégie, puis sélectionnez le niveau qui définit la stratégie.
   - Entrez les valeurs RTO et RPO pour la perturbation matérielle, la perturbation logicielle, la perturbation de la zone de disponibilité et la perturbation de la région (facultatif).
   - ChoisissezCréerpour terminer le processus.
3. Vous pouvez ajouter des balises internes pour rechercher, filtrer et gérer vos ressources AWS dans votre application.
   - Pour ajouter des balises, choisissezAjouter une nouvelle balise.
   - Saisissez les informations dans les champs Clé et Valeur.

Pour créer des stratégies de résilience basées sur une stratégie suggérée

1. Dans le menu de navigation de gauche, choisissezPolitiques Résilience.
2. DansPolitiques Résilience, choisissezSélectionnez une stratégie basée sur une stratégie suggérée.
   - Nommez et décrivez la stratégie.
   - Choisissez l'une des stratégies de résilience suivantes :

     Application non critique, niveau applicatif important, niveau d'application critique, niveau d'application critique global, niveau d'application critique, niveau d'application critique, niveau d'application critique global et niveau de service principal. Vous pouvez obtenir plus d'informations sur la stratégie ultérieurement.
   - Saisissez les cibles RTO et RPO de l'application client.
   - Saisissez les cibles RTO et RPO de Cloud Infrastructure.
   - ChoisissezCréerpour terminer le processus.
3. Vous pouvez ajouter des balises internes pour rechercher, filtrer et gérer vos ressources AWS dans votre application.

- Pour ajouter des balises, choisissezAjouter une nouvelle balise.
- Saisissez les informations dans les champs Clé et Valeur.

Accès aux détails de la stratégie de résilience

Lorsque vous ouvrez une stratégie de résilience, vous voyez des détails importants sur la stratégie. Vous pouvez également modifier ou supprimer la résilience.

Les détails de la politique de résilience comportent deux points de vue principaux : RécapitulatifetBalises.

Récapitulatif

Informations de base

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

RTO et RPO

Affiche le type de perturbation RTO et RPO associé à cette stratégie de résilience.

Balises

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

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

1. Dans le menu de navigation de gauche, choisissezStratégies.
2. DansPolitiques Résilience, ouvre une politique de résilience.
3. Choisissez Edit (Modifier). Saisissez les modifications appropriées pourInfos basiquesetTOetRPO. Ensuite, choisissez Enregistrer les modifications.

Pour modifier des stratégies de résilience dans la stratégie de résilience

1. Dans le menu de navigation de gauche, choisissezStratégies.
2. DansPolitiques Résilience, choisissez une politique de résilience.
3. ChoisissezActions, puis sélectionnezModifier.
4. Saisissez les modifications appropriées pourInfos basiquesetTOetRPO. Ensuite, choisissez Enregistrer les modifications.

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

1. Dans le menu de navigation de gauche, choisissezStratégies.
2. DansPolitiques Résilience, ouvre une politique de résilience.
3. Sélectionnez Delete (Supprimer). Confirmez votre suppression, puis choisissezSupprimer.

Pour supprimer des stratégies de résilience dans une stratégie de résilience

1. Dans le menu de navigation de gauche, choisissezStratégies.

2. DansPolitiques Résilience, choisissez une politique de résilience.
3. ChoisissezActions, puis sélectionnezSupprimer.
4. Confirmez votre suppression, puis choisissezSupprimer.

Exécution et gestion des évaluations de résilience Hub

Lorsque votre application change, vous devez effectuer une évaluation de résilience. L'évaluation compare chaque configuration de composant d'application à la stratégie et émet des recommandations d'alarme, de SOP et de test. Ces recommandations de configuration peuvent améliorer la vitesse des procédures de récupération.

Les recommandations d'alarme vous aident à définir des alarmes qui détectent les pannes. Les recommandations SOP fournissent des scripts qui gèrent les processus de récupération courants, tels que la récupération 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 récupération automatique, tels que la mise à l'échelle automatique ou l'équilibrage de charge en raison de problèmes réseau. Vous pouvez vérifier si les alarmes d'application sont déclenchées lorsque les ressources atteignent leurs limites. Vous pouvez également tester le bon fonctionnement des SOP dans les conditions que vous indiquez.

Exécution d'évaluations de résilience

Vous pouvez exécuter un rapport d'évaluation de la résilience à partir duActionsMenu, leÉvaluationsou dans la vueMise en routeBannière sur leApplication. Vous pouvez identifier et filtrer vos applications à partir du menu Applications en procédant comme suit :

- Nom: nom que vous avez attribué à l'application lors de son ajout à Resilience Hub.
- Statut de conformité— Resilience Hub définit l'état de l'application comme étantÉvalué,Non évalué,Politique violée, ou estChangements détectés.
  - Évalué- Resilience Hub a évalué votre application.
  - Non évalué- Resilience Hub n'a pas évalué votre application.
  - Politique violée- Resilience Hub a déterminé que votre application ne répondait pas aux objectifs de votre stratégie de résilience pour l'objectif de temps de récupération (RTO) et l'objectif de point de récupération (RPO). Examinez et utilisez les recommandations fournies par Resilience Hub avant de réévaluer la résilience de votre application. Pour de plus amples informations sur les recommandations, veuillez consulterÉtape suivante (p. 9).
  - Changements détectés- Resilience Hub a détecté les modifications apportées à la stratégie de résilience associée à votre application. Vous devez réévaluer votre application pour Resilience Hub afin de déterminer si votre application répond aux objectifs de votre stratégie de résilience.
- Évaluations planifiées— Le type de ressource identifie la ressource de composant pour votre application. Pour de plus amples informations sur les évaluations planifiées, veuillez consulterRésilience des applications (p. 21).
  - Actif- Cela indique que votre application est automatiquement évaluée quotidiennement par Resilience Hub.
  - Désactivé- Cela indique que votre application n'est pas automatiquement évaluée quotidiennement par Resilience Hub et que vous devez évaluer manuellement votre application.
- Heure de création— Date et heure de création de l'application.
- ARN— L'Amazon Resource Name (ARN) de la pile associée à votre application. Pour en savoir plus sur les ARN, consultez la section Amazon Resource Names (ARN) dans les Références générales AWS.

Pour exécuter une évaluation de résilience à partir du menu Actions

1. Dans le menu de navigation de gauche, choisissezApplications.
2. Choisissez votreApplication.
3. Cliquez sur l'ongletExécution d'une évaluation de la résià partir desActionsmenu.
4. Entrez un nom unique ou utilisez le nom généré.
5. Cliquez sur Run (Exécuter).

   Pour consulter le rapport d'évaluation, choisissezÉvaluationsdans votre application. Pour plus d'informations, consultez the section called "Examen des rapports d'évaluation" (p. 29).

Pour exécuter une évaluation de la résilience à partir de la bannière Commencer

1. Dans le menu de navigation de gauche, choisissezApplications.
2. DansApplications, ouvrez une application. DansMise en routeBannière au milieu de la page de l'application, choisissezÉvaluée la résilience.
3. DansExécution d'une évaluation de la résі, entrez un nom unique ou utilisez le nom généré, puis choisissezRun (Exécuter Lambda).

   Pour consulter le rapport d'évaluation, choisissezÉvaluationsdans votre application. Pour plus d'informations, consultez the section called "Examen des rapports d'évaluation" (p. 29).

Pour exécuter une évaluation de résilience à partir de la vue Évaluations

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

1. Dans le menu de navigation de gauche, choisissezApplications.
2. Choisissez votre application sousApplication.
3. Cliquez sur l'ongletÉvaluationonglet.
4. DansÉvaluations, choisissezExécution d'une évaluation de la résі. Entrez un nom unique ou utilisez le nom généré.
5. Cliquez sur Run (Exécuter).

   Pour consulter le rapport d'évaluation, choisissezÉvaluationsdans votre application. Pour plus d'informations, consultez the section called "Examen des rapports d'évaluation" (p. 29).

Examen des rapports d'évaluation

Vous trouverez des rapports d'évaluation dans leÉvaluationsvue de votre application.

Pour trouver un rapport d'évaluation

1. Dans le menu de navigation de gauche, choisissezApplications.
2. DansApplications, ouvrez une application.
3. DansÉvaluations, ouvrez un rapport d'évaluation dans leÉvaluations de la résiliencetable.

Lorsque vous ouvrez le rapport, les éléments suivants s'affichent :

- Aperçu général du rapport d'évaluation

- Recommandations pour améliorer la résilience
- Recommandations pour configurer des alarmes, des SOP et des tests
- Comment créer et gérer des balises pour rechercher et filtrer votreAWSressources

Vérification

Cette section fournit une présentation du rapport d'évaluation.AWS Resilience Hubrépertorie chaque type de perturbation et le composant d'application associé. Il répertorie également vos stratégies RTO et RPO réelles et détermine si le composant de l'application peut atteindre les objectifs de stratégie.

Présentation

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

Résumé du RTO

Affiche une représentation graphique indiquant si l'application répond aux objectifs des stratégies de résilience. Cela est basé sur la durée pendant laquelle une application peut être interrompue sans causer de dommages importants à l'organisation. L'évaluation est une estimation du RTO attendu.

Résumé du RPO

Affiche une représentation graphique indiquant si l'application répond aux objectifs des stratégies de résilience. Cela est basé sur le temps pendant lequel les données peuvent être perdues avant qu'un préjudice important pour l'entreprise ne se produise. L'évaluation est une estimation du RPO attendu.

Détails

Fournit des descriptions détaillées de chaque type de perturbation (application, infrastructure, zone de disponibilité et région), et fournit les informations suivantes à son sujet :

- Composant

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

- RTO réel (RTO de stratégie)

  Indique si la configuration de votre stratégie est alignée sur vos exigences de stratégie. Nous fournissons deux valeurs, notre estimation RTO et votre RTO actuel. Par exemple, supposons que cette valeur s'affiche pour la stratégie RTO réelle : 40 min (2 heures). Nous estimons ici un RTO de 40 minutes, tandis que votre RTO actuel est de deux heures. Nous basons notre calcul RTO sur la configuration, et non sur la stratégie. Par conséquent, une base de données Multi-Availability Zone aura le même RTO pour l'échec de la zone de disponibilité, quelle que soit la stratégie que vous sélectionnez.

- RPO réel (RPO de stratégie)

  Affiche la stratégie RPO réelle quiAWS Resilience Hubestimations, basées sur la stratégie RPO que vous avez définie pour chaque composant d'application. Par exemple, vous avez peut-être défini le RPO de stratégie pour les échecs de la zone de disponibilité sur une heure. Le résultat réel peut être calculé à zéro. Cela suppose qu'Aurora, où nous validons chaque transaction, réussit quatre nœuds sur six, couvrant plusieurs zones de disponibilité. Il peut s'écouler cinq minutes pour point-in-time restaurer.

  Le seul RTO et RPO que vous pouvez choisir de ne pas fournir est Region. 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, par exemple la définition de cibles RTO ou RPO pour la région, vous recevrez un temps de récupération estimé et des recommandations opérationnelles pour ces défaillances.

Examen des recommandations de résilience

Les recommandations de résilience évaluent les composants de l'application et recommandent comment optimiser par RTO et RPO, les coûts et les modifications minimales.

avecAWS Resilience Hub, vous pouvez optimiser l'optimisation dans les catégories suivantes :

Optimiser pour la zone de disponibilité RTO/RPO

Le RTO et le RPO les plus bas possibles lors d'une perturbation de la zone de disponibilité.

Optimiser le coût

Le coût le plus bas que vous pouvez consommer tout en respectant votre politique.

Optimiser pour des changements minimaux

Atteignez la limite de votre politique et réduisez les modifications de mise en œuvre

Les éléments suivants sont inclus dans les ventilations des catégories d'optimisation :

- Description

  Description de la suggestion.
- Coût estimé

  Une estimation approximative du coût de la configuration suggérée par rapport à votre configuration actuelle. Nous fondons notre estimation sur les prix catalogue et l'approximation de l'utilisation. Les valeurs évaluent l'impact des changements de configuration sur le RTO et le RPO par rapport au coût. Par exemple, si vous ajoutez un réplica passif, il double le coût en réduisant le RTO et le RPO à quelques minutes. L'utilisation des sauvegardes stockera le RTO et le RPO pendant des heures, voire des jours, mais le coût sera le stockage et la surcharge réseau supplémentaires.
- Type d'architecture

  Description en un mot de l'architecture pour les défaillances matérielles et de zone de disponibilité, telles que`NoRecoveryPlan`,`Backup&Restore`,`PilotLight`,`WarmStandBy`, ou`Multisite`.
- Modifications

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

  Le RTO estimé après les changements.
- RPO estimé

  Le RPO estimé après les changements.

Examen des recommandations opérationnelles

Les recommandations opérationnelles contiennent des recommandations pour configurer des alarmes, des SOP,AWS Fault Injection SimulatorExpériences, etAWS CloudFormationtests.

AWS Resilience Hubfournit CloudFormation modèles que vous pouvez télécharger.AWS Resilience Hubgère l'infrastructure des applications sous forme de code. Par conséquent, nous fournissons les recommandations dans CloudFormation afin que vous puissiez ajouter les recommandations au code de l'application.

Vous provisionnez les alarmes, SOP etAWS FISexpériences. Pour fournir des alarmes, des SOP etAWS FISChoix des expériences appropriées CloudFormation et saisissez un nom unique.AWS Resilience Hubcrée un modèle basé sur les recommandations que vous avez sélectionnées. DansModèles, vous pouvez accéder à vos modèles créés via une URL Amazon Simple Storage Service (Amazon S3).

Vous pouvez également créer et gérer des balises. Vous pouvez ajouter des balises à une application et afficher toutes les balises qui y sont associées. Vous pouvez également rechercher, ajouter et supprimer des balises pour une application.

Supprimer les évaluations de résilience

Vous pouvez supprimer des évaluations de résilience dans leÉvaluationsvue de votre application.

Pour supprimer une évaluation de résilience

1. Dans le menu de navigation de gauche, choisissezApplications.
2. DansApplications, ouvrez une application.
3. DansÉvaluations, choisissez un rapport d'évaluation dans laÉvaluations de la résiliencetable.
4. Pour confirmer la suppression, choisissez Supprimer.

   Le rapport n'apparaît plus dans leÉvaluations de la résiliencetable.

Comprendre les scores de résilience

Cette section décrit commentAWS Resilience Hubquantifie l'état de préparation des applications à partir de différents scénarios de perturbation.

AWS Resilience Hubindique l'état de préparation grâce à un score de résilience. Ce score reflète dans quelle mesure l'application suit de près nos recommandations pour respecter la politique de résilience, les alarmes, les procédures opératoires standard (SOP) et les tests de l'application. En fonction du type de ressources que l'application utilise,AWS Resilience Hubrecommande des alarmes, des SOP et un ensemble de tests pour chaque type de perturbation.

Le score de résilience le plus élevé est de 100 %. Pour obtenir un meilleur score, tous les tests recommandés doivent se terminer dans une période prédéfinie, déclencher toutes les alarmes correctes et initier toutes les SOP qui y sont attachées. Par exemple,AWS Resilience Hubrecommande un test avec une alarme et une SOP. Le test exécute et déclenche l'alarme et déclenche le SOP associé. S'ils fonctionnent correctement et que l'application respecte la stratégie de résilience, elle obtient un score de résilience de 100 %.

Types de recommandations

AWS Resilience Hubassocie les recommandations à des types de perturbations. Les types de perturbations incluent les applications, l'infrastructure, la zone de disponibilité etRégion AWS. Certaines recommandations peuvent s'appliquer à plusieurs types de perturbations. Par exemple, une recommandation peut consister à simuler le type de perturbation de l'infrastructure Amazon Relational Database Service (Amazon RDS) avec un test qui redémarre l'instance Amazon RDS. Pour améliorer les scores de résilience, vous devez régulièrement mettre en œuvre et vérifier des recommandations de priorité supérieure.

Calcul des scores de résilience

AWS Resilience Hubcalcule les scores de couverture pour les alarmes, les SOP, les tests et le respect de la stratégie de résilience pour chaque combinaison de composants d'application et de type de perturbation. Il les agrège ensuite en fonction du poids du composant de l'application et du type de perturbation.

Ce tableau présente les formulesAWS Resilience Hubpermet de déterminer les scores de résilience pour les alarmes, les SOP, les tests et le respect de la politique de résilience.

Formules de score de résilience

Name (Nom)	Description	Formule
AWS Resilience HubCouverture de test (T)	Un score normalisé (0 à 100 pour cent) basé sur le nombre de tests qui ont été exécutés avec succès sur le nombre de tests qui ont été effectuésAWS Resilience Hubrecommandé.	T = Nombre de tests exécutés/ Nombre total de tests recommandés.
Couverture des alarmes (A)	Un score normalisé (0 à 100 %) basé sur le nombre de CloudWatch alarmes qui ont été implémentées avec succès avec des données, hors du nombre d'alarmes CloudWatch quiAWS Resilience Hubrecommandé.	A = Nombre d'alarmes mises en œuvre/Nombre total d'alarmes recommandées.
Couverture SOP (S)	Un score normalisé (0 à 100 %) basé sur le nombre de SOP (manuels ou automatisés) testés avec succès à l'aide deAWS Resilience HubTeste le nombre de SOP quiAWS Resilience Hubrecommandé.	S = Nombre de SOP testables lancés/Nombre total de SOP testables recommandés.
Politique de résilience (P)	Un score normalisé (0 à 100 %) basé sur la conformité de l'application à sa politique de résilience.	P = poids total des types de perturbations respectant la politique de résilience/Poids total de tous les types de perturbations.

Calcul du niveau des composants de l'application et des types de perturbations

Cette section explique comment nous agrégons le score de type de recommandation pour les alarmes (A), les SOP (S), les tests (T) et la stratégie de résilience (P) pour calculer le score de résilience pour les composants d'application et les applications.

• Score de résilience par composant d'application par type de perturbation,`RSao = T * Weight(T) + A * Weight(A) + S * Weight(S) + P * Weight(P)`. En outre, le score de résilience par composant d'application et par type de perturbation est`RSao = Weighted Average (T, M, S, P)`.

• Score de résilience par composant d'application,`RSa = RSao(Application) * Weight(Application) + RSao(Infrastructure) * Weight(Infrastructure) + RSao(AZ) * Weight(AZ) + RSao(Region) * Weight(Region)`.

• Score de résilience pour les applications,`RS = SUM(RSao * Weight of corresponding disruption type)/SUM(Weight of corresponding disruption type)`. De plus, le score de résilience de l'application est`RS = SUM(RSao * Weight of corresponding application`

`component per disruption type)/SUM(Weight of corresponding application component per disruption type)`.

Tableaux de pondé

AWS Resilience Hubattribue une pondération à chaque type de recommandation pour le score de résilience totale.

Ces tableaux montrent le poids des alarmes, des SOP, des tests, de la stratégie de résilience et des types de perturbations.

Poids des alarmes, SOP, tests, cible de stratégie

Type de recommandation	Weight
Alarmes	20 pour cent
SOP	20 pour cent
Tests	20 pour cent
Résilience de la politique	40 pour cent

Poids pour type de perturbation

Type de recommandation	Weight
Région	10 pour cent
Zone de disponibilité	20 pour cent
Infrastructure	30 pour cent
Application	40 pour cent

> **Note**
>
> Si vous choisissez de ne pas définir de cibles RTO ou RPO pour votre stratégie, la pondération de la région est supprimée et les pondérations pour les autres types de perturbations sont augmentées de 3,33 % pour atteindre 100 %.

Accès aux scores de résilience

Vous pouvez voir les scores de résilience dans le tableau de bord ou depuis les applications.

Accès au score de résilience depuis le tableau de bord

1. Dans le menu de navigation de gauche, choisissezTableau de bord.
2. DansDernier score de résilience, choisissez une ou plusieurs applications dans leApplications de filtresdéroulant.
3. Consultez le score de résilience de l'application.

Accès au score de résilience à partir d'Applications

1. Dans le menu de navigation de gauche, choisissezApplications.

2. DansApplications, ouvrez une application.
3. ChoisissezRécapitulatif. DansRésilience de santé, vous pouvez voir le score de résilience.

Procédures d'exploitation normalisées

Une procédure d'exploitation standard (SOP) est un ensemble d'étapes normatives conçues pour récupérer efficacement votre application en cas de panne ou d'alarme. Préparez, testez et mesurez vos SOP à l'avance pour assurer une récupération rapide en cas de panne opérationnelle.

En fonction des composants de votre application,AWS Resilience Hubrecommande les SOP que vous devez préparer.AWS Resilience Hubtravaille avec Systems Manager pour automatiser les étapes de vos SOP en fournissant un certain nombre de documents SSM que vous pouvez utiliser comme base pour ces SOP.

Par exemple,AWS Resilience Hubpeut recommander une SOP pour ajouter de l'espace disque basé sur un document SSM Automation existant. Pour exécuter ce document SSM, vous devez disposer d'un rôle IAM spécifique avec les autorisations appropriées.AWS Resilience Hubcrée des métadonnées dans votre application indiquant quel document d'automatisation SSM exécuter en cas de pénurie de disque et quel rôle IAM est requis pour exécuter ce document SSM. Ces métadonnées sont ensuite enregistrées dans un paramètre SSM.

En plus de configurer l'automatisation SSM, il est également recommandé de le tester avec une expérience de service d'injection de défauts (FIS). Par conséquent,AWS Resilience Hubfournit également une expérience FIS qui appelle le document d'automatisation SSM. De cette façon, vous pouvez tester proactivement votre application pour vous assurer que le SOP que vous avez créé effectue le travail prévu.

AWS Resilience Hubfournit ses recommandations sous la forme d'unAWS CloudFormationmodèle que vous pouvez ajouter à votre base de code d'application. Ce modèle fournit les éléments suivants :

- Le rôle IAM avec les autorisations requises pour exécuter le SOP
- Une expérience FIS que vous pouvez utiliser pour tester les SOP
- Paramètre SSM qui contient des métadonnées d'application indiquant quel document SSM et quel rôle IAM doit être exécuté en tant que SOP et sur quelle ressource. Par exemple : `$(DocumentName) for SOP $(HandleCrisisA) on $(ResourceA)`.

La création d'un SOP peut nécessiter des essais et des erreurs. Exécution d'une évaluation de la résilience par rapport à votre application et génération d'unAWS CloudFormationà partir duAWS Resilience Hubles recommandations sont un bon début. Utilisation de l'AWS CloudFormationmodèle pour générer unAWS CloudFormation, puis utilisez les paramètres SSM et leurs valeurs par défaut dans votre SOP. Exécutez le SOP et découvrez les améliorations que vous devez apporter.

Étant donné que toutes les applications ont des exigences différentes, la liste par défaut des documents SSM quiAWS Resilience Hubles prestations ne seront pas suffisantes pour tous vos besoins. Vous pouvez cependant 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, de sorte que le document SSM approprié est 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, le cas échéant, ajoutez les documents SSM directement à votre base de code et effectuez les modifications ou personnalisations ultérieures. De cette façon, chaque fois que vous déployez votre application, vous déploierez également le SOP le plus récent.

Rubriques

Création d'un SOP basé surAWS Resilience Hubrecommandations

Pour créer un SOP basé surAWS Resilience Hubrecommandations, vous avez besoin d'unAWS Resilience Hubavec une stratégie de résilience attachée à celle-ci, et vous devez effectuer une évaluation de résilience par rapport à cette application. L'évaluation de la résilience génère les recommandations pour votre SOP.

Pour créer un SOP basé surAWS Resilience HubRecommandations :

1. Création d'unAWS CloudFormationmodèle pour le SOP :
    a. Ouvrez la AWS Resilience Hubconsole .
    b. Dans le volet de navigation, choisissez Applications.
    c. Dans la liste des applications, choisissez l'application pour laquelle vous souhaitez créer un SOP.
    d. Si nécessaire, développez leMise en routezone.
    e. ChoisissezConfiguration des recommandations.
    f. UNDERRecommandations opérationnelles, choisissezProcédures d'exploitation normalisées.
    g. Sélectionnez toutes les étapes à inclure dans votre SOP.
    h. ChoisissezCréation d'un modèle CloudFormation. La création du modèle peut prendre quelques minutes.
2. Consommez leAWS Resilience Hubrecommandations dans votre base de code :
    a. Lorsque le modèle est créé, sousRecommandations opérationnelles, choisissezModèles.
    b. Dans la liste des modèles, choisissez le nom du modèle SOP que vous venez de créer.
    c. UNDERDétails du modèle, cliquez sur le lien sousModèles S3pour ouvrir l'objet modèle dans Amazon S3.
    d. Dans la liste des objets, choisissez le lien du dossier SOP.
    e. Cochez la case devant le fichier JSON etOuvrirouTéléchargementça. Le fichier JSON contient les ressources requises pour le SOP : Rôle IAM, expérience FIS et paramètre SSM.
    f. Ajoutez ces ressources à votre base de code. Remplacez les références directes aux ressources applicatives par des références aux noms logiques utilisés dans vos scripts : (« Réf » : « LogicalName »).

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. Créez des documents SSM dans Systems Manager. Vous pouvez utiliser un document SSM existant comme base et modifier son contenu. Vous pouvez également créer un nouveau document entièrement.

Pour de plus amples informations sur l'utilisation de Systems Manager pour créer un document SSM, veuillez consulterProcédure : Utilisation de Document Builder pour créer un runbook personnalisé.

Pour de plus amples informations sur la syntaxe des documents SSM, veuillez consulterSyntaxe du document SSM.

Pour de plus amples informations sur l'automatisation des actions des documents SSM, veuillez consulterRéférence des actions d'automatisation Systems Manager.

Utilisation d'un document SSM personnalisé au lieu du document par défaut

Pour remplacer le document SSMAWS Resilience Hubsuggéré pour votre SOP avec 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 une expérience FIS pour tester votre document SSM.
3. Ajoutez un paramètre SSM pointant 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 dansAWS Resilience Hubet personnalisez-les au besoin. Par exemple, ajoutez ou supprimez les autorisations nécessaires pour le rôle IAM, modifiez la configuration de l'expérience pour pointer vers le nouveau document SSM ou modifier le paramètre SSM pour pointer vers votre nouveau document SSM.

Test des procédures d'application

Comme mentionné précédemment, la meilleure pratique consiste à ajouter des expériences FIS à vos pipelines CI/CD pour tester régulièrement vos SOP, ce qui garantit qu'elles sont prêtes à l'emploi en cas de panne.

Testez les deuxAWS Resilience Hub-les SOP fournis et personnalisés.

Expériences d'injection de pannes

Cette section décrit comment créer et exécuter des expériences d'injection de pannes dansAWS Resilience Hub. Vous effectuez des expériences d'injection de défauts pour mesurer la résilience de votreAWSles ressources et le temps que cela prend pour récupérer à partir de l'application, de l'infrastructure, de la zone de disponibilité etAWSPannes de la région.

Pour mesurer la résilience, ces expériences d'injection de défauts simulent les pannes de votreAWSAWS. Des exemples de pannes incluent les erreurs réseau indisponibles, les basculements, les processus arrêtés sur EC2/ASG, la récupération de démarrage dans Amazon RDS et les problèmes liés à votre zone de disponibilité. Lorsque l'expérience est terminée, vous pouvez déterminer si une application peut récupérer à partir des types de panne définis dans le RTO dans la stratégie de résilience.

Les expériences de Resilience Hub fournissentAWS Systems Manager(Systems Manager) documents d'automatisation que vous utilisez pour définir les expériences que Systems Manager doit effectuer. Les documents d'automatisation Systems Manager :

- Mettez en œuvre différents scénarios de défaillance.
- Validez les alarmes en cas d'échec.
- Vérifiez que l'application peut récupérer une fois le scénario d'échec terminé.

Vous pouvez utiliser les documents d'automatisation de Systems Manager dans leur état par défaut ou les personnaliser en fonction de vos besoins. Vous pouvez accéder aux documents Systems Manager de vos

expériences à partir des expériences d'injection de défauts d'application ou du rapport d'évaluation des applications.

Pour de plus amples informations sur les documents Systems Manager, veuillez consulterSyntaxe du document Systems ManageretRéférence de l'action d'automatisation des documents Systems Manager

Dans le rapport d'évaluation, choisissez une recommandation dans une liste de recommandations d'expériences Resilience Hub. Créez ensuite unAWS CloudFormationmodèle que vous pouvez ouvrir et copier le chemin du modèle.

Utiliser le chemin dansAWS CloudFormationpour créer une pile contenant des modèles d'expérience d'injection de défauts Resilience Hub. Après avoir créé la pile, ouvrez l'application pour afficher les modèles d'expérience d'injection de pannes provisionnés.

Un document Systems Manager contient la liste des étapes qui composent l'expérience. Chaque étape doit être exécutée dans les ordres spécifiés. Vous pouvez voir comment chaque étape s'est déroulée dans un document Systems Manager lorsque vous l'affichez dans votre compte Systems Manager.

Rubriques

Exécution d'une expérience d'injection de défauts

Dans votre application, vous devez d'abord créer un modèle d'expérience et charger le paramètre SSM surAWS FISavant que Resilience Hub puisse exécuter l'évaluation de la résilience.

Pour créer un modèle d'expérience

1. Dans le menu de navigation de gauche, choisissezApplications.
2. DansApplications, ouvrez une application et choisissezExperiments.
3. DansVue provisionnée, choisissezCréation d'un modèle d'expérience.
4. DansCréation d'un modèle d'expérience, saisissez un nom et une description facultative. Vous pouvez, le cas échéant, ajouter des balises pour ce modèle.
5. Choisissez Save (Enregistrer). Vous pouvez maintenant ajouter des composants à votre suite.

Pour créer une expérience dans Applications

Vous devez fournir le document et les paramètres Systems Manager pour que l'automatisation Systems Manager puisse configurer l'expérience.

1. Dans le menu de navigation de gauche, choisissezApplications.
2. DansApplications, ouvrez une application et choisissezExpérience.
3. DansAlloué, ouvrez une suite de tests provisionnée.
4. DansExperiments, choisissez ouCréerouCréation d'un modèle d'expérience.
5. DansDétails du modèle d'expérience, saisissez un nom et une description facultative. Si vous le souhaitez, vous pouvez saisir l'ID de compte etAWSRégion que vous souhaitez cibler pour le modèle.
6. DansAWS Systems Manager Document, choisissezSaisissez le nom du document Systems Manager.
7. DansNom du document, entrez le document Systems Manager qui contient le modèle souhaité.
8. ChoisissezTrouver un document. Si le document Systems Manager est trouvé, le message du document Systems Manager trouvé s'affiche.

9. Vous pouvez développer le menu pour sélectionner les champs que vous souhaitez personnaliser votre test. Il existe des champs qui exigent que vous fassiez une entrée.
10. Choisissez Save (Enregistrer). L'expérience apparaît dans votre suite de tests.

Exécution d'une expérience

1. Dans le menu de navigation de gauche, choisissezApplications.
2. DansApplications, ouvrez une application et choisissezExperiments.
3. Choisissez un modèle d'expérience, puis choisissezExécutez une expérience.
4. DansExperiments, vérifiez les informations, puis choisissezExecute.
5. DansExperiments, vous pouvez voir votre expérience et son statut.

Affichage d'expériences

1. DansExperiments, choisissezExécutions.
2. DansModèles d'expérience, ouvrez une expérience.

Création d'expériences à partir du rapport d'évaluation

Resilience Hub vous recommande de tester votre application après avoir exécuté un rapport d'évaluation. Vous pouvez accéder à ces tests et les exécuter à partir du rapport d'évaluation de votre application.

Resilience Hub fournit une liste d'expériences, qui sont des documents Systems Manager avec des paramètres de test. Lorsque vous sélectionnez une expérience dans la liste, Resilience Hub crée unAWS CloudFormationmodèle avec les paramètres que vous définissez dans le document Systems Manager. Après la création du CloudFormation , vous pouvez voir vos expériences provisionnées pour votre application.

Le CloudFormation est constitué d'un rôle IAM pour chaque document Systems Manager, avec les autorisations minimales requises pour s'exécuter.

Pour créer et exécuter une expérience à partir du rapport d'évaluation

1. Dans le menu de navigation de gauche, choisissezApplications.
2. DansApplications, ouvrez une application et choisissezÉvaluations.
3. DansÉvaluations de la résilience, ouvrez un rapport d'évaluation et choisissezRecommandations opérationnelles.
4. Choisissez un test, puis choisissezCréation d'un modèle CloudFormation.
5. DansCréer CloudFormation modèle, saisissez un nom pour l'expérience ou utilisez un nom généré de façon aléatoire. Resilience Hub affiche un message pour confirmer que le modèle est terminé.
6. DansRéactivité opérationnelle, choisissezModèles.
7. Copiez l'URL dans le chemin Templates S3 et créez la pile avec le modèle. L'expérience apparaît dans votre compte Systems Manager.

Échecs de l'expérience d'injection de défaillants/vérification

DansActions, vous pouvez suivre l'état d'une action exécutée en cours d'exécution par l'expérience.

Analyser l'exécution de l'expérience FIS

Après avoir exécuté une expérience FIS, vous pouvez afficher les détails de l'exécution dans leAWSSystems Manager.

1. Accéder àCloudTrail >Historique des événements.
2. Filtrer les événements parNom d'utilisateurà l'aide de l'ID d'expérience.
3. Affichage du StartAutomationExecution entrée. ID de demandeest l'ID d'automatisation SSM.
4. Accéder àAWSSystems Manager>Automation.
5. Filtrer parID d'exécutionà 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 .AWS Systems Manager AutomationGuide de l'utilisateur. Les paramètres d'entrée d'exécution apparaissent dans leParamètres d'entréeSection duDétails de l'exécutionet incluent des paramètres optionnels qui ne figurent pas dans l'expérience FIS.

   Vous pouvez trouver des informations sur l'état de l'étape et d'autres détails de l'étape en explorant des étapes spécifiques dans les étapes d'exécution.

Échecs courants

Les échecs courants rencontrés lors de l'exécution d'un rapport d'évaluation sont les suivants :

- Le modèle d'alarme n'a pas été déployé avant l'exécution de l'expérience test/SOP. Cela provoque un message d'erreur pendant l'étape d'automatisation.
  - Message d'échec : Les paramètres suivants n'ont pas été trouvés : [/RésilienceHub/Alarme/3DEE49A1-9877-452A-BB0C-A958479A8EF2/NAT-GW-Alarme-octets-Out-to-Source-2020-09-21_NAT-02AD9BC4FBD4E6135]. Assurez-vous que tous les paramètres SSM du document d'automatisation sont créés dans le magasin de paramètres SSM
  - Correction : Assurez-vous de restituer l'alarme pertinente et de déployer le modèle résultant avant de relancer l'expérience.
- Autorisations manquantes dans le rôle d'exécution. Ce message d'erreur se produit si le rôle d'exécution fourni ne dispose pas d'une autorisation et s'affiche dans les détails de l'étape.
  - Message d'échec : Une erreur s'est produite (opération non autorisée) lors de l'appel de l'opération DescribeInstanceStatus : Vous n'êtes pas autorisé à effectuer cette opération. Consultez le Guide de dépannage d'Automation Service pour plus de détails sur le diagnostic.
  - Correction : Vérifiez que vous avez fourni le rôle d'exécution correct. Si cela a été fait, ajoutez l'autorisation requise et réexécutez l'évaluation.
- L'exécution a réussi mais n'a pas eu le résultat escompté. Ceci est dû à des paramètres incorrects ou à un problème d'automatisation interne.
  - Message d'échec : L'exécution a réussi, donc aucun message d'erreur n'est affiché.
  - Correction : Vérifiez les paramètres d'entrée et examinez les étapes exécutées comme expliqué dans l'exécution de l'expérience Analyser FIS avant d'examiner les étapes individuelles des entrées et sorties attendues.

Gérer les alarmes

Lorsque vous effectuez une évaluation de la résilience,AWS Resilience Hubrecommande de configurer des alarmes Amazon CloudWatch pour surveiller la résilience de vos applications. 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 exécuter une évaluation de résilience pour vous assurer que vous disposez des alarmes correctes pour votre application mise à jour.

Création d'alarmes

Vous pouvez créer des alarmes à partir des recommandations opérationnelles. Cette vue contient des recommandations pour configurer des alarmes.AWS Resilience HubfournitAWS CloudFormationmodèles que vous pouvez télécharger.

Pour créer des alarmes dans des recommandations opérationnelles :

1. Passez en revue les recommandations d'alarme, choisissez celle qui convientAWS CloudFormationet saisissez un nom unique.AWS Resilience Hubcrée un modèle basé sur les recommandations que vous avez sélectionnées.
2. Accédez aux modèles que vous avez créés via une URL Amazon S3. Pour ce faire :
   - DansModèles, ouvrez une recommandation d'alarme.
   - DansChemin S3 des modèles, ouvrez le lien pour afficher la liste de tous les objets de votre compartiment Amazon S3.

Affichage des alarmes

AWS Resilience Hubcrée unAWS CloudFormationqui contient des détails pour créer les alarmes sélectionnées dans Amazon CloudWatch. Une fois le modèle généré, vous pouvez y accéder via une URL Amazon S3, puis le télécharger et le placer dans votre pipeline de code ou créer une pile via leAWS CloudFormationconsole

Dans l'évaluation de la résilience, sélectionnez les alarmes que vous souhaitez configurer pour votre application, puis choisissezCréer un modèle CloudFormation.

Pour afficher les alarmes

1. Dans le menu de navigation de gauche, choisissezApplications.
2. DansApplications, ouvrez une application.
3. DansAlarmes, vous pouvez voir une liste des alarmes générées à partir des recommandations d'alarme dansRecommandations opérationnelles. Il classe les alarmes par nom, statut, mesure et ressource.

Affichage des alarmes recommandées

Dans l'évaluation de la résilience, sélectionnez les alarmes que vous souhaitez configurer pour votre application, puis choisissezCréer un modèle CloudFormation.

AWS Resilience Hubcrée unAWS CloudFormationqui contient des détails pour créer les alarmes sélectionnées dans Amazon CloudWatch. Une fois le modèle généré, vous pouvez y accéder via une URL Amazon S3, et le télécharger et le placer dans votre pipeline de code ou créer une pile via leAWS CloudFormationconsole

Intégration des recommandations opérationnelles dans votre application avecAWS CloudFormation

Après avoir choisiCréation d'un modèle CloudFormationdans leRecommandations opérationnelles,AWS Resilience Hubcrée unAWS CloudFormationmodèle qui décrit l'expérience spécifique d'alarme, de procédure d'exploitation standard (SOP) ou de simulation d'injection de défauts (FIS) pour votre application.

LeAWS CloudFormationest stocké dans un compartiment Amazon S3, et vous pouvez vérifier le chemin S3 vers le modèle dans leDétails du modèledans leRecommandations opérationnelles.

Par exemple, la liste ci-dessous illustre un format JSONAWS CloudFormationmodèle qui décrit une recommandation d'alarme rendue parAWS Resilience Hub. Il s'agit d'une alarme de limitation de lecture pour une table DynamoDB appelée`Employees`.

Le`Resources`du modèle décrit la section`AWS::CloudWatch::Alarm`alarme activée lorsque le nombre d'événements d'accélération de lecture pour la table DynamoDB dépasse 1. Et les deux`AWS::SSM::Parameter`les ressources définissent des métadonnées qui permettentAWS Resilience Hubpour identifier les ressources installées sans avoir à analyser l'application réelle.

```
{
  "AWSTemplateFormatVersion" : "2010-09-09",
  "Parameters" : {
    "SNSTopicARN" : {
      "Type" : "String",
      "Description" : "The ARN of the 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" : "Alarm by Resilience Hub that reports when amount of read
 throttle events is 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"
        }
      }
    },

 "dynamodbalarmhealthreadthrottleevents20200401EmployeesONDEMAND0DynamoDBTablePXBZQYH3DCJ9AlarmSSMParam
 {
      "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."
      }
    },

 "dynamodbalarmhealthreadthrottleevents20200401EmployeesONDEMAND0DynamoDBTablePXBZQYH3DCJ9AlarmInfoSSMP
 {
      "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."
      }
    }
  }
}
```

Modification duAWS CloudFormationmodèle

Le moyen le plus simple d'intégrer une ressource alarme, SOP ou FIS 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 unAWS CloudFormationmodèle. Une application réelle est susceptible d'inclure plusieurs autres ressources, 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 maintenant remplacer les ressources codées en dur par une référence dynamique dans les piles d'applications.

Il en va de même de`AWS::CloudWatch::Alarm`définition de ressource, modifiez les éléments suivants :

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

vers ce qui suit :

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

Et sous le`AWS::SSM::Parameter`définition de ressource, modifiez les éléments suivants :

```
"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\"]}"
```

vers 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\"]}"
```

Lors de la modificationAWS CloudFormationmodèles de SOP et d'expériences de simulation d'injection de défauts (FIS), vous adopterez la même approche, en remplaçant les ID de référence codés en dur par des références dynamiques qui continuent de fonctionner même après des modifications matérielles.

En utilisant une référence à la table DynamoDB, vous autorisezAWS CloudFormationpour effectuer les tâches suivantes :

- Créez d'abord la table de base de données.
- Utilisez toujours l'ID réel de la ressource générée dans l'alarme et mettez à jour l'alarme dynamiquement siAWS CloudFormationdoit remplacer la ressource.

> **Note**
>
> Vous pouvez choisir des méthodes plus avancées pour gérer vos ressources applicatives avecAWS CloudFormationtels quePiles imbriquéesouse référant à des sorties de ressources dans unAWS CloudFormationempiler. (Mais si vous souhaitez que la pile de recommandations reste séparée 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).

Sécurité dans AWS Resilience Hub

Chez AWS, la sécurité dans le cloud est notre priorité numéro 1. En tant que client AWS, vous bénéficiez de centres de données et d'architectures réseau conçus pour répondre aux exigences des organisations les plus pointilleuses en termes de sécurité.

La sécurité est une responsabilité partagée entre 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 responsable de la protection de l'infrastructure qui exécute des services AWS dans le cloud AWS. AWS vous fournit également les services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des AWS programmes de conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent à AWS Resilience Hub, consultez Services AWS concernés par le programme de conformité.
- Sécurité dans le cloud : votre responsabilité est déterminée par le service AWS que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation de AWS Resilience Hub. Les rubriques suivantes expliquent comment configurer AWS Resilience Hub pour répondre à vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres services AWS pour surveiller et sécuriser vos ressources AWS Resilience Hub.

Table des matières

Protection des données dans AWS Resilience Hub

Le modèle de responsabilité partagée AWS s'applique à la protection des données dans AWS Resilience Hub. Comme décrit dans ce modèle, AWS est responsable de la protection de l'infrastructure globale sur laquelle l'ensemble du AWS Cloud s'exécute. La gestion du contrôle de votre contenu hébergé sur cette infrastructure est de votre responsabilité. Ce contenu comprend les tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour en savoir plus 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 AWSet RGPD sur le Blog de sécurité AWS.

À des fins de protection des données, nous vous recommandons de protéger les informations d'identification Compte AWS et de configurer les comptes utilisateur individuels avec 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 multi-facteur (MFA) avec chaque compte.
- Utilisez SSL/TLS pour communiquer avec les ressources AWS. Nous recommandons TLS 1.2 ou version ultérieure.
- Configurez une API et la journalisation des activités utilisateur avec AWS CloudTrail.
- Utilisez des solutions de chiffrement AWS, ainsi que tous les contrôles de sécurité par défaut au sein des services AWS.

- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données personnelles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés FIPS 140-2 lorsque vous accédez à AWS via une CLI ou une API, utilisez un point de terminaison FIPS. Pour en savoir plus sur les points de terminaison FIPS disponibles, consultez Norme de traitement de l'information fédérale (Federal Information Processing Standard (FIPS)) 140-2.

Nous vous recommandons vivement de ne jamais placer d'informations confidentielles ou sensibles, telles que des adresses électroniques, dans des balises ou des champs de format libre tels qu'un champ Nom. Cela s'applique notamment lorsque vous utilisez Resilience Hub ou d'autresAWSservices utilisant la console, l'API,AWS CLI, ouAWSKits SDK. Toutes les données que vous saisissez dans des identifications ou des champs de format libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification non chiffrées dans l'URL pour valider votre demande adressée au serveur.

Chiffrement au repos

AWS Resilience Hubchiffre vos données au repos. Les données contenues dans Resilience Hub sont chiffrées 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

Resilience Hub chiffre les données en transit entre le service et d'autres systèmes intégrés.AWSServices . Toutes les données transmises entre Resilience Hub et les services intégrés sont chiffrées à l'aide du protocole TLS (Transport Layer Security). Resilience Hub fournit des actions préconfigurées pour des types de cibles spécifiques à traversAWSet prend en charge les actions pour les ressources cibles.

Gestion des identités et des accès pour AWS Resilience Hub

AWS Identity and Access Management (IAM) est un Service AWS qui aide un administrateur à contrôler en toute sécurité l'accès aux ressources AWS. Les administrateurs IAM contrôlent qui peut êtreauthentifié(connecté) etautorisé(possédant les autorisations) pour utiliser les ressources Resilience Hub. IAM est un Service AWS que vous pouvez utiliser sans frais supplémentaires.

Table des matières

Public ciblé

Utilisation d'AWS Identity and Access Management(IAM) diffère selon le travail que vous accomplissez dans Resilience Hub.

Utilisateur du service— Si vous utilisez le service Resilience Hub pour effectuer votre tâche, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Plus vous utiliserez de fonctionnalités Resilience Hub pour effectuer votre travail, plus vous pourrez avoir besoin d'autorisations supplémentaires. Comprendre la gestion des accès peut vous aider à demander à votre administrateur les autorisations appropriées. Si vous ne pouvez pas accéder à une fonction dans Resilience Hub, consultezRésolution des problèmes d'identité et d'accès avec AWS Resilience Hub (p. 71).

administrateur de service— Si vous êtes le responsable des ressources du Resilience Hub dans votre entreprise, vous bénéficiez probablement d'un accès total à Resilience Hub. Il vous appartient de déterminer les fonctions et ressources Resilience Hub auxquelles vos employés peuvent accéder. Vous devrez 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 façon dont votre entreprise peut utiliser IAM avec Resilience Hub, veuillez consulter.Fonctionnement de AWS Resilience Hub avec IAM (p. 52).

Administrateur IAM— Si vous êtes un administrateur IAM, vous souhaiterez peut-être obtenir des détails sur la façon dont vous pouvez écrire des stratégies pour gérer l'accès à Resilience Hub. Pour voir des exemples de stratégies Resilience Hub basées sur l'identité que vous pouvez utiliser dans IAM, consultez.Exemples de stratégies AWS Resilience Hub (p. 55).

Authentification avec des identités

L'authentification correspond au processus par lequel vous vous connectez à AWS via vos informations d'identification. Pour plus d'informations sur la connexion à l'aide de la AWS Management Console, consultez Connexion à la AWS Management Console en tant qu'utilisateur IAM ou utilisateur racine dans le Guide de l'utilisateur IAM.

Vous devez vous authentifier (être connecté à AWS) en tant qu'utilisateur racine du Compte AWS, utilisateur IAM ou en endossant un rôle IAM. Vous pouvez également utiliser l'authentification de connexion unique de votre entreprise ou vous connecter par le biais de Google ou de Facebook. Dans ces cas, votre administrateur aura précédemment configuré une fédération d'identités avec des rôles IAM. Lorsque vous accédez à AWS avec des informations d'identification d'une autre entreprise, vous assumez indirectement un rôle.

Pour vous connecter directement à la AWS Management Console, utilisez votre mot de passe avec votre adresse électronique d'utilisateur racine ou votre nom d'utilisateur IAM. Vous pouvez accéder à AWS par programmation avec vos clés d'accès d'utilisateur IAM ou racine. AWS fournit un kit SDK et des outils de ligne de commande pour signer de manière chiffrée votre demande avec vos informations d'identification. Si vous n'utilisez pas les outils AWS, vous devez signer la requête vous-même. Pour ce faire, utilisez Signature Version 4, un protocole permettant d'authentifier les demandes d'API entrantes. Pour plus d'informations sur l'authentification des demandes, consultez Processus de signature de la version 4 dans les Références générales AWS.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être également fournir des informations de sécurité supplémentaires. Par exemple, AWS vous recommande d'utiliser l'authentification multi-facteur (MFA) pour améliorer la sécurité de votre compte. Pour en savoir plus, consultez Utilisation de l'Authentification multifacteur (MFA) dans la AWS du Guide de l'utilisateur IAM.

Utilisateur racine Compte AWS

Lorsque vous créez un Compte AWS, vous commencez avec une seule identité de connexion disposant d'un accès complet à tous les Services AWS et ressources du compte. Cette identité est appelée Compte AWS utilisateur racine. Vous pouvez y accéder en vous connectant à l'aide de l'adresse électronique et du 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, y compris pour les tâches administratives. Respectez plutôt la bonne pratique qui consiste à avoir recours à l'utilisateur racine uniquement pour créer le premier

utilisateur IAM. Ensuite, mettez en sécurité les informations d'identification de l'utilisateur racine et utilisez-les uniquement pour effectuer certaines tâches de gestion des comptes et des services.

Utilisateurs et groupes IAM

Un utilisateur IAM est une identité dans votre Compte AWS qui dispose d'autorisations spécifiques pour une seule personne ou application. Un utilisateur IAM peut disposer d'informations d'identification à long terme, comme un nom d'utilisateur et un mot de passe ou un ensemble de clés d'accès. Pour découvrir comment générer des clés d'accès, consultez Gestion des clés d'accès pour les utilisateurs IAM dans le Guide de l'utilisateur IAM. Lorsque vous générez des clés d'accès pour un utilisateur IAM, veillez à afficher et enregistrer la paire de clés de manière sécurisée. Vous ne pourrez plus récupérer la clé d'accès secrète à l'avenir. Au lieu de cela, vous devrez générer une nouvelle paire de clés d'accès.

Un groupe IAM est une identité qui concerne un ensemble d'utilisateurs IAM. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez avoir un groupe nommé IAMAdmins et accorder à ce groupe les autorisations d'administrer des ressources IAM.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des informations d'identification temporaires. Pour en savoir plus, consultez Quand créer un utilisateur IAM (au lieu d'un rôle) dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une entité au sein de votre Compte AWS qui dispose d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais le rôle IAM n'est pas associé à une personne en particulier. Vous pouvez temporairement endosser un rôle IAM dans la AWS Management Console en changeant de rôle. Vous pouvez obtenir un rôle en appelant une opération d'API AWS CLI ou AWS à l'aide d'une URL personnalisée. Pour en savoir plus sur les méthodes d'utilisation des rôles, consultez Utilisation des rôles IAM dans le Guide de l'utilisateur IAM.

Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

- Autorisations utilisateur IAM temporaires : un utilisateur IAM peut endosser un rôle IAM pour accepter différentes autorisations temporaires concernant une tâche spécifique.
- Accès par des utilisateurs fédérés : au lieu de créer un utilisateur IAM, vous pouvez utiliser des identités existantes provenant d'AWS Directory Service, de votre répertoire d'utilisateurs d'entreprise ou d'un fournisseur d'identité web. On parle alors d'utilisateurs fédérés. AWS attribue un rôle à un utilisateur fédéré lorsque l'accès est demandé via un fournisseur d'identité. Pour en savoir plus sur les utilisateurs fédérés, consultez Utilisateurs fédérés et rôles dans le Guide de l'utilisateur IAM.
- Accès comptes multiples : 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 entre plusieurs comptes. Toutefois, certains Services AWS vous permettent d'attacher une politique directement à une ressource (au lieu d'utiliser un rôle en tant que proxy). Pour en savoir plus sur la différence entre les rôles et les politiques basées sur les ressources pour l'accès comptes multiples, consultez Différence entre les rôles IAM et les politiques basées sur les ressources dans le Guide de l'utilisateur IAM.
- Accès inter-services : certains Services AWS utilisent des fonctions dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant pour ce service d'exécuter des applications dans Amazon EC2 ou de stocker des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, une fonction de service ou un rôle lié au service.
  - Autorisations de principaux : lorsque vous utilisez un utilisateur ou un rôle IAM afin d'effectuer des actions dans AWS, vous êtes considéré comme principal. Les politiques accordent des autorisations

au principal. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui déclenche une autre action dans un autre service. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour savoir si une action nécessite d'autres actions supplémentaires dans une stratégie, veuillez consulter URL LIST dans leRéférence de l'autorisation de service.

- Fonction de service : il s'agit d'un rôle IAM attribué à un service afin de réaliser des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour de plus amples informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.
- Rôle lié au service : un rôle lié au service est un type de fonction du service lié à un Service AWS. Le service peut assumer le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service s'affichent dans votre compte IAM et sont la propriété du service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

- Applications s'exécutant sur Amazon EC2 - vous pouvez utiliser un rôle IAM pour gérer des informations d'identification temporaires pour les applications s'exécutant sur une instance EC2 et effectuant des requêtes d'API AWS CLI ou AWS. Cette solution est préférable au stockage des clés d'accès au sein de l'instance EC2. Pour attribuer un rôle AWS à une instance EC2 et le rendre disponible à toutes les applications associées, vous pouvez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes qui s'exécutent sur l'instance EC2 d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez Utilisation d'un rôle IAM pour accorder des autorisations à des applications s'exécutant sur des instances Amazon EC2 dans le Guide de l'utilisateur IAM.

Pour savoir dans quel cas utiliser des rôles ou des utilisateurs IAM, consultez Quand créer un rôle IAM (au lieu d'un utilisateur) dans le Guide de l'utilisateur IAM.

Gestion de l'accès à l'aide de politiques

Vous contrôlez les accès dans AWS en créant des politiques et en les attachant à des identités IAM ou à des ressources AWS. Une politique est un objet dans AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit ses autorisations. Vous pouvez vous connecter en tant qu'utilisateur racine ou IAM ou vous pouvez endosser un rôle IAM. Lorsque vous effectuez ensuite une demande, AWS évalue les politiques relatives basées sur l'identité ou les ressources. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées dans AWS en tant que documents JSON. Pour plus d'informations sur la structure et le contenu des documents de politique JSON, consultez Présentation des politiques JSON dans le Guide de l'utilisateur IAM.

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

Chaque entité IAM (utilisateur ou rôle) démarre sans autorisation. En d'autres termes, par défaut, les utilisateurs ne peuvent rien faire, pas même changer leurs propres mots de passe. Pour autoriser un utilisateur à effectuer une opération, un administrateur doit associer une politique d'autorisations à ce dernier. Il peut également ajouter l'utilisateur à un groupe disposant des autorisations prévues. Lorsqu'un administrateur accorde des autorisations à un groupe, tous les utilisateurs de ce groupe se voient octroyer ces autorisations.

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 avec cette politique peut obtenir des informations utilisateur à partir de la AWS Management Console, de la AWS CLI ou de l'API AWS.

Politiques basées sur l'identité

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques

contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Création de politiques IAM dans le Guide de l'utilisateur IAM.

Les politiques basées sur l'identité peuvent être classées comme étant 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 lier à plusieurs utilisateurs, groupes et rôles de votre compte Compte AWS. Les politiques gérées incluent les politiques gérées par AWS et les politiques gérées par le client. Pour découvrir comment choisir entre une politique gérée et une politique en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment Amazon S3. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. 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 mandataires peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou des Services AWS.

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les politiques gérées AWS depuis IAM dans une politique basée sur une ressource.

Listes de contrôle d'accès (ACL)

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

Amazon S3, AWS WAF et Amazon VPC sont des exemples de services prenant en charge les ACL. Pour en savoir plus sur les listes de contrôle d'accès, consultez Présentation des listes de contrôle d'accès (ACL) dans le Guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de politiques moins courantes. 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 fonction 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 obtenues représentent la combinaison des politiques basées sur l'identité de l'entité et de ses limites d'autorisations. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques remplace l'autorisation. Pour plus d'informations sur les limites d'autorisations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.
- Politiques de contrôle des services (SCP) - les SCP sont des politiques JSON qui spécifient le nombre maximal d'autorisations pour une organisation ou une unité d'organisation (OU) dans AWS Organizations. AWS Organizations est un service qui vous permet de regrouper et de gérer de façon centralisée plusieurs Comptes AWS détenus par votre entreprise. Si vous activez toutes les fonctions d'une organisation, vous pouvez appliquer les politiques de contrôle de service (SCP) à l'un ou à l'ensemble de vos comptes. Les politiques de contrôle des services (SCP) limitent les autorisations pour les entités dans les comptes membres, y compris chaque utilisateur racine de compte Compte AWS.

Pour plus d'informations sur les organisations et les SCP, consultez Fonctionnement des SCP dans le Guide de l'utilisateur AWS Organizations.

- Politiques de séance : les politiques de séance sont des politiques avancées que vous passez en tant que paramètre lorsque vous programmez afin de créer une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de la séance obtenue 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 remplace l'autorisation. Pour plus d'informations, consultez Politiques de séance dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations obtenues sont plus compliquées à comprendre. Pour découvrir la façon dont AWS détermine s'il convient d'autoriser une demande en présence de plusieurs types de politiques, consultez Logique d'évaluation de politiques dans le Guide de l'utilisateur IAM.

Fonctionnement de AWS Resilience Hub avec IAM

Avant d'utiliser IAM pour gérer l'accès à Resilience Hub, assurez-vous de comprendre quelles sont les fonctions IAM qui peuvent être utilisées dans Resilience Hub. Pour obtenir une vue globale de la façon dont Resilience Hub et autresAWSservices fonctionnent avec IAM, consultezAWSServices qui fonctionnent avec IAMdans leIAM User Guide.

Table des matières

AWS Resilience HubPolitiques basées sur l'identité

Avec les stratégies IAM basées sur l'identité, vous pouvez spécifier des actions et ressources autorisées ou refusées et les conditions dans lesquelles les actions sont autorisées ou refusées. Resilience Hub prend en charge des actions, ressources et clés de condition spécifiques. Pour plus d'informations sur tous les éléments que vous utilisez dans une stratégie JSON, veuillez consulter.Références des éléments de stratégie JSON IAMdans leIAM User Guide.

Actions

Les administrateurs peuvent utiliser les politiques JSON AWS 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 politique possèdent généralement le même nom que l'opération d'API AWS 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.

Actions de stratégie dansAWS Resilience Hubutilisez le préfixe suivant avant l'action : `resiliencehub:`. Par exemple, pour accorder à une personne l'autorisation de créer une application, vous incluez le`resiliencehub:CreateApp`action dans leur politique. Les déclarations de politique doivent inclure un élément `Action` ou `NotAction`. AWS Resilience Hub définit son propre ensemble d'actions qui décrivent les tâches que vous pouvez effectuer avec ce service.

Pour spécifier plusieurs actions dans une seule déclaration, séparez-les par des virgules comme suit :

```
"Action": [
       "resiliencehub:action1",
       "resiliencehub:action2"
```

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

```
"Action": "resiliencehub:List*"
```

Pour afficher une liste desAWS Resilience Hubactions, voir https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_Operations.html dans leRéférence de l'API AWS Resilience Hub.

Ressources

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

L'élément de politique JSON `Resource` indique le ou les objets pour lesquels 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": "*"
```

Par exemple, une application possède l'ARN suivant :

```
arn:${Partition}:resiliencehub:${Region}:${Account}:app/${appId}
```

Pour plus d'informations sur le format des ARN, consultez Noms ARN (Amazon Resource Name) et Espaces de noms du service AWS.

Vous ne pouvez pas exécuter certaines actions Resilience Hub, telles que la création de ressources, sur une ressource précise. Dans ces cas-là, vous devez utiliser le caractère générique (*).

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

Certaines actions d'API Resilience Hub nécessitent plusieurs ressources. Pour spécifier plusieurs ressources dans une seule instruction, séparez leurs ARN par des virgules, comme dans l'exemple suivant.

```
"Resource": [
       "resource1",
```

```
        "resource2"
```

Clés de condition

Les administrateurs peuvent utiliser les politiques JSON AWS pour spécifier qui a accès à quoi. C'est à dire, quel principal peut exécuter 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 opération `OR` 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 à un service. Pour afficher toutes les clés de condition globales AWS, consultez Clés de contexte de condition globale AWS dans le Guide de l'utilisateur IAM.

Pour afficher une liste desAWS Resilience Hubclés de condition, consultez l'URL des CONDITIONS dans leRéférence de l'autorisation de service. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, consultez https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_Operations.html.

Politiques basées sur les ressources

Resilience Hub ne prend pas en charge les stratégies basées sur les ressource.

Autorisation basée sur les balises Resilience Hub

Vous pouvez attacher des balises aux ressources du Resilience Hub ou transmettre des balises dans une demande à Resilience Hub. Pour utiliser des balises pour contrôler l'accès, vous devez fournir des informations de balise dans leélément de conditiond'une stratégie utilisant le`aws:ResourceTag/key-name`,`aws:RequestTag/key-name`, ou`aws:TagKeys`clés de condition

Pour obtenir un exemple de stratégie, veuillez consulter Exemple : Utiliser des balises pour contrôler l'utilisation des ressources (p. 58).

Rôles IAM Resilience Hub

Un rôle IAM est une entité au sein de votre compte AWS qui dispose d'autorisations spécifiques.

Utilisation des informations d'identification temporaires avec Resilience Hu

Vous pouvez utiliser des informations d'identification temporaires pour vous connecter à l'aide de la fédération pour endosser un rôle IAM ou bien un rôle entre comptes. Vous obtenez des informations d'identification de sécurité temporaires en appelantAWS STSOpérations API, telles queAssumeRoleouGetFederationToken.

AWS Resilience Hub prend en charge l'utilisation des informations d'identification temporaires.

Exemples de stratégies AWS Resilience Hub

Par défaut, les utilisateurs et les rôles IAM ne sont pas autorisés à créer ou modifier les ressources AWS Resilience Hub. Ils ne peuvent pas non plus exécuter des tâches à l'aide de AWS Management Console, AWS CLI ou de l'API AWS. Un administrateur IAM doit créer des politiques IAM autorisant les utilisateurs et les rôles à exécuter des opérations d'API spécifiques sur les ressources spécifiées dont ils ont besoin. Il doit ensuite attacher ces politiques aux utilisateurs ou aux groupes IAM ayant besoin de ces autorisations.

Pour plus d'informations sur la création d'une stratégie IAM basée sur l'identité à l'aide de ces exemples de document de stratégie JSON, consultez.Création de stratégies dans l'onglet JSONdans leIAM User Guide.

Exemples

Bonnes pratiques en matière de politiques

Les stratégies basées sur l'identité permettent de déterminer si une personne peut créer, consulter ou supprimer des ressources 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 :

- Accorder le moins d'autorisations requises— Lorsque vous créez des stratégies personnalisées, accordez uniquement les autorisations requises pour exécuter une seule tâche. Commencez avec un minimum d'autorisations et accordez-en d'autres si nécessaire. Cette méthode est plus sûre que de commencer avec des autorisations trop permissives et d'essayer de les restreindre plus tard. Pour plus d'informations, consultez Accorder le moindre privilège possible dans le Guide de l'utilisateur IAM.
- Activer la MFA pour les opérations confidentielles : pour plus de sécurité, demandez aux utilisateurs IAM d'utiliser l'Authentification multifacteur (MFA) pour accéder à des ressources ou à des opérations d'API confidentielles. Pour plus d'informations, consultez Utilisation de l'authentification multifacteur (MFA) dans AWS dans le Guide de l'utilisateur IAM.
- Utiliser des conditions de politique pour davantage de sécurité : dans la mesure du possible, définissez les conditions dans lesquelles vos politiques basées sur l'identité autorisent l'accès à une ressource. Par exemple, vous pouvez rédiger les conditions pour spécifier une plage d'adresses IP autorisées d'où peut provenir une demande. Vous pouvez également écrire des conditions pour autoriser les requêtes uniquement à une date ou dans une plage de temps spécifiée, ou pour imposer l'utilisation de SSL ou de MFA. Pour de plus amples informations, veuillez consulterÉléments de stratégie JSON IAM : Conditiondans leIAM User Guide.

Exemple : Utiliser la console Resilience Hub

Pour accéder à la console AWS Resilience Hub, vous devez disposer d'un ensemble minimum d'autorisations. Ces autorisations doivent vous permettre de répertorier et de consulter les informations relatives aux ressources Resilience Hub dans votreAWS. Si vous créez une politique basée sur l'identité

qui est plus restrictive que les autorisations minimales requises, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs et rôles IAM) tributaires de cette politique.

La stratégie suivante accorde aux utilisateurs l'autorisation de répertorier et de consulter toutes les ressources dans la console Resilience Hub, mais pas à les créer, à les mettre à jour ou à les supprimer.

```
{
     "Version": "2012-10-17",
     "Statement": [
         {
             "Effect": "Allow",
             "Action": [
                 "resiliencehub:List*",
                 "resiliencehub:Get*"
             ],
             "Resource": "*"
         }
     ]
 }
```

Vous n'avez pas besoin d'accorder les autorisations minimales de console pour les utilisateurs qui effectuent des appels uniquement à AWS CLI ou à l'API AWS. Autorisez plutôt l'accès à uniquement aux actions qui correspondent à l'opération d'API que vous tentez d'effectuer.

Exemple : Liste des applications Resilience Hub disponibles

La stratégie suivante accorde aux utilisateurs l'autorisation de répertorier les applications Resilience Hub disponibles.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PolicyExample",
      "Effect": "Allow",
      "Action": [
          "resiliencehub:ListApps"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Exemple : Commencer une évaluation d'application

La stratégie suivante accorde aux utilisateurs l'autorisation de lancer une évaluation pour une situation précise.AWS Resilience Hubapplication.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PolicyExample",
      "Effect": "Allow",
      "Action": [
          "resiliencehub:StartAppAssessment"
      ],
      "Resource": [
        "arn:aws:resiliencehub:*:*:app/appId"
```

```
      ]
    }
  ]
}
```

Exemple : Supprimer une évaluation d'application

La stratégie suivante accorde aux utilisateurs l'autorisation de supprimer une évaluation pour une évaluation précise.AWS Resilience Hubapplication.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PolicyExample",
      "Effect": "Allow",
      "Action": [
          "resiliencehub:DeleteAppAssessment"
      ],
      "Resource": [
        "arn:aws:resiliencehub:*:*:app/appId"
      ]
    }
  ]
}
```

Exemple : Création d'un modèle de recommandation pour une application spécifique

La stratégie suivante accorde aux utilisateurs l'autorisation de créer un modèle de recommandation pour un modèle de recommandation spécifique.AWS Resilience Hubapplication.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PolicyExample",
      "Effect": "Allow",
      "Action": [
          "resiliencehub:CreateRecommendationTemplate"
      ],
      "Resource": [
        "arn:aws:resiliencehub:*:*:app/appId"
      ]
    }
  ]
}
```

Exemple : Supprimer un modèle de recommandation pour une application spécifique

La stratégie suivante accorde aux utilisateurs l'autorisation de supprimer un modèle de recommandation pour un modèle de recommandation spécifique.AWS Resilience Hubapplication.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PolicyExample",
      "Effect": "Allow",
```

```
      "Action": [
          "resiliencehub:DeleteRecommendationTemplate"
      ],
      "Resource": [
        "arn:aws:resiliencehub:*:*:app/appId"
      ]
    }
  ]
}
```

Exemple : Mettre à jour une application avec une stratégie de résilience spécifique

La stratégie suivante accorde aux utilisateurs l'autorisation de mettre à jour unAWS Resilience Hubapplication 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/*" }
      }
    }
  ]
}
```

Exemple : Utiliser des balises pour contrôler l'utilisation des ressources

La stratégie suivante permet aux utilisateurs d'utiliser des balises pour contrôler l'utilisation des ressources.

```
{
     "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "resiliencehub:StartAppAssessment"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Purpose": "Test"
                }
            }
        }
    ]
}
```

Exemple : Supprimer une application avec une balise spécifique

La stratégie suivante accorde aux utilisateurs l'autorisation de supprimer unAWS Resilience Hubapplication avec une balise spécifique.

```
{
     "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "resiliencehub:DeleteApp"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Purpose": "Test"
                }
            }
        }
    ]
}
```

Référence des autorisations AWS Resilience Hub

Les stratégies et extraits de stratégie IAM suivants définissent les autorisations nécessaires à l'utilisationAWS Resilience Hub.

Table des matières

Autorisations requises pour utiliserAWS Resilience Hubpour gérer une application en une seuleAWScompte

La stratégie IAM suivante est requise pour un seulAWSqui aura les autorisations nécessaires pour effectuer toutes les actions deAWS Resilience Hub.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "resiliencehub:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudformation:DescribeStacks",
                "cloudformation:ListStackResources",
                "cloudformation:ValidateTemplate"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
```

```
            "Action": [
                "servicecatalog:GetApplication",
                "servicecatalog:ListAssociatedResources"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "resource-groups:ListGroupResources",
                "resource-groups:GetGroup",
                "tag:GetResources"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:DescribeAlarms",
                "cloudwatch:GetMetricData",
                "cloudwatch:GetMetricStatistics",
                "cloudwatch:PutMetricData"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "fis:GetExperimentTemplate",
                "fis:ListExperimentTemplates",
                "fis:ListExperiments"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:GetParametersByPath"
            ],
            "Resource": "arn:aws:ssm:*:customer_account_id:parameter/ResilienceHub/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetBucketVersioning",
                "s3:GetReplicationConfiguration",
                "s3:ListBucket",
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:PutObject",
                "s3:GetObject"
            ],
            "Resource": "arn:aws:s3:::aws-resilience-hub-artifacts-*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "autoscaling:DescribeAutoScalingGroups"
            ],
            "Resource": "*"
```

```
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeFastSnapshotRestores",
                "ec2:DescribeInstances",
                "ec2:DescribeSnapshots",
                "ec2:DescribeVolumes",
                "ec2:DescribeNatGateways",
                "ec2:DescribeSubnets",
                "ec2:DescribeRegions"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "rds:DescribeDBClusters",
                "rds:DescribeDBInstanceAutomatedBackups",
                "rds:DescribeDBInstances",
                "rds:DescribeGlobalClusters",
                "rds:DescribeDBClusterSnapshots"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "elasticloadbalancing:DescribeTargetGroups"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "lambda:GetFunction",
                "lambda:GetFunctionConcurrency"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "backup:GetBackupPlan",
                "backup:GetBackupSelection",
                "backup:ListBackupPlans",
                "backup:ListBackupSelections"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "dynamodb:DescribeTable",
                "dynamodb:DescribeGlobalTable",
                "dynamodb:ListGlobalTables",
                "dynamodb:DescribeContinuousBackups",
                "dynamodb:DescribeLimits"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "elasticfilesystem:DescribeMountTargets",
                "elasticfilesystem:DescribeFileSystems"
```

```
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "sqs:GetQueueAttributes"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "apigateway:GET"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ecs:DescribeClusters",
                "ecs:ListServices",
                "ecs:DescribeServices",
                "ecs:DescribeCapacityProviders",
                "ecs:DescribeContainerInstances",
                "ecs:ListContainerInstances",
                "ecs:DescribeTaskDefinition"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "route53-recovery-readiness:ListReadinessChecks",
                "route53-recovery-readiness:GetResourceSet",
                "route53-recovery-readiness:GetReadinessCheckStatus",
                "route53-recovery-control-config:ListClusters",
                "route53:ListHealthChecks",
                "route53:ListHostedZones",
                "route53:ListResourceRecordSets",
                "route53:GetHealthCheck"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "drs:DescribeSourceServers",
                "drs:DescribeJobs",
                "drs:GetReplicationConfiguration"
            ],
            "Resource": "*"
        }

    ]
}
```

Note

Si vous souhaitez utiliser votre propre compartiment Amazon S3, vous pouvez passer le`bucketName`paramètre du paramètre de configuration`CreateRecommendationTemplate`Action d'API. Si c'est le cas, vous n'aurez pas besoin du`s3:CreateBucket`mais vous aurez besoin de la`s3:PutObject`et`s3:GetObject`autorisations pour le compartiment d'entrée.

Autorisations requises pour utiliserAWS Resilience Hubpour gérer les évaluations planifiées en un seulAWScompte

La stratégie IAM suivante est requise pour le`AwsResilienceHubPeriodicAssessmentRole`pour avoir les autorisations nécessaires pour effectuer des actions d'évaluation planifiées dansAWS Resilience Hub.

> **Note**
>
> Le nom du rôle est `AwsResilienceHubPeriodicAssessmentRole`.

```
{
    "Version": "2012-10-17",
    "Statement": [
    {
              "Effect": "Allow",
              "Action": [
                 "iam:GetRole",
                 "iam:PassRole",
                 "sts:AssumeRole"
             ],
             "Resource": "arn:aws:iam::primary_account_id:role/
AwsResilienceHubAdminAccountRole"
    },
        {
            "Effect": "Allow",
            "Action": [
                "resiliencehub:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudformation:DescribeStacks",
                "cloudformation:ListStackResources",
                "cloudformation:ValidateTemplate"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "servicecatalog:GetApplication",
                "servicecatalog:ListAssociatedResources"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "resource-groups:ListGroupResources",
                "resource-groups:GetGroup",
                "tag:GetResources"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:DescribeAlarms",
                "cloudwatch:GetMetricData",
                "cloudwatch:GetMetricStatistics",
                "cloudwatch:PutMetricData"
            ],
```

```
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "fis:GetExperimentTemplate",
                "fis:ListExperimentTemplates",
                "fis:ListExperiments"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:GetParametersByPath"
            ],
            "Resource": "arn:aws:ssm:*:customer_account_id:parameter/ResilienceHub/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetBucketVersioning",
                "s3:GetReplicationConfiguration",
                "s3:ListBucket",
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:PutObject",
                "s3:GetObject"
            ],
            "Resource": "arn:aws:s3:::aws-resilience-hub-artifacts-*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "autoscaling:DescribeAutoScalingGroups"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeFastSnapshotRestores",
                "ec2:DescribeInstances",
                "ec2:DescribeSnapshots",
                "ec2:DescribeVolumes",
                "ec2:DescribeNatGateways",
                "ec2:DescribeSubnets",
                "ec2:DescribeRegions"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "rds:DescribeDBClusters",
                "rds:DescribeDBInstanceAutomatedBackups",
                "rds:DescribeDBInstances",
                "rds:DescribeGlobalClusters",
                "rds:DescribeDBClusterSnapshots"
            ],
```

```
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "elasticloadbalancing:DescribeTargetGroups"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "lambda:GetFunction",
                "lambda:GetFunctionConcurrency"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "backup:GetBackupPlan",
                "backup:GetBackupSelection",
                "backup:ListBackupPlans",
                "backup:ListBackupSelections"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "dynamodb:DescribeTable",
                "dynamodb:DescribeGlobalTable",
                "dynamodb:ListGlobalTables",
                "dynamodb:DescribeContinuousBackups",
                "dynamodb:DescribeLimits"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "elasticfilesystem:DescribeMountTargets",
                "elasticfilesystem:DescribeFileSystems"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "sqs:GetQueueAttributes"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "apigateway:GET"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ecs:DescribeClusters",
                "ecs:ListServices",
                "ecs:DescribeServices",
```

```
                "ecs:DescribeCapacityProviders",
                "ecs:DescribeContainerInstances",
                "ecs:ListContainerInstances",
                "ecs:DescribeTaskDefinition"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "route53-recovery-readiness:ListReadinessChecks",
                "route53-recovery-readiness:GetResourceSet",
                "route53-recovery-readiness:GetReadinessCheckStatus",
                "route53-recovery-control-config:ListClusters",
                "route53:ListHealthChecks",
                "route53:ListHostedZones",
                "route53:ListResourceRecordSets",
                "route53:GetHealthCheck"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "drs:DescribeSourceServers",
                "drs:DescribeJobs",
                "drs:GetReplicationConfiguration"
            ],
            "Resource": "*"
        }
    ]
}
```

La stratégie d'approbation associée au rôle d'évaluations planifiées, (`AwsResilienceHubPeriodicAssessmentRole`), donne des autorisations pour leAWS Resilience Hubservice pour assumer le rôle des évaluations planifiées.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "resiliencehub.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Autorisations requises pour utiliserAWS Resilience Hubpour gérer les applications dans plusieurs comptes

Les stratégies d'autorisations IAM suivantes sont nécessaires si vous utilisezAWS Resilience Hubavec plusieurs comptes Chaque compte peut avoir besoin d'autorisations différentes en fonction de votre cas d'utilisation.

Autorisations du compte d'

La stratégie IAM suivante est requise pour leAWScompte qui ne dispose que des autorisations nécessaires pour appelerAWS Resilience Hub.

```
{
    "Version": "2012-10-17",
    "Statement": [
    {
        "Effect": "Allow",
        "Action": [
            "iam:GetRole",
            "iam:PassRole",
            "sts:AssumeRole"
        ],
        "Resource": "arn:aws:iam::primary_account_id:role/AwsResilienceHubAdminAccountRole"
    },
    {
        "Effect": "Allow",
        "Action": [
            "resiliencehub:*"
        ],
        "Resource": "*"
    }
  ]
}
```

Autorisations du compte administrateur

La stratégie IAM suivante est requise pour leAWScompte disposant des autorisations d'administrateur pourAWS Resilience Hub.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": ["sts:AssumeRole"],
      "Resource": ["arn:aws:iam::secondary_account_id:role/
AwsResilienceHubExecutorAccountRole"],
      "Effect": "Allow"
    }
  ]
}
```

La stratégie d'approbation associée au rôle d'administrateur est la suivante, où*caller_IAM_role*est le rôle utilisé dans le compte principal pour appeler les API pourAWS Resilience Hub.

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

Autorisations du rôle de compte exécuteur

La stratégie IAM suivante est requise pour leAWScompte qui aura les autorisations de rôle de compte d'exécuteur pourAWS Resilience Hub.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cloudformation:DescribeStacks",
                "cloudformation:ListStackResources",
                "cloudformation:ValidateTemplate"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "resource-groups:ListGroupResources",
                "resource-groups:GetGroup",
                "tag:GetResources"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:DescribeAlarms",
                "cloudwatch:GetMetricData",
                "cloudwatch:GetMetricStatistics",
                "cloudwatch:PutMetricData"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "fis:GetExperimentTemplate",
                "fis:ListExperimentTemplates",
                "fis:ListExperiments"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:DescribeAutomationExecutions"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "autoscaling:DescribeAutoScalingGroups"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeFastSnapshotRestores",
                "ec2:DescribeInstances",
                "ec2:DescribeSnapshots",
```

```
            "ec2:DescribeVolumes",
            "ec2:DescribeNatGateways",
            "ec2:DescribeSubnets",
            "ec2:DescribeRegions"
        ],
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "rds:DescribeDBClusters",
            "rds:DescribeDBInstanceAutomatedBackups",
            "rds:DescribeDBInstances",
            "rds:DescribeGlobalClusters",
            "rds:DescribeDBClusterSnapshots"
        ],
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "elasticloadbalancing:DescribeTargetGroups"
        ],
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "lambda:GetFunction",
            "lambda:GetFunctionConcurrency"
        ],
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "backup:GetBackupPlan",
            "backup:GetBackupSelection",
            "backup:ListBackupPlans",
            "backup:ListBackupSelections"
        ],
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "dynamodb:DescribeTable",
            "dynamodb:DescribeGlobalTable",
            "dynamodb:ListGlobalTables",
            "dynamodb:DescribeContinuousBackups",
            "dynamodb:DescribeLimits"
        ],
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "elasticfilesystem:DescribeMountTargets",
            "elasticfilesystem:DescribeFileSystems"
        ],
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "s3:GetBucketVersioning",
```

```
                "s3:GetReplicationConfiguration",
                "s3:ListBucket",
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "sqs:GetQueueAttributes"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "apigateway:GET"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:GetParametersByPath"
            ],
            "Resource": "arn:aws:ssm:*:secondary_account_id:parameter/ResilienceHub/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ecs:DescribeClusters",
                "ecs:ListServices",
                "ecs:DescribeServices",
                "ecs:DescribeCapacityProviders",
                "ecs:DescribeContainerInstances",
                "ecs:ListContainerInstances",
                "ecs:DescribeTaskDefinition"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "route53-recovery-readiness:ListReadinessChecks",
                "route53-recovery-readiness:GetResourceSet",
                "route53-recovery-readiness:GetReadinessCheckStatus",
                "route53-recovery-control-config:ListClusters",
                "route53:ListHealthChecks",
                "route53:ListHostedZones",
                "route53:ListResourceRecordSets",
                "route53:GetHealthCheck"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "drs:DescribeSourceServers",
                "drs:DescribeJobs",
                "drs:GetReplicationConfiguration"
            ],
            "Resource": "*"
        }
    ]
}
```

Stratégie d'approbation associée au rôle de compte d'exécuteur. Cela donne l'autorisation pour le rôle de compte principal (`AwsResilienceHubAdminAccountRole`) pour assumer les comptes secondaires.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::primary_account_id:role/AwsResilienceHubAdminAccountRole"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Résolution des problèmes d'identité et d'accès avec AWS Resilience Hub

Utilisez les informations suivantes pour identifier et résoudre les problèmes d'accès courants que vous pouvez rencontrer lorsque vous travaillez avec Resilience Hub et IAM.

Problèmes

- Je ne suis pas autorisé à exécuter : iam:PassRole (p. 71)
- Je veux afficher mes clés d'accès (p. 71)
- Je suis un administrateur et je veux autoriser d'autres utilisateurs à accéder à Resilience Hub (p. 72)
- Je veux autoriser des personnes extérieures à monAWSpour accéder à mes ressources Resilience Hub (p. 72)

Je ne suis pas autorisé à exécuter : iam:PassRole

Si vous recevez un message d'erreur selon lequel vous n'êtes pas autorisé à exécuter l'action `iam:PassRole`, vous devez contacter votre administrateur pour obtenir de l'aide. Votre administrateur est la personne qui vous a fourni votre nom d'utilisateur et votre mot de passe. Demandez à cette personne de mettre à jour vos stratégies pour vous permettre de transmettre un rôle à Resilience Hub.

Certains Services AWS vous permettent de transmettre un rôle existant à ce service, au lieu de créer un nouveau rôle de service ou 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 exécuter une action dans Resilience Hub. Toutefois, l'action nécessite que le service ait des autorisations accordées par une fonction du 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, Mary demande à son administrateur de mettre à jour ses politiques pour lui permettre d'exécuter l'action `iam:PassRole`.

Je veux afficher mes clés d'accès

Une fois les clés d'accès utilisateur IAM créées, vous pouvez afficher votre ID de clé d'accès à tout moment. Toutefois, vous ne pouvez pas revoir votre clé d'accès secrète. Si vous perdez votre clé d'accès secrète, vous devez créer une nouvelle paire de clés.

Les clés d'accès se composent de deux parties : un ID de clé d'accès (par exemple, `AKIAIOSFODNN7EXAMPLE`) et une clé d'accès secrète (par exemple, `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`). À l'instar d'un nom d'utilisateur et un mot de passe, vous devez utiliser à la fois l'ID de clé d'accès et la clé d'accès secrète pour authentifier vos demandes. Gérez vos clés d'accès de manière aussi sécurisée que votre nom d'utilisateur et votre mot de passe.

> **Important**
>
> Ne communiquez pas vos clés d'accès à un tiers, même pour qu'il vous aide à trouver votre ID utilisateur canonique. En effet, vous lui accorderiez ainsi un accès permanent à votre compte.

Lorsque vous créez une paire de clé d'accès, enregistrez l'ID de clé d'accès et la clé d'accès secrète dans un emplacement sécurisé. La clé d'accès secrète est accessible uniquement au moment de sa création. Si vous perdez votre clé d'accès secrète, vous devez ajouter de nouvelles clés d'accès pour votre utilisateur IAM. Vous pouvez avoir un maximum de deux clés d'accès. Si vous en avez déjà deux, vous devez supprimer une paire de clés avant d'en créer une nouvelle. Pour afficher les instructions, consultez Gestion des clés d'accès dans le Guide de l'utilisateur IAM.

Je suis un administrateur et je veux autoriser d'autres utilisateurs à accéder à Resilience Hub

Pour permettre à d'autres utilisateurs d'accéder à Resilience Hub, vous devez créer une entité IAM (utilisateur ou rôle) pour la personne ou l'application nécessitant cet accès. Ils utiliseront les informations d'identification de cette entité pour accéder à AWS. Vous devez ensuite associer une stratégie à l'entité qui leur accorde les autorisations appropriées dans Resilience Hub.

Pour démarrer immédiatement, consultez Création de votre premier groupe et utilisateur délégué IAM dans le Guide de l'utilisateur IAM.

Je veux autoriser des personnes extérieures à monAWSpour accéder à mes ressources 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 la personne à qui vous souhaitez confier le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACL), vous pouvez utiliser ces politiques pour donner l'accès à vos ressources.

Pour en savoir plus, consultez les éléments suivants :

- Pour savoir si Resilience Hub prend en charge ces fonctionnalités, consultezFonctionnement de AWS Resilience Hub avec IAM (p. 52).
- Pour savoir comment octroyer l'accès à vos ressources à des Comptes AWS dont vous êtes propriétaire, veuillez consulter la section Fournir l'accès à un utilisateur IAM dans un autre Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.
- Pour savoir comment octroyer l'accès à vos ressources à des Comptes AWS tiers, consultez Fournir l'accès aux Comptes AWS appartenant à des tiers dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.
- Pour découvrir quelle est la différence entre l'utilisation des rôles et l'utilisation des politiques basées sur les ressources pour l'accès entre comptes, consultez Différence entre les rôles IAM et les politiques basées sur les ressources dans le Guide de l'utilisateur IAM.

Sécurité de l'infrastructure dans AWS Resilience Hub

En tant que service géré,AWS Resilience Hub; (Resilience Hub) est protégé par leAWSprocédures de sécurité réseau globales décrites dans leAmazon Web Services : Présentation des processus de sécuritélivre blanc.

Vous utilisezAWSappels d'API publiés pour accéder à Resilience Hub via le réseau. Les clients doivent supporter le protocole TLS (Sécurité de la couche transport) 1.0 ou une version ultérieure. Nous recommandons TLS 1.2 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.

Utilisation d'autres services

Cette section décritAWSservices qui interagissent avecAWS Resilience Hub.

Création de ressources AWS Resilience Hub avecAWS CloudFormation

AWS Resilience Hub est intégré àAWS CloudFormation, un service qui vous aide à modéliser et à configurer votreAWSafin que vous puissiez consacrer moins de temps à la création et à la gestion de vos ressources et de votre infrastructure. Vous créez un modèle qui décrit tous les élémentsAWSles ressources que vous souhaitez (telles que AWS# ResilienceHub# :ResiliencyPolicy et AWS# ResilienceHub# :App), etAWS CloudFormationalloue et configure ces ressources à votre place.

Lorsque vous utilisezAWS CloudFormation, vous pouvez réutiliser votre modèle pour configurer vos ressources Resilience Hub de manière cohérente et répétée. Décrivez vos ressources une seule fois, puis allouez-les autant de fois que vous le souhaitez dans plusieursAWScomptes et régions.

Hub de Résilience etAWS CloudFormationmodèles

Pour mettre en service et configurer des ressources pour Resilience Hub et les services associés, vous devez maîtriserAWS CloudFormationmodèles. Les modèles sont des fichiers texte formatés en JSON ou YAML. Ces modèles décrivent les ressources que vous souhaitez allouer dans vos piles AWS CloudFormation. Si JSON ou YAML ne vous est pas familier, vous pouvez utiliser AWS CloudFormation Designer pour vous aider à démarrer avec des modèles AWS CloudFormation. Pour plus d'informations, consultez Qu'est-ce qu'AWS CloudFormation Designer ? dans le Guide de l'utilisateur AWS CloudFormation.

Resilience Hub prend en charge la création d'AWS# ResilienceHub# :ResiliencyPolicy et AWS# ResilienceHub# :App dansAWS CloudFormation. Pour de plus amples informations, y compris des exemples de modèles JSON et YAML pour AWS# ResilienceHub# :ResiliencyPolicy et AWS# ResilienceHub# :App, consultez leAWS Resilience Hub resource type referencedans leAWS CloudFormationGuide de l'utilisateur.

Vous pouvez utiliserAWS CloudFormationpiles pour définir les applications Resilience Hub. Une pile permet de gérer les ressources connexes en tant qu'unité unique. Une pile peut contenir toutes les ressources dont vous avez besoin pour exécuter une application web, telle qu'un serveur web ou des règles de mise en réseau.

En savoir plus sur AWS CloudFormation

Pour plus d'information sur AWS CloudFormation, consultez les ressources suivantes :

- AWS CloudFormation
- Guide de l'utilisateur AWS CloudFormation
- Référence API AWS CloudFormation
- Guide de l'utilisateur de l'interface de ligne de commande AWS CloudFormation

AWS CloudTrail

AWS Resilience Hub(Resilience Hub) est intégré àAWS CloudTrail, un service qui enregistre les actions réalisées par un utilisateur, un rôle ou unAWSservice dans Resilience Hub. CloudTrail capture les appels d'API pour Resilience Hub en tant qu'événements. Les appels capturés incluent les appels de la console Resilience Hub et les appels de code aux opérations de l'API Resilience Hub. Si vous créez un journal d'activité, vous pouvez activer la livraison continue d'événements CloudTrail à un compartiment Amazon S3, y compris des événements pour Resilience Hub. Si vous ne configurez pas de journal d'activité, vous pouvez toujours afficher les événements les plus récents dans la console CloudTrail dans Historique des événements. Avec les informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été envoyée à Resilience Hub, l'adresse IP à partir de laquelle la demande a été effectuée, l'auteur et la date de la demande, ainsi que d'autres détails.

Pour de plus amples informations sur CloudTrail, veuillez consulter le AWS CloudTrailGuide de l’utilisateur .

AWS Systems Manager

AWS Resilience Hubtravaille avec Systems Manager pour automatiser les étapes de vos SOP en fournissant un certain nombre de documents SSM que vous pouvez utiliser comme base pour ces SOP.

AWS Resilience Hubvous fournitAWS CloudFormationmodèles contenant les rôles IAM nécessaires à l'exécution de différents documents Systems Manager, un rôle par document avec les autorisations requises pour le document spécifique. Après avoir créé une pile avec leAWS CloudFormation, il va configurer les rôles IAM et enregistrer les métadonnées dans le paramètre Systems Manager pour le document d'automatisation de Systems Manager à exécuter pour différentes procédures de récupération.

Pour plus d'informations sur l'utilisation des SOP, consultezProcédures d'exploitation normalisées (p. 35).

Historique du Guide de l'utilisateur AWS Resilience Hub

Le tableau suivant décrit la documentation pour cette version du AWS Resilience Hub.

- Version de l'API : dernière en date
- Dernière mise à jour de la documentation : 10 novembre 2021

update-history-change	update-history-description	update-history-date
Nouveau contenu : Concept de statut de conformité des applications (p. 2)	Ajout du type d'état Modifications détectées.	2 juin 2022
Présentation d'AWS Resilience Hub (p. 76)	AWS Resilience Hubest désormais disponible. Ce guide décrit comment utiliser les.AWS Resilience Hubpour analyser votre infrastructure, obtenir des recommandations pour améliorer la résilience de votreAWSapplications, vérifiez les scores de résilience, et bien plus encore.	10 novembre 2021

Glossaire AWS

Pour connaître la terminologie la plus récente d'AWS, consultez le glossaire AWS dans la Référence générale d'AWS.

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.