aws

ユーザーガイド

AWS レジリエンスハブ

AWS レジリエンスハブ: ユーザーガイド

Table of Contents

とは何ですか AWS Resilience Hub?

AWS Resilience Hub アプリケーションのレジリエンス態勢を一元的に管理および改善できる場所です。 AWS AWS Resilience Hub レジリエンス目標を定義し、その目標に対するレジリエンス態勢を評価し、Well-Architected Frameworkに基づいて改善のための推奨事項を実施することができます。 AWS AWS Resilience Hub内部では、Amazon Fault Injection Service のテストを作成して実行することもできます。これにより、アプリケーションの実際の障害を模倣して、依存関係の理解を深め、潜在的な弱点を明らかにすることができます。 AWS Resilience Hub AWS レジリエンス体制を継続的に強化するために必要なすべてのサービスとツールを 1 か所にまとめています。 AWS Resilience Hub 他のサービスと連携して推奨事項を提示し、アプリケーションリソースの管理を支援します。詳細については、「他の サービスでの使用」を参照してください。

次の表は、関連するすべての障害耐性サービスのドキュメントリンクを示しています。

AWS 関連するレジリエンシーサービスと参考資料

AWS レジリエンシーサービス	ドキュメントのリンク
AWS Elastic Disaster Recovery	Elastic ディザスタリカバリとは
AWS Backup	とは AWS Backup
Amazon Route 53 Application Recovery Controller (Route 53 ARC)	Amazon Route 53 Application Recovery Controller とは

トピック

- AWS Resilience Hub — レジリエンス管理
- AWS Resilience Hub — レジリエンステスト
- AWS Resilience Hub コンセプト
- AWS Resilience Hub サポート対象リソース

AWS Resilience Hub — レジリエンス管理

AWS Resilience Hub アプリケーションの耐障害性を一元的に定義、検証、追跡できます AWS 。 AWS Resilience Hub アプリケーションを中断から保護し、復旧コストを削減して事業継続性を最

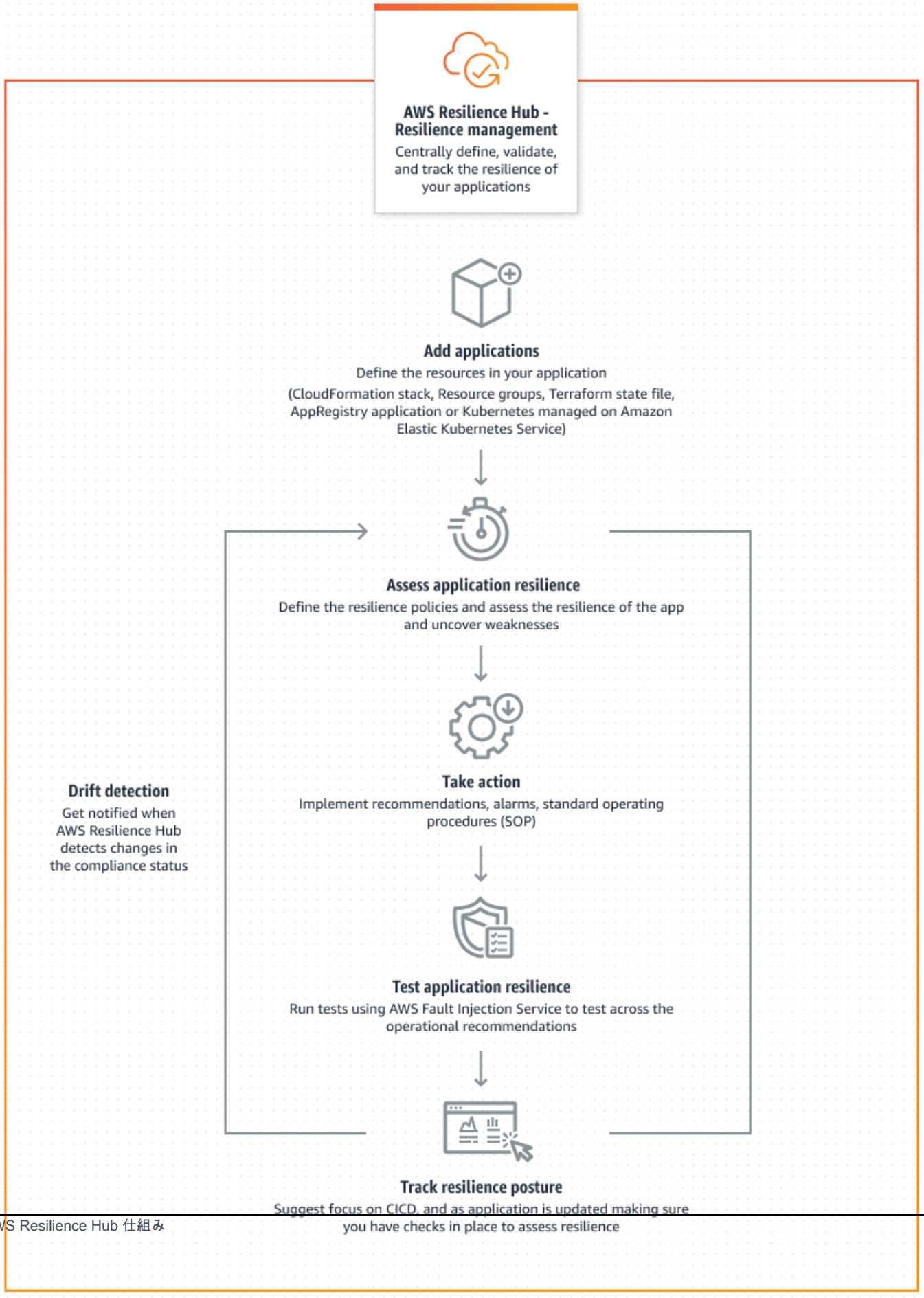
適化し、コンプライアンスや規制の要件を満たすのに役立ちます。を使用すると AWS Resilience Hub 、次のことが可能になります。

- インフラストラクチャを分析し、アプリケーションの障害耐性を向上させるための推奨事項を入手してください。推奨事項には、アプリケーションの障害耐性を向上させるためのアーキテクチャガイダンスに加えて、障害耐性ポリシーを満たすためのコード、テスト、アラーム、標準作業手順書 (SOP) を実装するためのコードが含まれています。これらのコードは、統合と配信 (CI/CD) パイプラインでアプリケーションとともにデプロイおよび実行できます。
- 目標復旧時間 (RTO) と目標復旧時点 (RPO) の目標をさまざまな条件で評価します。
- 復旧コストを削減しながら、事業継続性を最適化します。
- 本番環境で問題が発生する前に問題を特定して解決します。

アプリケーションを本番環境にデプロイしたら、CI/CD AWS Resilience Hub パイプラインに追加して、本番環境にリリースされる前にすべてのビルドを検証できます。

仕組み AWS Resilience Hub

次の図は、 AWS Resilience Hub 仕組みの概要を示しています。


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

説明

AWS CloudFormation スタック、Terraform 状態ファイル、 AWS Resource Groups Amazon Elastic Kubernetes Service クラスターからリソースをインポートしてアプリケーションを記述します。または、ですでに定義されているアプリケーションから選択することもできます。 AWS Service Catalog AppRegistry

定義

アプリケーションの回復力ポリシーを定義します。これらのポリシーには、アプリケーション、インフラストラクチャ、アベイラビリティーゾーン、リージョンの中断に関する RTO と RPO の目標が含まれます。これらの目標は、アプリケーションが障害耐性ポリシーを満たしているかどうかを推定するために使用されます。

評価

アプリケーションについて説明し、それに障害耐性ポリシーを添付したら、障害耐性評価を実行します。 AWS Resilience Hub 評価では、 AWS Well-Architected Frameworkのベストプラクティスを使用してアプリケーションのコンポーネントを分析し、潜在的な耐障害性の弱点を明らかにします。これらの弱点は、インフラストラクチャの設定が不完全であること、設定ミス、または追加の設定改善が必要な状況によって発生する可能性があります。障害耐性を向上させるには、評価レポートの推奨事項に従ってアプリケーションと障害耐性ポリシーを更新してください。推奨事項には、コンポーネント、アラーム、テスト、リカバリ SOP の設定が含まれます。その後、別の評価を行い、その結果を前回のレポートと比較して、障害耐性がどの程度向上するかを確認できます。推定ワークロード RTO と推定ワークロード RPO が RTO と RPO 目標を達成するまで、このプロセスを繰り返します。

検証

テストを実行して、 AWS リソースの耐障害性と、アプリケーション、インフラストラクチャ、アベイラビリティーゾーン、インシデントからの回復にかかる時間を測定します。 AWS リージョン 回復力を測定するために、これらのテストではリソースの停止をシミュレートします。AWS 停止の例としては、ネットワークの利用不可エラー、フェイルオーバー、プロセスの停止、Amazon RDS のブートリカバリ、アベイラビリティーゾーンの問題などがあります。

表示と追跡

アプリケーションを本番環境にデプロイした後も、 AWS AWS Resilience Hub を使用してアプリケーションの耐障害性の状態を引き続き追跡できます。障害が発生した場合、オペレーターは停止状況を確認し、関連する復旧プロセスを開始できます。 AWS Resilience Hub

AWS Resilience Hub — レジリエンステスト

AWS Resilience Hub AWS ワークロードに対して Amazon Fault Injection Service (AWS FIS) のテストや実験を行い、最適な耐障害性を維持することができます。これらのテストでは、アプリケーションがどのように反応するかを観察できるように、破壊的なイベントを生成することでアプリケーションにstress をかけます。 AWS FIS あらかじめ用意された複数のシナリオと、中断の原因となるアクションを多数用意しています。さらに、生産で実験を実行するために必要なコントロールとガードレールも含まれています。コントロールとガードレールには、特定の条件が満たされた場合に自動ロールバックを実行したり、実験を停止したりするオプションが含まれています。 AWS FIS AWS Resilience Hub を使用してコンソールから実験を実行し始めるには、セクションで定義されている前提条件を満たしてください。the section called “前提条件”

次の表は、 AWS FIS ナビゲーションペインで使用できるすべてのオプションと、 AWS FIS AWS FIS コンソールからテストの使用を開始する手順を含む関連ドキュメントへのリンクを示しています。 AWS Resilience Hub

AWS FIS ナビゲーションメニューのオプションと参考資料

AWS FIS ナビゲーションメニューオプション	AWS FIS ドキュメンテーション
[回復力テスト]	実験テンプレートの作成
[シナリオライブラリ]	AWS FIS 図書館
[実験テンプレート]	の実験テンプレート AWS FIS

次の表は、 AWS FIS レジリエンステストセクションのドロップダウンメニューから利用できるすべてのオプションと、 AWS FIS AWS FIS AWS Resilience Hub コンソールからテストの使用を開始する手順を含む関連ドキュメントへのリンクを示しています。

AWS FIS ドロップダウンメニューのオプションと参考資料

AWS FIS ドロップダウンメニューオプション	AWS FIS ドキュメンテーション
[実験テンプレートの作成]	実験テンプレートの作成
[シナリオから実験を作成]	シナリオの使用

AWS Resilience Hub コンセプト

これらの概念は、アプリケーションの耐障害性を向上させ、 AWS Resilience Hubアプリケーションの停止を防ぐためののアプローチをよりよく理解するのに役立ちます。

回復性

可用性を維持し、ソフトウェアや運用の中断から指定期間内に復旧する機能。

目標復旧時点 (RPO)

データが最後に復旧した時点からの最大許容時間。これにより、最後の回復時点からサービスが中断されるまでの間に許容できるデータ喪失がどの程度になるかが決まります。

目標復旧時間 (RTO)

サービスが中断してから復旧するまでの最大許容時間 (遅延)。これにより、サービスが利用できなくなったときに許容できる時間枠が決まります。

ワークロードの推定復旧時間目標

推定ワークロード復旧時間目標 (推定ワークロード RTO) は、インポートしたアプリケーション定義に基づいてアプリケーションが満たすと推定され、評価を実行する RTO です。

ワークロード目標復旧時点

推定ワークロード回復ポイント目標 (推定ワークロード RPO) は、インポートしたアプリケーション定義に基づいてアプリケーションが達成すると推定され、評価を実行する RPO です。

アプリケーション

AWS Resilience Hub アプリケーションとは、 AWS サポート対象のリソースの集まりであり、それらのリソースは継続的に監視および評価され、耐障害性を管理しています。

アプリケーションコンポーネント

1 つのユニットとして動作し、 AWS 障害が発生する関連リソースの集まり。たとえば、プライマリデータベースとレプリカデータベースがある場合、両方のデータベースは同じアプリケーションコンポーネント (AppComponent) に属します。

AWS Resilience Hub AWS どのリソースをどのタイプに属させること
ができるかを決定します AppComponent。例えば、ある `DBInstance`
が、`AWS::ResilienceHub::DatabaseAppComponent` に属していても
`AWS::ResilienceHub::ComputeAppComponent` に属さない場合があります。

アプリケーションコンプライアンスステータス

AWS Resilience Hub アプリケーションの以下のコンプライアンスステータスタイプを報告します。

ポリシーに一致

アプリケーションは、ポリシーで定義されている RTO と RPO 目標を達成すると推定されます。そのコンポーネントはすべて、定義されたポリシー目標を達成しています。たとえば、 AWS 地域全体での中断について、RTO と RPO の目標を 24 時間に設定したとします。 AWS Resilience Hub バックアップがフォールバックリージョンにコピーされていることを確認できます。それでも、バックアップ標準作業手順書 (SOP) からの復旧を維持し、それをテストして時間を計ることが求められます。これは運用上の推奨事項に含まれており、全体的な障害耐性スコアの一部でもあります。

ポリシー違反

アプリケーションがポリシーで定義されている RTO と RPO 目標を達成していると推定できませんでした。そのうちの 1 AppComponents つ以上がポリシー目標を達成していません。たとえば、AWS リージョン間の中断について RTO と RPO の目標を 24 時間に設定したが、データベース構成には、グローバルレプリケーションやバックアップコピーなど、リージョン間の復旧方法が含まれていないとします。

評価は行われていません

申請には評価が必要です。現在、評価も追跡もされていません。

変更が検出されました

まだ評価されていない新しい発行済みバージョンのアプリケーションがあります。

障害耐性ドリフト

AWS Resilience Hub アプリケーションの評価中にドリフト検出を実行して、アプリケーションが耐障害性ポリシーに準拠しているかどうかを確認します。比較のため、 AWS Resilience Hub 前回のアプリケーションの評価で定義された耐障害性ポリシーを使用します。

- ドリフト — アプリケーションが障害耐性ポリシーに違反しており、リスクにさらされていることを示します。
- ドリフトなし — アプリケーションのコンプライアンスが前回の評価から変わっていないことを示します。

障害耐性評価

AWS Resilience Hub ギャップと考えられる対策のリストを使用して、選択したポリシーが災害からの回復と継続にどの程度効果があるかを測定します。各アプリケーションコンポーネントまたはアプリケーションのポリシー遵守状況を評価します。このレポートには、コスト最適化に関する推奨事項と潜在的な問題に関する参考資料が含まれています。

障害耐性スコア

AWS Resilience Hub アプリケーションの耐障害性ポリシー、アラーム、標準運用手順 (SOP)、およびテストを満たすために、アプリケーションが当社の推奨事項にどの程度従っているかを示すスコアを生成します。

中断タイプ

AWS Resilience Hub 次のような停止に対する耐障害性を評価するのに役立ちます。

アプリケーション

インフラストラクチャは正常だが、アプリケーションまたはソフトウェアスタックは必要に応じて動作しません。これは、新しいコードのデプロイ、設定の変更、データの破損、またはダウンストリームの依存関係の誤動作の後に発生することがあります。

[クラウドインフラストラクチャ]

システム停止のため、クラウドインフラストラクチャが期待どおりに機能していません。1 つ以上のコンポーネントのローカルエラーが原因で、機能停止が発生する可能性があります。ほとんどの場合、この種の機能停止は、障害のあるコンポーネントを再起動、リサイクル、またはリロードすることで解決されます。

[クラウドインフラストラクチャ AZ の中断]

1 つ以上のアベイラビリティーゾーンが使用できません。このタイプの障害は、別のアベイラビリティーゾーンに切り替えることで解決できます。

[クラウドインフラストラクチャリージョンインシデント]

1 つ以上のリージョンが利用できません。このタイプのインシデントは、別の AWS リージョンに切り替えることで解決できます。

故障注入実験

AWS Resilience Hub さまざまな種類の停止に対するアプリケーションの耐障害性を検証するためのテストを推奨します。停止には、アプリケーション、インフラストラクチャ、アベイラビリティーゾーン (AZ)、またはアプリケーションコンポーネントの AWS リージョン インシデントが含まれます。

これらの実験では、次の作業を行うことができます。

- 障害を発生させます。
- アラームが停止を検出できることを確認します。
- 復旧手順または標準作業手順書 (SOP) が正しく機能して、停止状態からアプリケーションを復旧できることを確認します。

SOP のテストでは、推定ワークロード RTO と推定ワークロード RPO を測定します。さまざまなアプリケーション構成をテストし、出力 RTO と RPO がポリシーで定義された目標を満たしているかどうかを測定できます。

SOP

標準作業手順書 (SOP) は、システム停止やアラームが発生した場合にアプリケーションを効率的に復旧するための規範的な一連の手順です。アプリケーションの評価に基づいて、 AWS Resilience Hub 一連のSOPを推奨し、障害発生前にSOPを準備、テスト、測定して、タイムリーな復旧を確保することを推奨します。

AWS Resilience Hub サポート対象リソース

障害が発生した場合にアプリケーションのパフォーマンスに影響するリソースは、 AWS Resilience Hub `AWS::RDS::DBInstance`やなどのトップレベルのリソースによって完全にサポートされます。`AWS::RDS::DBCluster`

AWS Resilience Hub サポートされているすべてのサービスのリソースを評価に含めるために必要な権限の詳細については、を参照してください。the section called “AWSResilienceHubAsssessmentExecutionPolicy”

AWS Resilience Hub AWS 以下のサービスのリソースをサポートします。

- コンピューティング
  - Amazon Elastic Compute Cloud (Amazon EC2)
  - AWS Lambda
  - Amazon Elastic Kubernetes Service (Amazon EKS)
  - Amazon Elastic Container Service (Amazon ECS)
  - AWS Step Functions
- データベース
  - Amazon Relational Database Service (Amazon RDS)
  - Amazon DynamoDB
  - Amazon DocumentDB
- ネットワークとコンテンツ配信
  - Amazon Route 53
  - Elastic Load Balancing
  - ネットワークアドレス変換 (NAT)
- [Storage (ストレージ)]
  - Amazon Elastic Block Store (Amazon EBS)
  - Amazon Elastic File System (Amazon EFS)
  - Amazon Simple Storage Service (Amazon S3)
  - Amazon FSx for Windows File Server
- その他
  - Amazon API Gateway
  - Amazon Route 53 Application Recovery Controller (Amazon Route 53 ARC)
  - Amazon Simple Notification Service
  - Amazon Simple Queue Service
  - AWS Auto Scaling
  - AWS Backup
  - AWS 伸縮自在な災害復旧

Note

- AWS Resilience Hub 各リソースのサポート対象インスタンスを表示できるようにすることで、アプリケーションリソースの透明性を高めます。さらに、 AWS Resilience Hub 評価プロセス中にリソースインスタンスを検出しながら、各リソースの固有のインスタンスを特定することで、より正確な耐障害性に関する推奨事項を提示します。アプリケーションにリソースインスタンスを追加する方法については、AWS Resilience Hub のアプリケーションリソースへのタグ付け を参照してください。
- AWS Resilience Hub Amazon EKS とAmazon ECS をサポートしています。 AWS Fargate
- AWS Resilience Hub AWS Backup 以下のサービスの一環としてリソースの評価をサポートします。
  - Amazon EBS
  - Amazon EFS
  - Amazon S3
  - Amazon Aurora Global Database
  - Amazon DynamoDB
  - Amazon RDS サービス
  - Amazon FSx for Windows File Server
- Amazon Route 53 ARC では、Amazon DynamoDB グローバル、Elastic Load Balancing、Amazon RDS、 AWS Resilience Hub およびグループのみを評価します。 AWS Auto Scaling
- AWS Resilience Hub クロスリージョンリソースを評価するには、リソースを 1 つのアプリケーションコンポーネントにグループ化します。各 AWS Resilience Hub アプリケーションコンポーネントでサポートされるリソースとグループリソースの詳細については、リソースをグループ化する AppComponent を参照してください。
- 現在、Amazon EKS クラスターが配置されている場合、またはアプリケーションがオプトインが有効なリージョンで作成されている場合、Amazon EKS AWS Resilience Hub クラスターのクロスリージョン評価はサポートされていません。 AWS
- 現在、は次の Kubernetes AWS Resilience Hub リソースタイプのみを評価しています。
  - デプロイ
  - ReplicaSets
  - ポッド

AWS Resilience Hub 以下のタイプのリソースは無視されます。

- 推定ワークロード RTO または推定ワークロード RPO に影響しないリソース — 推定ワークロード RTO または推定ワークロード RPO に影響を与えない `AWS::RDS::DBParameterGroup` のようなリソースは、 AWS Resilience Hubで無視されます。
- 非トップレベルリソース — トップレベルのリソースのプロパティをクエリすることで他のプロパティを導出できるため、 AWS Resilience Hub トップレベルのリソースのみをインポートします。例えば、`AWS::ApiGateway::RestApi` と `AWS::ApiGatewayV2::Api` は Amazon API Gateway でサポートされるリソースです。ただし、`AWS::ApiGatewayV2::Stage` は最上位のリソースではありません。そのため、によるインポートは行われません。 AWS Resilience Hub

> **Note**
>
> サポートされていないデータソース
>
> - AWS Resource Groups (Amazon Route 53 RecordSets と API-GW HTTP) と Amazon Aurora グローバルリソースを使用して複数のリソースを識別することはできません。評価の一環としてこれらのリソースを分析する場合は、リソースを手動でアプリケーションに追加する必要があります。ただし、評価用に Amazon Aurora Global リソースを追加する場合は、Amazon RDS インスタンスのアプリケーションコンポーネントとグループ化する必要があります。リソースを編集する詳細については、「the section called “アプリケーションリソースの表示”」を参照してください。
> - これらのリソースはアプリケーションの復旧に影響する可能性がありますが、 AWS Resilience Hub 現時点では完全にはサポートされていません。 AWS Resilience Hub AWS CloudFormation アプリケーションがスタック、Terraform 状態ファイル、またはアプリケーションによって支えられている場合、サポートされていないリソースについてユーザーに警告するよう努めています AWS Resource Groups。 AppRegistry

はじめに

このセクションでは、AWS Resilience Hub を使い始める方法について説明します。これには、アカウントの AWS Identity and Access Management (IAM) 権限の作成が含まれます。

前提条件

AWS Resilience Hub開始するには、以下の前提条件を満たす必要があります。

- AWS のアカウント –AWS Resilience Hub で 使用したいアカウントタイプ (プライマリ、セカンダリ、リソースアカウント) ごとに 1 つ以上の AWS のアカウントを作成します。AWS アカウントを作成および管理する方法については、以下を参照してください。
  - 初めてのAWS ユーザー– はじめに 初めてのユーザーですか？
  - AWSアカウント– https://docs.aws.amazon.com/accounts/latest/reference/managing-accounts.htmlの管理
- AWS Identity and Access Management (IAM) による権限 – AWS のアカウントを作成したら、作成した各アカウントに必要なロールと IAM による権限を設定する必要があります。たとえば、アプリケーションリソースにアクセスするための AWS のアカウントを作成した場合、新しいロールを設定し、アカウントからアプリケーションリソースにアクセスするために必要な AWS Resilience Hub の IAM による権限を設定する必要があります。IAM による権限の詳細については、the section called “AWS レジリエンスハブと IAM の連携の仕組み” ロールにポリシーを追加する方法の詳細については、the section called “JSON ファイルを使用した信頼ポリシーの定義” を参照してください。

  ユーザー、グループ、ロールへの IAM による権限の追加をすぐに開始するには、AWS のマネージドポリシー the section called “AWS 管理ポリシー” を使用できます。自身でポリシーを記述するよりも、AWS アカウント で利用可能な共通ユースケースを対象とする AWS のマネージドポリシーを使用する方が簡単です。AWS Resilience Hub は AWS のマネージドポリシーにアクセス権限を追加して、他の AWS のサービスへのサポートを拡大したり、新しい機能を追加したりします。そのため、

  - 既存のお客様で、評価で最新の機能強化をアプリケーションに使用したい場合は、アプリケーションの新しいバージョンを公開し、新しい評価を実行する必要があります。詳細については、次のトピックを参照してください。
    - the section called “新しいアプリケーションバージョンの公開”
    - the section called “障害耐性評価の実行”

- AWS のマネージドポリシーを使用してユーザー、グループおよびロールに適切な IAM による権限を割り当てていない場合は、これらの権限を手動で設定する必要があります。AWS 管理ポリシーの詳細については、「the section called "AWSResilienceHubAsssessmentExecutionPolicy"」を参照してください。

アプリケーションの追加 AWS Resilience Hub

AWS Resilience Hub ソフトウェア開発ライフサイクルに統合される耐障害性の評価と検証を行います。 AWS Resilience Hub 以下の機能により、 AWS アプリケーションを積極的に準備し、中断から保護するのに役立ちます。

- 障害耐性の弱点を明らかにする。
- 目標復旧時間 (RTO) と目標復旧時点 (RPO) を達成できるかどうかを見積もる。
- 本番環境にリリースされる前に問題を解決する。

このセクションでは、アプリケーションを追加する手順を説明します。 AWS CloudFormation AppRegistry 既存のアプリケーションやスタックからリソースを収集し、 AWS Resource Groups適切な耐障害性ポリシーを作成します。アプリケーションを記述したら、そのアプリケーションを公開して AWS Resilience Hub、アプリケーションの耐障害性に関する評価レポートを生成できます。その後、評価で得た推奨事項を参考にして障害耐性を向上させることができます。別の評価を実施して結果を比較し、推定ワークロード RTO と推定ワークロード RPO が RTO と RPO の目標を達成するまで繰り返すことができます。

トピック

ステップ 1: アプリケーションを開始して作業を開始する

まずは、 AWS アプリケーションの詳細を説明し、 AWS Resilience Hub レポートを作成して耐障害性を評価することから始めましょう。

はじめに、 AWS Resilience Hub ホームページの [はじめに] の下にある [アプリケーションを追加] を選択します。

関連する費用と請求について詳しくは AWS Resilience Hub、「AWS Resilience Hub 価格設定」を参照してください。

AWS Resilience Hubにアプリケーションの詳細を記載してください。

このセクションでは、 AWS で既存のアプリケーションの詳細を記述する方法を説明します AWS Resilience Hub。

アプリケーションの詳細を記載するには

1. アプリケーションの名前を入力します。
2. (オプション) アラームの説明を入力します。

次へ

ステップ 2: アプリケーションはどのように管理されているか

ステップ 2: アプリケーションはどのように管理されているか

AWS CloudFormation スタック、 AppRegistry アプリケーション AWS Resource Groups、および Terraform ステートファイルに加えて、Amazon Elastic Kubernetes サービス (Amazon EKS) クラスターにあるリソースを追加できます。つまり、AWS Resilience Hub では、Amazon EKS クラスターにあるリソースをオプションリソースとして追加できます。このセクションには、アプリケーションリソースの場所を特定するのに役立つ以下のオプションがあります。

- [リソースコレクション] – いずれかのリソースコレクションからリソースを検索する場合は、このオプションを選択します。リソースコレクションには、 AWS CloudFormation スタック、アプリケーション AWS Resource Groups、 AppRegistry Terraform 状態ファイルが含まれます。

  このオプションを選択した場合は、the section called “リソースコレクションを追加する” に記載されているいずれかの手順を完了する必要があります。

- [EKS のみ] – Amazon EKS クラスター内の名前空間からリソースを検出する場合は、このオプションを選択します。

  このオプションを選択した場合は、the section called “EKS クラスターを追加します” に記載されている手順を完了する必要があります。
- [リソースコレクションと EKS] – いずれかのリソースコレクションからAmazon EKS クラスターリソースを検索する場合は、このオプションを選択します。

  このオプションを選択した場合は、the section called “リソースコレクションを追加する” に記載されている手順のいずれかを実行してから、the section called “EKS クラスターを追加します” の手順を完了してください。

> **Note**
>
> アプリケーションごとにサポートされるリソースの数については、「Service Quotas」を参照してください。

次へ

ステップ 3: アプリケーションにリソースを追加する AWS Resilience Hub

ステップ 3: アプリケーションにリソースを追加する AWS Resilience Hub

このセクションでは、アプリケーション構造の基礎となる以下のオプションについて説明します。

- the section called “リソースコレクションを追加する”
- the section called “EKS クラスターを追加します”

リソースコレクションを追加する

このセクションでは、アプリケーション構造の基礎となる以下の方法について説明します。

- AWS CloudFormation スタックの使用
- 使用する AWS Resource Groups
- AppRegistry アプリケーションを使う
- Terraform 状態ファイルの使用

- AWS Resilience Hub 既存のアプリケーションを使用する

AWS CloudFormation スタックの使用

AWS CloudFormation 説明するアプリケーションで使用したいリソースを含むスタックを選択してください。スタックは、 AWS アカウント アプリケーションの説明に使用しているものでも、別のアカウントや異なるリージョンのものでもかまいません。

アプリケーション構造の基礎となるリソースを見つけるには

1. CloudFormation スタックを選択すると、スタックベースのリソースが表示されます。
2. 「スタックを選択」ドロップダウンリストから、自分とリージョンに関連するスタックを選択します。 AWS アカウント

   異なる AWS アカウント、別のリージョン、あるいはその両方にあるスタックを使用するには、[リージョン外にスタックを追加] ボックスにスタックの Amazon リソースネーム (ARN) を入力し、[スタック ARN を追加] を選択します。 AWS ARN の詳細については、AWS 全般のリファレンスの Amazon リソースネーム (ARN) を参照してください。

を使用する AWS Resource Groups

AWS Resource Groups 説明するアプリケーションで使用したいリソースを含むものを選択してください。

アプリケーション構造の基礎となるリソースを見つけるには

1. 「リソースグループ」を選択すると、 AWS Resource Groups そのリソースを含むグループが表示されます。
2. [リソースグループの選択] ドロップダウンリストからリソースを選択します。

   異なる AWS アカウント、別のリージョン、 AWS Resource Groups あるいはその両方にあるものを使用するには、スタックの Amazon リソースネーム (ARN) を [リソースグループ ARN] ボックスに入力し、[リソースグループ ARN を追加] を選択します。ARN の詳細については、AWS 全般のリファレンスの Amazon リソースネーム (ARN) を参照してください。

AppRegistry アプリケーションを使用する

AppRegistry 一度に追加できるアプリケーションは 1 つだけです。

AppRegistry 説明するアプリケーションで使用したいリソースを含むアプリケーションを選択してください。

アプリケーション構造の基礎となるリソースを見つけるには

1. AppRegistryで作成されたアプリケーションのリストから選択できます。AppRegistry
2. 「アプリケーションの選択」ドロップダウンリストから AppRegistry、で作成されたアプリケーションを選択します。一度につき 1 つのアプリケーションのみを選択できます。

Terraform 状態ファイルの使用

説明するアプリケーションで使いたい S3 バケットリソースを含む Terraform ステートファイルを選択します。Terraform 状態ファイルの場所に移動することも、別のリージョンにある Terraform 状態ファイルへのリンクを提供することもできます。

> **Note**
>
> AWS Resilience Hub Terraform `0.12` ステートファイルバージョン以降をサポートします。

アプリケーション構造の基礎となるリソースを見つけるには

1. [Terraform 状態ファイル] を選択して S3 バケットリソースを検索します。
2. [状態ファイルの選択] セクションから [S3 を参照] を選択し、Terraform 状態ファイルの場所に移動します。

   別のリージョンにある Terraform 状態ファイルを使用するには、[S3 のURL] フィールドに Terraform 状態ファイルの場所へのリンクを入力し、[S3 の URL を追加] を選択します。

   Terraform 状態ファイルの上限は 4 メガバイト (MB) です。
3. [バケット] セクションから S3 バケットを選択します。
4. [オブジェクト] セクションからキーを選択し、[選択] を選択します。

既存のアプリケーションを使用する AWS Resilience Hub

開始するには、既存のアプリケーションを使用してください。

アプリケーション構造の基礎となるリソースを見つけるには

1. 既存のアプリケーションからアプリケーションを構築するには、[既存のアプリケーション] を選択します。
2. [既存のアプリケーションを選択] ドロップダウンリストからアプリケーションを選択します。

EKS クラスターを追加します

このセクションでは、Amazon EKS クラスターを使用してアプリケーション構造の基礎を形成する方法について説明します。

> **Note**
>
> Amazon EKS クラスターに接続するには、Amazon EKS 権限と追加の IAM ロールが必要です。単一アカウントとクロスアカウントの Amazon EKS アクセス権限と追加の IAM ロールを追加してクラスターに接続する方法の詳細については、以下のトピックを参照してください。
>
> - AWS Resilience Hub アクセス権限リファレンス
> - the section called “Amazon EKS AWS Resilience Hub クラスターへのアクセスを有効にする”

記述するアプリケーションで使用するAmazon EKS クラスターと名前空間リソースを含む のスタックを選択します。Amazon EKS クラスターは、 AWS アカウント アプリケーションの記述に使用しているクラスターのものでも、別のアカウントや異なるリージョンのものでもかまいません。

> **Note**
>
> Amazon EKS AWS Resilience Hub クラスターを評価するには、「EKS クラスターと名前空間」セクションの各 Amazon EKS クラスターに関連する名前空間を手動で追加する必要があります。名前空間名は Amazon EKS クラスターの名前空間名と完全に一致する必要があります。

Amazon EKS クラスターを追加するには

1. 「EKS クラスターの選択」ドロップダウンリストから、 AWS アカウント ご自身とリージョンに関連する Amazon EKS クラスターを選択します。
2. 異なる AWS アカウント、異なるリージョン、あるいはその両方にある Amazon EKS クラスターを使用するには、スタックの Amazon リソースネーム (ARN) を [クロスアカウント] ボックスまたは [リージョン] ボックスに入力し、[EKS ARN を追加] を選択します。ARN の詳細については、AWS 全般のリファレンスの Amazon リソースネーム (ARN) を参照してください。

   クロスリージョンの Amazon Elastic Kubernetes Service クラスターへのアクセス許可の追加に関する詳細については、「the section called “Amazon EKS AWS Resilience Hub クラスターへのアクセスを有効にする”」を参照してください。

選択した Amazon EKS クラスターから名前空間を追加するには

1. [名前空間の追加] セクションの [EKS クラスターと名前空間] テーブルで、Amazon EKS クラスター名の左側にあるラジオボタンを選択し、[名前空間の更新] を選択します。

   Amazon EKS クラスターは次の方法で識別できます。

   - [EKS クラスター名] – 選択した Amazon EKS クラスターの名前を示します。
   - [名前空間の数] – Amazon EKS クラスターで選択された名前空間の数を示します。
   - ステータス — 選択した Amazon EKS AWS Resilience Hub クラスターの名前空間がアプリケーションに含まれているかどうかを示します。次のオプションを使用して、ステータスを識別できます。
     - [名前空間が必要] – Amazon EKS クラスターの名前空間を一切含めていないことを示します。
     - [名前空間が追加されました] – Amazon EKS クラスターから 1 つ以上の名前空間を含めたことを示します。
2. 名前空間を追加するには、[名前空間の更新] ダイアログボックスで [新しい名前空間の追加] を選択します。

   [名前空間の更新] ダイアログボックスには、Amazon EKS クラスターから選択したすべての名前空間が編集可能なオプションとして表示されます。
3. [名前空間の更新] ダイアログボックスには、以下の編集オプションがあります。

- 新しい名前空間を追加するには、[新しい名前空間の追加] を選択し、[名前空間] のボックスに名前空間名を入力します。

  名前空間名は Amazon EKS クラスターの名前空間名と完全に一致する必要があります。
- 名前空間を削除するには、名前空間の横にある [削除] を選択します。
- 選択した名前空間をすべての Amazon EKS クラスターに適用するには、[すべての EKS クラスターに名前空間を適用] を選択します。

  このオプションを選択すると、他の Amazon EKS クラスターで以前に選択した名前空間が、現在の名前空間の選択で上書きされます。

4. 更新した名前空間をアプリケーションに追加するには、[更新] を選択します。

次へ

ステップ 4: RTO と RPO を設定する

ステップ 4: RTO と RPO を設定する

独自の RTO/RPO 目標を使用して新しい障害耐性ポリシーを定義することも、RTO/RPO 目標があらかじめ定義されている既存の障害耐性ポリシーを選択することもできます。既存の障害耐性ポリシーのいずれかを使用する場合は、[既存のポリシーオプションを選択] を選択し、[オプション項目] ドロップダウンリストから既存のターゲットアプリケーションを選択します。

独自の RTO/RPO ターゲットを定義するには

1. [レジリエンシーポリシーを新規作成] オプションを選択します。
2. ポリシーの名前を入力します。
3. (オプション) 障害耐性ポリシーの説明を入力します。
4. [RTO/RPO ターゲット] セクションで RTO/RPO を定義します。

> **Note**
>
> - アプリケーションのデフォルトの RTO と RPO を設定しました。RTO と RPO は今すぐ変更することも、アプリケーションを評価した後に変更することもできます。
> - AWS Resilience Hub 耐障害性ポリシーの RTO フィールドと RPO フィールドに値ゼロを入力できます。ただし、アプリケーションを評価する際、最も低い評価結果はゼ

> 口に近いです。したがって、[RTO] と [RPO] のフィールドにゼロを入力すると、推定ワークロード RTO と推定ワークロード RPO の結果はほぼゼロになり、アプリケーションの [コンプライアンスステータス] は [ポリシー違反] に設定されます。

5. インフラストラクチャと AZ の RTO/RPO を定義するには、右矢印を選択して [インフラストラクチャ RTO と RPO] セクションを展開します。
6. [RTO/RPO ターゲット] では、ボックスに数値を入力し、その値が [RTO] と [RPO] の両方を表す時間単位を選択します。

   [インフラストラクチャ RTO と RPO] セクションの [インフラストラクチャ] と [アベイラビリティーゾーン] についても同じエントリを繰り返します。
7. (オプション) マルチリージョンアプリケーションを使用していて、リージョン RTO と RPO を定義したい場合は、[リージョン-オプション] をオンにしてください。

   [RTO] と [RPO] では、ボックスに数値を入力し、その値が [RTO] と [RPO] の両方で表す時間単位を選択します。

次へ

the section called “ステップ 5: 障害耐性ドリフト検出の設定”

ステップ 5: ドリフト検出

AWS Resilience Hub では、障害耐性ドリフト検出を設定してアプリケーションを毎日評価し、ドリフトが検出された場合や評価が失敗した場合に通知を受け取ることができます。

障害耐性ドリフト検出の設定

1. アプリケーションを毎日評価するには、[このアプリケーションを毎日自動的に評価する] をオンにしてください。

   このオプションをオンにすると、日次評価スケジュールは次の条件を満たした後にのみ開始されます。

   - アプリケーションがはじめに手動で正常に評価された。
   - アプリケーションに適切な IAM ロール が設定されている。
   - アプリケーションが現在の IAM ユーザー権限で設定されている場合は、`AwsResilienceHubPeriodicAssessmentRole` を作成する必要があります。

the section called “AWS レジリエンスハブと IAM の連携の仕組み” でロールが適切な手順を使用している。

2. AWS Resilience Hub コンプライアンスステータスの変化が検出されたとき、または毎日の回復力評価が失敗した場合に通知を受けるには、回復力ポリシー違反の通知を受け取ることをオンにしてください。

   このオプションをオンにした場合、ドリフト通知を受信するには、Amazon Simple Notification Service (Amazon SNS) トピックを指定する必要があります。Amazon SNS トピックを提供するには、[SNS トピックの提供] セクションで [SNS トピックオプションを選択] を選択し、[SNS トピックの選択] ドロップダウンリストから Amazon SNS トピックを選択します。

   > **Note**
   >
   > - AWS Resilience Hub が Amazon SNS トピックに通知を発行できるようにするには、Amazon SNS トピックに適切なアクセス権限を設定する必要があります。アクセス許可の設定については、「the section called “Amazon SNS AWS Resilience Hub トピックへのパブリッシュを有効にする”」を参照してください。
   > - 毎日の評価は、実行の割り当てに影響する可能性があります。クォータの詳細については、AWS 全般リファレンスの「AWS Resilience Hub エンドポイントとクォータ」を参照してください。

   AWS アカウント 異なるリージョンまたは異なるリージョン、あるいはその両方にある Amazon SNS トピックを使用するには、[SNS トピック ARN を入力] を選択し、[SNS トピックを提供する] ボックスに Amazon SNS トピックの Amazon リソースネーム (ARN) を入力します。ARN の詳細については、AWS 全般のリファレンスの Amazon リソースネーム (ARN) を参照してください。

次へ

ステップ 6: アクセス許可の設定

ステップ 6: アクセス許可の設定

AWS Resilience Hub プライマリアカウントとセカンダリアカウントに必要な権限を設定して、リソースの検出と評価を行うことができます。ただし、この手順を個別に実行して、アカウントごとに権限を設定する必要があります。

IAM ロールと IAM のアクセス許可を設定するには

1. 現在のアカウントのリソースへのアクセスに使用される既存の IAM ロールを選択するには、「Select an IAM role」ドロップダウンリストから IAM ロールを選択します。

   > **Note**
   >
   > クロスアカウント設定の場合、[IAM ロール ARN を入力] ボックスに IAM ロールの Amazon リソースネーム (ARN) を指定しない場合、すべてのアカウントの [IAM ロールの選択] ドロップダウンリストから選択した IAM AWS Resilience Hub ロールが使用されます。

   アカウントに既存の IAM ロールがアタッチされていない場合は、以下のオプションのいずれかを使用して IAM ロールを作成できます。

   - AWS IAM コンソール — このオプションを選択する場合は、「IAM コンソールで AWS Resilience ハブロールを作成するには」の手順を完了する必要があります。
   - AWS CLI — このオプションを選択する場合、AWS CLI のすべてのステップを完了する必要があります。
   - CloudFormation テンプレート — このオプションを選択した場合、アカウントの種類 (プライマリアカウントまたはセカンダリアカウント) に応じて、 AWS CloudFormation 適切なテンプレートを使用してロールを作成する必要があります。
2. 右矢印を選択し、[クロスアカウントから IAM ロールを追加 - オプション] セクションを展開します。
3. クロスアカウントから IAM ロールを選択するには、[IAM ロール ARN を入力] ボックスに IAM ロールの ARN を入力します。入力する IAM ロールの ARN が現在のアカウントに属していないことを確認してください。
4. 現在の IAM ユーザーを使用してアプリケーションリソースを検索する場合は、右矢印を選択して [現在の IAM ユーザー権限を使用する] セクションを展開し、[AWS Resilience Hub内で必要

な機能を有効にするには、手動で権限を設定する必要があることを理解しました] を選択します。

このオプションを選択すると、 AWS Resilience Hub 一部の機能 (回復力ドリフト検出など) が期待どおりに機能せず、ステップ 1 とステップ 3 で入力した内容が無視されることがあります。

次へ

ステップ 8: タグの追加

ステップ 7: アプリケーションの設定パラメータを設定する

このセクションでは、 AWS Elastic Disaster Recoveryを使用したクロスリージョンフェイルオーバーサポートの詳細を入力できます。 AWS Resilience Hub この情報を使用して、耐障害性に関する推奨事項を提供します。

アプリケーション構成パラメータの詳細については、「アプリケーションの設定パラメータ」を参照してください。

アプリケーション設定パラメータを追加するには (オプション)

1. [アプリケーション構成パラメータ] セクションを展開するには、右矢印を選択します。
2. [アカウント ID] ボックスにフェイルオーバーアカウント ID を入力します。デフォルトでは、このフィールドには使用するアカウント ID があらかじめ入力されていますが AWS Resilience Hub、この情報は変更できます。
3. [リージョン] ドロップダウンリストからフェイルオーバーリージョンを選択します。

> **Note**
>
> この機能を無効にする場合は、ドロップダウンリストから [–] を選択します。

次へ

ステップ 8: タグの追加

ステップ 8: タグの追加

リソースにタグやラベルを割り当てて、 AWS リソースを検索したりフィルタリングしたり、コストを追跡したりできます AWS 。

(オプション) アプリケーションにタグを追加するには、1 つ以上のタグをアプリケーションに関連付けたい場合は [新しいタグを追加] を選択します。タグの詳細については、AWS 参考文献のリソースのタグ付けを参照してください。

[アプリケーションを追加] を選択してアプリケーションを作成します。

次へ

ステップ 9: AWS Resilience Hub アプリケーションを確認して公開する

ステップ 9: AWS Resilience Hub アプリケーションを確認して公開する

公開した後でも、アプリケーションをレビューし、そのリソースを編集できます。終了したら、[公開] を選択してアプリケーションを公開します。

アプリケーションの確認とリソースの編集の詳細については、以下を参照してください。

- the section called “アプリケーション概要の表示”
- the section called “アプリケーションリソースの表示”

次へ

ステップ 10: AWS Resilience Hub アプリケーションの評価を実行する

ステップ 10: AWS Resilience Hub アプリケーションの評価を実行する

公開したアプリケーションは [概要] ページに表示されます。

AWS Resilience Hub アプリケーションを公開すると、耐障害性評価を実行できるアプリケーション概要ページにリダイレクトされます。評価では、アプリケーションにアタッチされているレジリエンシーポリシーと照らし合わせてアプリケーション構成を評価します。アプリケーションが障害耐性ポリシーの目標に対してどのように対応しているかを示す評価レポートが生成されます。

障害耐性評価を実行するには:

1. [アプリケーションの概要] ページで、[障害耐性の評価] を選択します。

2. [耐障害性評価を実行] ダイアログで、レポートの一意の名前を入力するか、[レポート名] ボックスに生成された名前を使用します。
3. [実行] を選択します。
4. 評価レポートが生成されたことが通知されたら、[評価] タブを選択し、評価を選択してレポートを表示します。
5. [レビュー] タブを選択すると、アプリケーションの評価レポートが表示されます。

AWS Resilience Hub を使用する

AWS Resilience Hub は、AWS 上のアプリケーションの回復力を向上させアプリケーションが停止した場合の復旧時間を短縮するのに役立ちます。

では を使用します。

- AWS Resilience Hub でAWSアプリケーションを説明します。
- AWS Resilience Hub でAWSリソースを管理します。
- 効果的な回復力ポリシーを作成します。
- アプリケーションの回復力を示す評価を管理します。
- アプリケーションのアラーム、標準作業手順書 (SOP)、テストを管理します。

AWS Resilience Hub アプリケーションの記述と管理

AWS Resilience Hubアプリケーションは、AWSアプリケーションの中断を防ぎ、回復するために構造化されたAWSリソースの集合体です。

AWS Resilience Hub アプリケーションを記述するには、アプリケーション名、1つまたは複数のAWS CloudFormationスタックからのリソース、および適切な回復力ポリシーを指定します。既存のAWS Resilience Hub アプリケーションをテンプレートとして使用して、アプリケーションを記述することもできます。

アプリケーションを記述したら、それを公開し、回復力評価を実行できるようにしなければなりません。次に、評価の推奨事項を使用して、評価の実行および結果の比較によって耐障害性を向上させることができます。次に、推定ワークロードの RTO と RPO の目標を達成するまで、評価の実行および結果の比較のプロセスを繰り返します。

アプリケーションの変更を追跡しやすくするため、AWS Resilience Hub は、アプリケーションがAWS Resilience Hub に作成された時点からの以前のバージョンを表示します。この可視性により、過去のアプリケーション構成を確認したり、現在のアプリケーション構成に関する決定を下したりするのに役立ちます。AWS Resilience Hub は、次のステータスを使用してアプリケーションのバージョンを識別します。

- ドラフト – アプリケーションバージョンが変更中で、まだ公開されていないことを示します。

- 現在のリリース – このアプリケーションバージョンが最近公開されたバージョンであることを示します。 AWS Resilience Hub は、このアプリケーションバージョンを使用して耐障害性評価を実行します。
- すべてのバージョンを表示 – 以前のバージョンをすべて読み取り専用形式で表示するには、プラス記号 (+) を選択します。

「アプリケーション」ページでは、次の方法でアプリケーションを識別できます。

- 名前 – AWS Resilience Hub での定義時に指定したアプリケーションの名前。
- 説明 – AWS Resilience Hub での定義時に指定したアプリケーションの説明。
- コンプライアンスステータス– AWS Resilience Hub は、アプリケーションのステータスを 評価済み、未評価、ポリシー違反、または 変更が検出されました に設定します。
  - 評価済み -AWS Resilience Hub 申請を評価しました。
  - 評価未了 -AWS Resilience Hub - 申請を評価していません。
  - ポリシー違反 - AWS Resilience Hub が、アプリケーションがレジリエンシーポリシーの目標復旧時間 (RTO) と目標復旧時点 (RPO) を満たしていないと判断されました。アプリケーションの耐障害性を再評価する前に、AWS Resilience Hub に記載されている推奨事項を確認して使用してください。レコメンダーの詳細については、「アプリケーションの追加 AWS Resilience Hub」を参照してください。
  - 変更が検出されました - AWS Resilience Hub は、アプリケーションに関連する耐障害性ポリシーに変更が加えられたことを検出しました。アプリケーションがレジリエンシーポリシーの目的を満たしているかどうかを判断するには、AWS Resilience Hub についてアプリケーションを再評価する必要があります。
- 定期評価 – リソースタイプによって、アプリケーションのコンポーネントリソースが特定されます。予定されている評価についての詳細は、アプリケーション耐障害性スコアを参照してください。
  - アクティブ - アプリケーションが AWS Resilience Hub によって 1 日ごとに自動的に評価されることを示します。
  - 無効 - これは、アプリケーションが AWS Resilience Hub によって毎日自動的に評価されるわけではないため、手動でアプリケーションを評価する必要があることを示します。
- 耐障害性ドリフトステータス – アプリケーションが前回の成功した評価から逸脱したかどうかを示し、次のステータスのいずれかを設定します。

  - ドリフト - 前回の評価でレジリエンシーポリシーに準拠していたアプリケーションが、現在はレジリエンシーポリシーに違反しており、アプリケーションが危険にさらされていることを示します。
  - ドリフトなし - ポリシーで定義されている RTO と RPO の目標をアプリケーションがまだ満たしていると推定されていることを示します。
- 推定ワークロード RTO – アプリケーションの推定最大ワークロード RTO を示します。この値は、前回成功した評価からのすべての中断タイプの最大推定ワークロード RTO です。
- 推定ワークロード RPO – アプリケーションの推定最大ワークロード RPO を示します。この値は、前回成功した評価からのすべての中断タイプの最大推定ワークロード RTO です。
- 最終評価時間 – アプリケーションが最後に正常に評価された日付と時刻を示します。
- 作成日時 –ジョブを作成した日付と時刻。
- ARN - アプリケーションのAmazon リソースネーム (ARN)。ARN の詳細については、AWS 全般のリファレンスの Amazon リソースネーム (ARN) を参照してください。

> **Note**
>
> AWS Resilience Hub は、クロスリージョン Amazon ECS リソースの耐障害性を完全に評価できるのは、イメージリポジトリに Amazon ECR を使用している場合のみです。

さらに、アプリケーションページの以下のオプションのいずれかを使用してアプリケーションリストをフィルタリングすることもできます。

- アプリケーションの検索 – アプリケーション名を入力すると、そのアプリケーションの名前で結果がフィルタリングされます。
- 最終評価日時を日付と時間範囲で絞り込む – このフィルターを適用するには、カレンダーアイコンを選択し、以下のオプションのいずれかを選択して、時間範囲に一致する結果で絞り込みます。
  - 相対範囲 – 使用可能なオプションを 1 つ選択して 適用 を選択します。

    カスタマイズ範囲 オプションを選択した場合は、「期間を入力」ボックスに期間を入力し、「時間単位」ドロップダウンリストから適切な時間単位を選択して、適用 を選択します。
  - 絶対範囲– 日付と時刻の範囲を指定するには、開始時刻と終了時刻を指定し、適用 を選択します。

以下のトピックでは、AWS Resilience Hub のアプリケーションを説明するさまざまな方法とその管理方法を示します。

トピック

AWS Resilience Hubアプリケーション概要の表示

AWS Resilience Hubコンソールのアプリケーション概要ページには、アプリケーション情報と回復力の状態の概要が表示されます。

アプリケーション概要を表示するには

1. ナビゲーションペインで、「アプリケーション」を選択します。
2. アプリケーション」 ページで、テーブルからアプリケーションを選択します。

アプリケーション概要ページには、次のセクションが含まれています。

トピック

詳細

アプリケーション概要の詳細セクションには、アプリケーションの選択内容の概要が表示されます。

- アプリケーションステータス — アプリケーションがアクティブかどうかを示します。
- 説明 アプリケーションバージョンの説明。
- コンプライアンスステータス — アプリケーションのコンプライアンスステータスを示します。
- スケジュールされた評価時間 — アプリケーションが最後に評価された日付と時刻を示します。
- 回復力ポリシー — アプリケーションに添付されている回復力ポリシーの名前が表示されます。リソースポリシーの詳細については、「回復力ポリシーの管理」を参照してください。
- スケジュールされた評価 — 日次評価がアクティブか非アクティブかを示します。
- 回復力ドリフトステータス — アプリケーションが前回の成功した評価からずれているかどうかを示します。
- 最終ドリフト時間 — アプリケーションにドリフトがないかチェックされた日付と時刻を示します。

スケジュールされた評価を更新するには

1. アプリケーションのスケジュールされた評価を更新するには、アクションから回復力ドリフト検出の更新を選択します。
2. 回復力ドリフト検出を更新するには、ステップ 5: ドリフト検出 のステップを完了してからこのプロセスに戻ります。
3. 「更新」 を選択します。

> **Note**
>
> 既存のアプリケーションで回復力ドリフト検出を有効にするには、回復力ドリフト検出特徴量を初めて有効にした後に手動で評価を実行する必要があります。非アクティブな評価の詳細については、「障害耐性評価の実行」を参照してください。

アプリケーション耐障害性スコア

アプリケーションの回復力セクションに表示されるメトリックは、アプリケーションの最新の回復力評価からのものです。

耐障害性スコア

回復力スコアは、潜在的な中断に対処する準備状況を定量化するのに役立ちます。このスコアは、アプリケーションの回復力ポリシー、アラーム、標準作業手順書 (SOP) 、および AWS Resilience Hub テストを満たすための推奨事項にアプリケーションがどの程度準拠しているかを反映しています。

アプリケーションが達成できる最大回復力スコアは 100% です。このスコアは、事前定義された期間内に実行されるすべての推奨テストを表します。テストによって正しいアラームが開始され、アラームによって正しい SOP が開始されたことが示されます。

たとえば、 AWS Resilience Hub が 1 つのアラームと 1 つの SOP によるテストを推奨するとします。テストが実行されると、アラームは関連する SOP を開始し、その後正常に実行されます。スコアの詳細については、「障害耐性スコアの理解」を参照してください。

時間の経過に伴う回復力スコア

時間の経過に伴う回復力スコアを使用して、過去 30 日間のアプリケーションの回復力グラフを表示できます。ドロップダウンメニューにはアプリケーションを 10 個まで一覧表示できますが、AWS Resilience Hubは一度に最大 4 つのアプリケーションのグラフしか表示できません。詳細については、「関連付けのスケジューリングについて」を参照してください。

> **Note**
>
> AWS Resilience Hub はスケジュールされた評価を同時に実行できません。そのため、アプリケーションの日次評価を確認するために、時間の経過に伴う回復力スコアのグラフに戻る必要がある場合があります。

AWS Resilience Hub はまた、Amazon CloudWatch を使用してこれらのグラフを生成します。CloudWatch でメトリクスを表示 を選択すると、アプリケーションの回復力に関するより詳細な情報を CloudWatch ダッシュボードに作成して表示できます。詳細については、「Amazon CloudWatch ユーザーガイド」の「Amazon CloudWatch ダッシュボードの使用」を参照してください。

アラームの実装

アプリケーション概要の実装済みアラームセクションには、アプリケーションを監視するために Amazon CloudWatch で設定したアラームが一覧表示されます。アラームの詳細については、「アラーム」を参照してください。

実施した実験

アプリケーション概要の故障注入実験セクションには、故障注入実験のリストが表示されます。障害挿入クエリの詳細については、「Amazon Fault Injection Service の実験」を参照してください。

AWS Resilience Hub のアプリケーションリソースへのタグ付け

正確で役立つ耐障害性評価を受けるには、アプリケーションの説明が更新され、実際の AWS のアプリケーションやリソースと一致していることを確認してください。評価レポート、検証、および推奨事項は、記載されているリソースに基づいています。リソースを AWS のアプリケーションに追加したり、アプリケーションから削除したりする場合は、それらの変更を AWS Resilience Hub に反映する必要があります。

AWS Resilience Hub はアプリケーションのソースを透明化できます。アプリケーション内のリソースとアプリケーションソースを識別して編集できます。

> **Note**
>
> リソースを編集すると、アプリケーションの AWS Resilience Hub の参照のみが変更されます。実際のリソースは変更されません。

不足しているリソースを追加したり、既存のリソースを変更したり、不要なリソースを削除したりできます。リソースは論理的なアプリケーションコンポーネント (AppComponents) にグループ化されます。AppComponents はアプリケーションの構造をより正確に反映するように編集できます。

アプリケーションのドラフトバージョンを編集し、その変更を新しい (リリース) バージョンに公開することで、アプリケーションリソースを追加または更新します。 AWS Resilience Hub は、アプリケーションのリリースバージョン (更新されたリソースを含む) を使用して耐障害性評価を実行します。

アプリケーションの耐障害性を評価するには

1. ナビゲーションペインで、アプリケーション を選択します。
2. 「アプリケーション」ページで、編集するアプリケーション名を選択します。
3. 「アクション」メニューから 耐障害性の評価 を選択します。
4. 「耐障害性評価の実行」ダイアログで、レポートの一意の名前を入力するか、「レポート名」ボックスに生成された名前を使用します。

5. 実行 を選択します。
6. 評価レポートが生成されたことが通知されたら、評価 タブを選択し、評価を選択してレポートを表示します。
7. アプリケーションの評価レポートの レビュー タブを選択します。

アプリケーションの耐障害性ドリフト検出を更新するには

1. ナビゲーションペインで、アプリケーション を選択します。
2. 「アプリケーション」ページで、耐障害性ドリフト検出を有効または無効にするアプリケーションを選択します。
3. 「アクション」 から 耐障害性ドリフト検出の更新 を選択します。
4. 耐障害性ドリフト検出を更新するには、ステップ 5: ドリフト検出 の手順を完了してからこの手順に戻ります。
5. 更新 を選択します。

アプリケーションのセキュリティ権限を更新するには

1. ナビゲーションペインで、アプリケーション を選択します。
2. 「アプリケーション」ページで、セキュリティ権限を更新するアプリケーションを選択します。
3. 「アクション」 から 権限の更新 を選択します。
4. セキュリティ権限を更新するには、ステップ 6: アクセス許可の設定 の手順を完了してからこの手順に戻ります。
5. 保存とテスト を選択します。

レジリエンシーポリシーをアプリケーションにアタッチするには

1. ナビゲーションペインで、アプリケーション を選択します。
2. 「アプリケーション」ページで、編集するアプリケーション名を選択します。
3. 「アクション」メニューから レジリエンシーポリシーをアタッチ を選択します。
4. 「ポリシーをアタッチ」ダイアログで、「レジリエンシーポリシーの選択」ドロップダウンリストからレジリエンシーポリシーを選択します。
5. 添付 を選択します。

アプリケーションの入力ソース、リソース、AppComponents を編集するには

1. ナビゲーションペインで、アプリケーション を選択します。
2. 「アプリケーション」ページで、編集するアプリケーション名を選択します。
3. アプリケーション構造 タブを選択します。
4. 「バージョン」の前にあるプラス記号「+」を選択し、ステータスが「ドラフト」のアプリケーションバージョンを選択します。

5. アプリケーションの入力ソース、リソース、AppComponents を編集するには、以下の手順のステップを実行します。

アプリケーションの入力ソースを編集するには

1. アプリケーションの入力ソースを編集するには、入力ソース タブを選択します。

   「入力ソース」セクションには、アプリケーションリソースのすべての入力ソースが一覧表示されます。次の方法で入力ソースを特定できます。

   - ソース名 – 入力ソースの名前。ソース名を選択すると、それぞれのアプリケーションで詳細が表示されます。手動で追加した入力ソースの場合、リンクは使用できません。たとえば、AWS CloudFormation のスタックからインポートされるソース名を選択すると、AWS CloudFormation のコンソールのスタック詳細ページにリダイレクトされます。
   - ソース ARN - 入力ソースの Amazon リソースネーム (ARN)。ARN を選択すると、その詳細がそれぞれのアプリケーションに表示されます。手動で追加した入力ソースの場合、リンクは使用できません。たとえば、AWS CloudFormation のスタックからインポートされる ARN を選択すると、AWS CloudFormation のコンソールのスタック詳細ページにリダイレクトされます。
   - ソースタイプ – 入力ソースのタイプ。入力ソースには、Amazon EKS クラスター AWS CloudFormation スタック、AppRegistry アプリケーション、AWS Resource Groups、Terraform ステートファイル、手動で追加されたリソースが含まれます。
   - 関連リソース – 入力ソースに関連付けられているリソースの数。番号を選択すると、入力ソースのすべての関連リソースが リソース タブに表示されます。

2. 入力ソースをアプリケーションに追加するには、「入力ソース」セクションから 入力ソースを追加 を選択します。ソーシャル IdP の追加の詳細については、「the section called “ステップ 3: AWS Resilience Hub アプリケーションにリソースを追加する”」を参照してください。

3. 入力ソースを編集するには、入力ソースを選択し、「アクション」から以下のいずれかのオプションを選択します。

   - 入力ソースの再インポート (最大 5 つ) – 選択した入力ソースを最大 5 つまで再インポートします。
   - 入力ソースを削除 – 選択した入力ソースを削除します。

     アプリケーションを公開するには、少なくとも 1 つの入力ソースが含まれている必要があります。入力ソースをすべて削除すると、「新規バージョンを公開」は無効になります。

アプリケーションのリソースを編集するには

1. アプリケーションの入力ソースを編集するには、リソース タブを選択します。

   > **Note**
   >
   > 未評価のリソースのリストを表示するには、未評価のリソースを表示 を選択します。

   「リソース」セクションには、アプリケーション記述のテンプレートとして使用することを選択したアプリケーションのリソースが一覧表示されます。検索しやすくするため、AWS Resilience Hub は複数の検索条件に基づいてリソースをグループ化しています。これらの検索条件には、AppComponent タイプ、サポートされていないリソース、除外されたリソースが含まれます。「リソース」テーブルの検索条件に基づいてリソースをフィルタリングするには、各検索条件の下にある番号を選択します。

   次の方法でリソースを特定できます。

   - 論理 ID – 論理 ID は、AWS CloudFormation のスタック、Terraform 状態ファイル、手動で追加したアプリケーション、AppRegistry アプリケーション、または AWS Resource Groups 内のリソースを識別するために使用される名前です。

     > **Note**
     >
     > - Terraform では、異なるリソースタイプに同じ名前を使用できます。そのため、同じ名前を共有するリソースの論理 ID の末尾には「- resource type」が表示されます。

- すべてのアプリケーションリソースのインスタンスを表示するには、論理 ID の前にあるプラス (+) 記号を選択します。すべてのアプリケーションリソースのインスタンスを表示するには、論理 ID の前にあるプラス (+) 記号を選択します。

  サポートされるリソースタイプの詳細については、the section called “ AWS Resilience Hub サポート対象リソース”を参照してください。

- リソースタイプ – リソースタイプはアプリケーションのコンポーネントリソースを識別します。たとえば、`AWS::EC2::Instance` は Amazon EC2 インスタンスを宣言します。AppComponent リソースのグループ化の詳細については、「リソースをグループ化する AppComponent」を参照してください。
- ソース名 – 入力ソースの名前。ソース名を選択すると、それぞれのアプリケーションで詳細が表示されます。手動で追加した入力ソースの場合、リンクは使用できません。たとえば、AWS CloudFormation スタックからインポートされるソース名を選択すると、AWS CloudFormation のスタック詳細ページにリダイレクトされます。
- ソースタイプ – 入力ソースのタイプ。入力ソースには、AWS CloudFormation スタック、AppRegistry アプリケーション、AWS Resource Groups、Terraform ステートファイル、手動で追加されたリソースが含まれます。

  > **Note**
  >
  > Amazon EKS クラスターを編集するには、「AWS Resilience Hub のアプリケーションプロシージャの入力ソースを編集するには」のステップを実行します。

- ソーススタック – リソースを含む AWS CloudFormation のスタック。この列は、選択したアプリケーション構造のタイプによって異なります。
- 物理 ID – Amazon EC2 インスタンス ID や S3 バケット名など、そのリソースに実際に割り当てられた識別子。
- 含まれている – AWS Resilience Hub で、これらのリソースがアプリケーションに含まれるかどうかを示します。
- ステータス – AWS Resilience Hub がリソースの耐障害性を評価するかどうかを示します。
- AppComponents –アプリケーション構造が見つかったときにこのリソースに割り当てられた AWS Resilience Hub のコンポーネント。
- 名前 –リソースの名前 (該当する場合)。
- アカウント - 物理リソースを所有するアカウント。

2. リストにないリソースを検索するには、検索ボックスにリソースの論理 ID を入力します。
3. アプリケーションからリソースを削除するには、リソースを選択し、「「アクション」から リソースを除外 を選択します。
4. アプリケーションのリソースを解決するには、リソースの更新 を選択します。
5. 既存のアプリケーションリソースを変更するには、以下のステップを実行します。

   a. リソースを選択し、「アクション」から スタックを更新 を選択します。

   b. 「スタックの更新」ページでリソースを更新するには、ステップ 3: アプリケーションにリソースを追加する AWS Resilience Hub で該当する手順を完了してから、この手順に戻ります。

   c. 保存 を選択します。

6. アプリケーションにリソースを追加するには、「アクション」から リソースの追加 を選択し、以下の手順を実行します。

   a. リリースタイプ ドロップダウンリストから少なくとも 1 つのリソースタイプを選択します。

   b. 「AppComponent」ドロップダウンリストからAppComponentを選択します。

   c. 「リソース名」ボックスにリソースの論理 ID を入力します。

   d. 「リソース識別子」ボックスに、物理リソース ID、リソース名、またはリソースARN を入力します。

   e. 追加 を選択します。

7. リソース名を編集するには、リソースを選択し、「アクション」から「リソース名を編集」を選択し、次の手順を実行します。

   a. 「リソース名」ボックスにリソースの論理 ID を入力します。

   b. 保存 を選択します。

8. リソース名を編集するには、リソースを選択し、「アクション」から「リソース名を編集」を選択し、次の手順を実行します。

   a. 「リソース識別子」ボックスに、物理リソース ID、リソース名、またはリソースARN を入力します。

   b. 保存 を選択します。

9. AppComponent を変更するには、リソースを選択し、「アクション」から AppComponent を変更 を選択して、次の手順を実行します。

a. 「AppComponent」ドロップダウンリストからAppComponentを選択します。

b. 追加 追加 を選択します。

10. リソースを削除するには、リソースを選択し、「アクション」から リソースを削除 を選択します。

11. リソースを削除するには、リソースを選択し、「アクション」から リソースを削除 を選択します。

アプリケーションの AppComponents を編集するには

1. アプリケーションの AppComponents を編集するには、AppComponents タブを選択します。

> **Note**
>
> AppComponent リソースのグループ化の詳細については、「リソースをグループ化する AppComponent」を参照してください。

「AppComponents」セクションには、リソースをグループ化するすべての論理コンポーネントが一覧表示されます。次の方法で AppComponents を特定できます。

- AppComponent 名 – アプリケーション構造が検出されたときにこのリソースに割り当てられた AWS Resilience Hub のコンポーネントの名前。
- AppComponent タイプ – AWS Resilience Hub のコンポーネントのタイプ。
- ソース名 – 入力ソースの名前。ソース名を選択すると、それぞれのアプリケーションで詳細が表示されます。たとえば、AWS CloudFormation スタックからインポートされるソース名を選択すると、AWS CloudFormation のスタック詳細ページにリダイレクトされます。
- リソース数 – 入力ソースに関連付けられているリソースの数。番号を選択すると、入力ソースのすべての関連リソースが リソース タブに表示されます。

2. AppComponent を作成するには、「アクション」メニューから AppComponent を新規作成 を選択し、以下の手順を実行します。

a. 「AppComponent 名」ボックスに AppComponent の名前を入力します。参考までに、このフィールドにはサンプル名があらかじめ入力されています。

b. 「AppComponent タイプ」ドロップダウンリストから AppComponent のタイプを選択します。

c. 保存 を選択します。

3. AppComponent を編集するには、AppComponent を選択し、「アクション」から AppComponent の編集 を選択します。
4. AppComponent を編集するには、AppComponent を選択し、「アクション」から AppComponent の編集 を選択します。

リソースリストを変更すると、アプリケーションのドラフトバージョンに変更が加えられたことを示すアラートが表示されます。正確な耐障害性評価を実行するには、アプリケーションの新しいバージョンを公開する必要があります。新しいバージョンを公開する方法に関する詳細については、「新しいアプリケーションバージョンの発行」を参照してください。

リソースをグループ化する AppComponent

AppComponent は、1 つのユニットとして動作し、 AWS 障害が発生する関連リソースのグループです。たとえば、プライマリデータベースとレプリカデータベースがある場合、両方のデータベースは同じアプリケーションコンポーネント (AppComponent) に属します。 AWS Resilience Hub には、 AWS どのリソースをどのタイプに属させることができるかを規定するルールがあります。 AppComponent例えば、ある `DBInstance` が、`AWS::ResilienceHub::DatabaseAppComponent` に属していても `AWS::ResilienceHub::ComputeAppComponent` に属さない場合があります。

AWS Resilience Hub AWS CloudFormation アプリケーションをスタックにインポートすると、Terraform 状態ファイル AWS Resource Groups、Amazon Elastic Kubernetes Service クラスター、 AppRegistry またはアプリケーションは、 AWS Resilience Hub 関連するリソースを同じリソースにグループ化するために最善を尽くしますが AppComponent、常に 100% 正確であるとは限りません。アプリケーションのアーキテクチャを最もよく知っているので、すでにグループ化されているリソースを別のものに再グループ化できます。 AWS Resilience Hub AppComponentたとえば、AWS CloudFormation スタックに 3 つの EC2 インスタンスがある場合、EC2 AppComponent インスタンスごとに 1 AWS Resilience Hub つ作成しますが、3 つの EC2 インスタンスすべてが同じアプリケーションソフトウェアを実行している可能性があります。この場合の正しい選択は、3 つの EC2 インスタンスを 1 つの `ComputeAppComponent` に再グループ化することです。リソースを再グループ化するときには、リソースを 1 つにだけ再グループ化する必要があります。 AppComponent リソースリストを拡張して、グループ化されていないリソースをにまとめることもできます。 AppComponent

AWS Resilience Hub AppComponents は以下のリソースをサポートします。

- AWS::ResilienceHub::ComputeAppComponent
  - AWS::ApiGateway::RestApi
  - AWS::ApiGatewayV2::Api
  - AWS::AutoScaling::AutoScalingGroup
  - AWS::EC2::Instance
  - AWS::ECS::Service
  - AWS::EKS::Deployment
  - AWS::EKS::ReplicaSet
  - AWS::EKS::Pod
  - AWS::Lambda::Function
  - AWS::StepFunctions::StateMachine
- AWS::ResilienceHub::DatabaseAppComponent
  - AWS::DocDB::DBCluster
  - AWS::DynamoDB::Table
  - AWS::RDS::DBCluster
  - AWS::RDS::DBInstance
- AWS::ResilienceHub::NetworkingAppComponent
  - AWS::EC2::NatGateway
  - AWS::ElasticLoadBalancing::LoadBalancer
  - AWS::ElasticLoadBalancingV2::LoadBalancer
  - AWS::Route53::RecordSet
- AWS:ResilienceHub::NotificationAppComponent
  - AWS::SNS::Topic
- AWS::ResilienceHub::QueueAppComponent
  - AWS::SQS::Queue
- AWS::ResilienceHub::StorageAppComponent
  - AWS::Backup::BackupPlan
  - AWS::EC2::Volume
  - AWS::EFS::FileSystem
  - AWS::FSx::FileSystem

- > **Note**
  >
  > 現在、Windows ファイルサーバー用の Amazon FSx AWS Resilience Hub のみをサポートしています。

- `AWS::S3::Bucket`

正しいグループ分けの例を以下に示します。

- プライマリデータベースとレプリカを 1 つのデータベースにグループ化します。 AppComponent
- Amazon S3 バケットとそのレプリケーションを 1 つのバケットにグループ化します AppComponent。
- 同じアプリケーションを実行する Amazon EC2 インスタンスを 1 つのインスタンスにグループ化します AppComponent。
- Amazon SQS キューとそのデッドレターキューを 1 つにまとめます。 AppComponent
- Amazon ECS サービスをあるリージョンにグループ化し、別のリージョンの Amazon ECS サービスを単一のリージョンにフェイルオーバーします。 AppComponent

> **Note**
>
> AWS Resilience Hub 推定ワークロード RTO と推定ワークロード RPO を計算して推奨事項を生成できるように、正しいグループ化が必要です。

にリソースを割り当てるには AppComponent

1. ナビゲーションペインで、[アプリケーション] を選択します。
2. [アプリケーション] ページで、再グループ化するリソースを含むアプリケーション名を選択します。
3. [アプリケーション構造] タブを選択します。
4. [バージョン] で、ステータスが [ドラフト] のアプリケーションバージョンを選択します。
5. [リソース] タブを選択します。
6. 再グループ化するリソースを選択します。
7. 「アクション」 から「変更」を選択します AppComponent。

「変更 AppComponent」ダイアログ・ボックスが表示されます。

8. AppComponent AppComponentセクションから現在の名前を削除するには、 AppComponent 現在の名前が表示されているラベルの右上隅にある X を選択します。
9. リソースを別のリソースにグループ化するには AppComponent、「選択」 AppComponent AppComponentドロップダウンリストから別のリソースを選択します。
10. [追加] を選択します。
11. AppComponents AppComponentsタブから空欄をすべて削除します。
12. [新しいバージョンを発行] を選択します。
13. [アプリケーション構造] タブを選択します。
14. アプリケーションの公開バージョンを表示するには、以下の手順を実行します。

    a. [バージョン] タブで、[現在のリリース] ステータスのアプリケーションバージョンを選択します。

    b. [リソース] タブを選択します。

リソースをグループ化するには

1. ナビゲーションペインで、[アプリケーション] を選択します。
2. [アプリケーション] ページで、グループ化するリソースを含むアプリケーション名を選択します。
3. [アプリケーション構造] タブを選択します。
4. [バージョン] タブで、ステータスが [ドラフト] のアプリケーションバージョンを選択します。
5. [リソース] タブを選択します。
6. グループ化するリソースグループを選択します。

> **Note**
>
> 手動で追加したリソースは選択できません。

7. [アクション] を選択し、[リソースの追加] を選択します。

「結合 AppComponent」ウィンドウが表示されます。

8. 「選択」 AppComponent AppComponent ドロップダウンリストから、リソースをグループ化したいリソースを選択します。

9. [保存] を選択します。
10. [新しいバージョンを発行] を選択します。
11. [アプリケーション構造] タブを選択します。
12. アプリケーションの公開バージョンを表示するには、以下の手順を実行します。

    a. [バージョン] タブで、[現在のリリース] ステータスのアプリケーションバージョンを選択します。

    b. [リソース] タブを選択します。

新しいアプリケーションバージョンの発行

AWS Resilience Hub のアプリケーションリソースへのタグ付け で説明されているように AWS Resilience Hub のアプリケーションリソースに変更を加えたら、アプリケーションの新しいバージョンを公開して、正確な耐障害性評価を実行する必要があります。また、新しい推奨アラーム、SOP、テストをアプリケーションに追加した場合は、アプリケーションの新しいバージョンを公開する必要がある場合があります。

アプリケーションの新しいバージョンを発行するには

1. ナビゲーションペインで、アプリケーション を選択します。
2. アプリケーション ページで、テーブルからアプリケーションを選択します。
3. アプリケーション構造 タブを選択します。
4. 新しいバージョンを発行 を選択します。
5. 「バージョンを公開」ダイアログの「名前」ボックスに、アプリケーションバージョンの名前を入力するか、AWS Resilience Hub で提案されるデフォルトの名前を使用できます。
6. 発行 を選択します。

   アプリケーションの新しいバージョンを公開すると、そのバージョンが耐障害性評価を実行したときに評価されるバージョンになります。また、変更を加えるまで、ドラフトバージョンはリリースされたバージョンと同じになります。

アプリケーションの新しいバージョンを公開したら、新しい耐障害性評価レポートを実行して、アプリケーションがまだレジリエンシーポリシーを満たしていることを確認することをお勧めします。評価の実行については、「AWS Resilience Hub レジリエンス評価の実行と管理」を参照してください。

すべての AWS Resilience Hub のアプリケーションバージョンを表示する

アプリケーションの変更を追跡しやすくするため、AWS Resilience Hub は、アプリケーションが AWS Resilience Hub に作成された時点以前のバージョンを表示します。

アプリケーションのすべてのバージョンを表示するには

1. ナビゲーションペインで、アプリケーション を選択します。
2. アプリケーションページで、アプリケーションの名前を選択します。
3. アプリケーション構造 タブを選択します。
4. アプリケーションの以前のバージョンをすべて表示するには、すべてのバージョンを表示 の前にあるプラス記号 (+) を選択します。 AWS Resilience Hubアプリケーションのドラフトバージョンと最近リリースされたバージョンをそれぞれ「ドラフト」と「現在のリリース」ステータスを使用して示します。アプリケーションの任意のバージョンを選択して、そのリソース、AppComponent、入力ソース、およびその他の関連情報を表示できます。

   さらに、アプリケーションページの以下のオプションのいずれかを使用してアプリケーションリストをフィルタリングすることもできます。

   - バージョン名で絞り込む – 名前を入力すると、アプリケーションのバージョン名で結果が絞り込まれます。
   - 日付と時間の範囲によるフィルタリング – このフィルターを適用するには、カレンダーアイコンを選択し、以下のオプションのいずれかを選択して、時間範囲に一致する結果で絞り込みます。
     - 相対範囲 – 使用可能なオプションを 1 つ選択して 適用 を選択します。

       カスタマイズ範囲 オプションを選択した場合は、「期間を入力」ボックスに期間を入力し、「時間単位」ドロップダウンリストから適切な時間単位を選択して、適用 を選択します。
     - 絶対範囲– 日付と時刻の範囲を指定するには、開始時刻と終了時刻を指定し、適用 を選択します。

アプリケーションリソースの表示

アプリケーションのリソースを表示します。

1. ナビゲーションペインで、アプリケーション を選択します。

2. 「アプリケーション」ページで、セキュリティ権限を更新するアプリケーションを選択します。
3. 「アクション」 から「リソースを表示」を選択します。

リソース タブでは、以下の方法で「リソース」テーブル内のリソースを識別できます。

- 論理 ID – 論理 ID は、AWS CloudFormation のスタック、Terraform 状態ファイル、手動で追加したアプリケーション、AppRegistry アプリケーション、または AWS Resource Groups 内のリソースを識別するために使用される名前です。

> **Note**
>
> - Terraform では、異なるリソースタイプに同じ名前を使用できます。そのため、同じ名前を共有するリソースの論理 ID の末尾には「- resource type」が表示されます。
> - すべてのアプリケーションリソースのインスタンスを表示するには、論理 ID の前にあるプラス (+) 記号を選択します。すべてのアプリケーションリソースのインスタンスを表示するには、論理 ID の前にあるプラス (+) 記号を選択します。
>
> サポートされるリソースタイプの詳細については、the section called “ AWS Resilience Hub サポート対象リソース”を参照してください。

- ステータス – AWS Resilience Hub がリソースの耐障害性を評価するかどうかを示します。
- リソースタイプ – リソースタイプはアプリケーションのコンポーネントリソースを識別します。たとえば、`AWS::EC2::Instance` は Amazon EC2 インスタンスを宣言します。AppComponent リソースのグループ化の詳細については、「リソースをグループ化する AppComponent」を参照してください。
- ソース名 – 入力ソースの名前。ソース名を選択すると、それぞれのアプリケーションで詳細が表示されます。手動で追加した入力ソースの場合、リンクは使用できません。たとえば、AWS CloudFormation スタックからインポートされるソース名を選択すると、AWS CloudFormation のスタック詳細ページにリダイレクトされます。
- ソースタイプ – 入力ソースのタイプ。
- AppComponent タイプ – 入力ソースのタイプ。入力ソースには、AWS CloudFormation スタック、AppRegistry アプリケーション、AWS Resource Groups、Terraform ステートファイル、手動で追加されたリソースが含まれます。

> **Note**
>
> Amazon EKS クラスターを編集するには、「AWS Resilience Hub のアプリケーションプロシージャの入力ソースを編集するには」のステップを実行します。

- 物理 ID – Amazon EC2 インスタンス ID や S3 バケット名など、そのリソースに実際に割り当てられた識別子。
- 含まれている – AWS Resilience Hub で、これらのリソースがアプリケーションに含まれるかどうかを示します。
- AppComponents –アプリケーション構造が見つかったときにこのリソースに割り当てられた AWS Resilience Hub のコンポーネント。
- 名前 –アプリケーションリソースの名前。
- 物理リソースを所有する アカウント。

4. 更新と終了 を選択します。

アプリケーションの削除

アプリケーションの上限の 10 に達したら、1 つ以上のアプリケーションを削除してからでないと追加できません。

アプリケーションを削除するには

1. ナビゲーションペインで、アプリケーション を選択します。
2. アプリケーションバージョン ページで、削除するすべてのアプリケーションバージョンを選択します。
3. アクション を選択してから、アプリケーションの削除 を選択します。
4. 削除を確定するには、「削除」ボックスに「削除」と入力し、削除 を選択します。

アプリケーションの設定パラメータ

AWS Resilience Hub は、アプリケーションに関連するリソースに関する追加情報を収集するための入力メカニズムが提供されるようになりました。この情報により、AWS Resilience Hub はお客様のリソースをより深く理解し、より優れた耐障害性に関する推奨事項を提示できるようになります。

「アプリケーション構成パラメーター」セクションには、AWS Elastic Disaster Recovery のクロスリージョンフェイルオーバーサポートのすべての構成パラメーターが一覧表示されています。以下により、構成パラメータを特定できます。

- トピック – 設定されているアプリケーションの領域を示します。たとえば、フェイルオーバー構成などです。
- 目的 – AWS Resilience Hub が情報を要求した理由を示します。
- パラメーター – アプリケーションの分野に固有の詳細を示し、AWS Resilience Hub がアプリケーションに関する推奨事項の提示に使用します。現在、このパラメータは 1 つのフェイルオーバーリージョンと 1 つの関連アカウントのキー値のみを使用しています。

アプリケーション設定パラメータの更新

このセクションでは、AWS Elastic Disaster Recovery の構成パラメータを更新し、アプリケーションを公開して、更新後のパラメータを耐障害性評価に含めることができます。

アプリケーション設定パラメータを更新するには

1. ナビゲーションペインで、アプリケーション を選択します。
2. 「アプリケーション」ページで、編集するアプリケーション名を選択します。
3. アプリケーション設定パラメータ タブを選択します。
4. 更新 を選択します。
5. 「アカウント ID」ボックスにフェイルオーバーアカウント IDを入力します。
6. 「リージョン」ドロップダウンリストからフェイルオーバーリージョンを選択します。

> **Note**
>
> この機能を無効にする場合は、ドロップダウンリストから「–」を選択します。

7. 更新して公開 を選択します。

回復力ポリシーの管理

このセクションでは、アプリケーションの回復力ポリシーを作成する方法について説明します。回復力ポリシーを正しく設定することで、アプリケーションの回復力状態を把握できます。回復力ポリシーには、ソフトウェア、ハードウェア、アベイラビリティーゾーン、AWS リージョンなどの中断

タイプからアプリケーションが回復する見込みがあるかどうかを評価するための情報と目標が含まれています。これらのポリシーが実際のアプリケーションを変えたり、影響したりすることはありません。複数のアプリケーションに同じ回復力ポリシーを適用することができます。

回復力ポリシーを作成するときは、目標復旧時間 (RTO) と目標復旧時点 (RPO) を定義します。目標によって、アプリケーションが回復力ポリシーを満たしているかどうかが決まります。ポリシーをアプリケーションに添付し、回復力評価を実行します。ポートフォリオ内のアプリケーションの種類ごとに異なるポリシーを作成できます。たとえば、リアルタイム取引アプリケーションには、月次レポートアプリケーションとは異なる回復力ポリシーが適用されます。

> **Note**
>
> AWS Resilience Hub では回復力ポリシーの RTO フィールドと RPO フィールドにゼロを入力できます。ただし、アプリケーションを評価する際、最も低い評価結果はゼロに近いです。したがって、RTO と RPO のフィールドにゼロを入力すると、推定ワークロード RTO と推定ワークロード RPO の結果はほぼゼロになり、アプリケーションのコンプライアンスステータスはポリシー違反に設定されます。

この評価では、添付されている回復力ポリシーと照らし合わせてアプリケーション構成を評価します。プロセスの最後に、AWS Resilience Hub は、アプリケーションが回復力ポリシーの回復対象に対してどのように対策しているかを評価します。

回復力ポリシーは、アプリケーションでもレジリエンシーポリシーでも作成できます。ポリシーに関連する詳細にアクセスしたり、ポリシーを変更したり削除したりできます。

AWS Resilience Hub はRTO と RPO の目標値を使用して、次のような潜在的な中断に対する回復力を測定します。

- アプリケーション — 必要なソフトウェアサービスまたはプロセスの喪失。
- クラウドインフラストラクチャ — EC2 インスタンスなどのハードウェアの喪失。
- クラウドインフラストラクチャアベイラビリティーゾーン (AZ) — 1 つ以上のアベイラビリティーゾーンが使用できません。
- クラウドインフラストラクチャリージョン — 1 つ以上のリージョンが使用できません。

AWS Resilience Hub を使用すると、カスタマイズされた回復力ポリシーを作成したり、推奨されるオープン標準の回復力ポリシーを使用したりできます。カスタマイズされたポリシーを作成するとき

は、ポリシーに名前を付けて説明し、ポリシーを定義する適切なレベルまたは階層を選択します。これらの階層には、基礎 IT コアサービス、ミッションクリティカル、クリティカル、クリティカル、重要、非クリティカルが含まれます。

アプリケーションのクラスに適した階層を選択します。たとえば、リアルタイム取引システムをクリティカルと分類し、月次レポートアプリケーションを非クリティカルと分類できます。標準ポリシーを使用する場合は、事前に構成された層と中断タイプごとの RTO および RPO ターゲットの値を備えた回復力ポリシーを選択できます。必要な場合には、階層と RTO、RPO 目標を変更できます。

回復力ポリシーは、回復力ポリシーで作成することも、新しいアプリケーションを記述するときに作成することもできます。

回復力ポリシーの作成

AWS Resilience Hub では、回復力ポリシーを作成できます。回復力ポリシーには、ソフトウェア、ハードウェア、アベイラビリティーゾーン、AWS リージョンなどの中断タイプからアプリケーションが回復できるかどうかを評価するための情報と目標が含まれています。これらのポリシーは、実際のアプリケーションを変えたり、影響を与えたりすることはありません。複数のアプリケーションに同じ回復力ポリシーを適用することができます。

回復力ポリシーを作成するときは、目標復旧時間 (RTO) と目標復旧時点 (RPO) を定義します。評価を実行すると、AWS Resilience Hub は、アプリケーションが回復力ポリシーで定義された目標を満たしていると推定されるかどうかを判断します。

評価では、添付されている回復力ポリシーと照らし合わせてアプリケーション構成を評価します。プロセスの最後に、AWS Resilience Hubは、アプリケーションが回復力ポリシーの対象に対してどのように対策しているかを評価します。

> **Note**
>
> AWS Resilience Hub では回復力ポリシーの RTO フィールドと RPO フィールドに値ゼロを入力できます。ただし、アプリケーションを評価する際、最も低い評価結果はゼロに近いです。したがって、RTO と RPO のフィールドにゼロを入力すると、推定ワークロード RTO と推定ワークロード RPO の結果はほぼゼロになり、アプリケーションのコンプライアンスステータスはポリシー違反に設定されます。

回復力ポリシーは、アプリケーションでもレジリエンシーポリシーでも作成できます。ポリシーに関連する詳細にアクセスしたり、ポリシーを変更したり削除したりできます。

アプリケーションで回復力ポリシーを作成するには

1. 左側のナビゲーションメニューで、アプリケーションを選択します。
2. the section called “ステップ 1: アプリケーションを開始して作業を開始する”からthe section called “ステップ 8: アプリケーションにタグを追加する ”までの手順を完了してください。
3. 回復力ポリシー セクションで、回復力ポリシーの作成を選択します。

   回復力ポリシーの作成ページが表示されます。
4. 作成方法の選択 セクションで 、推奨ポリシーに基づいてポリシーを選択を選択します。
5. ポリシーの名前を入力します。
6. 「オプショナル」 ポリシーの説明を入力します。
7. ティア ドロップダウンリストから次のいずれかを選択します。

   - 基本 IT コアサービス
   - ミッションクリティカル
   - 非常事態
   - 重要
   - 非クリティカル
8. RTO と RPO の両方の目標について、カスタマーアプリケーション RTO と RPO のボックスに数値を入力し、その値が表す時間単位を選択します。

   インフラストラクチャとアベイラビリティゾーンのインフラストラクチャ RTO と RPOでこれらのエントリを繰り返します。
9. 「オプショナル」 マルチリージョンアプリケーションを使用している場合は、リージョンの RTO と RPO のターゲットを定義できます。

   リージョンをオンにします。リージョン RTO と RPO の両方の目標について、カスタマーアプリケーション RTO と RPO のボックスに数値を入力し、その値が表す時間単位を選択します。
10. 「オプショナル」 タグを追加する場合は、ポリシーの作成を続行しながら追加することができます。タグの詳細については、AWS参考文献のリソースのタグ付けを参照してください。
11. 「作成」を選択して、ポリシーを作成します。

回復力ポリシーで回復力ポリシーを作成するには

1. 左側のナビゲーションメニューで ポリシー を選択します。

2. 回復力ポリシーセクションで、回復力ポリシーの作成を選択します。

   回復力ポリシーの作成ページが表示されます。
3. ポリシーの名前を入力します。
4. 「オプショナル」 ポリシーの説明を入力します。
5. ティア トから次のいずれかを選択します。

   - 基本 IT コアサービス
   - ミッションクリティカル
   - 非常事態
   - 重要
   - 非クリティカル
6. リージョン RTO と RPO の両方の目標について、カスタマーアプリケーション RTO と RPO のボックスに数値を入力し、その値が表す時間単位を選択します。

   インフラストラクチャとアベイラビリティゾーンのインフラストラクチャ RTO と RPOでこれらのエントリを繰り返します。
7. 「オプショナル」 マルチリージョンアプリケーションを使用している場合は、リージョンの RTO と RPO のターゲットを定義できます。

   リージョンをオンにします。リージョン RTO と RPO の両方の目標について、カスタマーアプリケーション RTO と RPO のボックスに数値を入力し、その値が表す時間単位を選択します。
8. 「オプショナル」 タグを追加する場合は、ポリシーの作成を続行しながら追加することができます。タグの詳細については、AWS参考文献のリソースのタグ付けを参照してください。
9. 「 作成」 を選択して、ポリシーを作成します。

推奨ポリシーに基づいて回復力ポリシーを作成するには

1. 左側のナビゲーションメニューで ポリシー を選択します。
2. 作成方法の選択 セクションで 、推奨ポリシーに基づいてポリシーを選択を選択します。
3. 回復力ポリシーセクションで、回復力ポリシーの作成を選択します。

   回復力ポリシーの作成ページが表示されます。
4. ポリシーの名前を入力します。
5. 「オプショナル」 ポリシーの説明を入力します。

6. 推奨回復力ポリシーセクションで、以下の定義済みの回復力ポリシー階層の中から1つ選択してください。

   - 重要度の低いアプリケーション
   - 重要なアプリケーション
   - クリティカルアプリケーション
   - グローバル・クリティカル・アプリケーション
   - ミッションクリティカルアプリケーション
   - グローバル・ミッション・クリティカル・アプリケーション
   - ファンダメンタル・コア・サービス

7. 回復力ポリシーを作成するには、ポリシーの作成を選択します。

回復力ポリシーの詳細へのアクセス

回復力ポリシーを開くと、そのポリシーに関する重要な詳細が表示されます。キューを編集または削除することもできます。

回復力ポリシーの詳細は、概要とタグという 2 つの主要なビューで構成されています。

概要

基本情報

回復力ポリシーについて、名前、説明、階層、コスト階層、および作成日という情報が表示されます。

推定ワークロード RTO と推定ワークロード RPO

この回復力ポリシーに関連する推定ワークロード RTO と推定ワークロード RPO の中断タイプが表示されます。

タグ

このビューを使用して、アプリケーション内部のタグを管理、追加、および削除します。

回復力ポリシーの詳細で回復力ポリシーを編集するには

1. 左側のナビゲーションメニューで ポリシー を選択します。

2. 回復力ポリシーで、回復力ポリシーを開きます。
3. 編集 を選択します。基本情報、RTO、RPO の各フィールドに適切な変更を入力します。次に、変更の保存を選択します。

回復力ポリシーで回復力ポリシーを編集するには

1. 左側のナビゲーションメニューで ポリシー を選択します。
2. 回復力ポリシーで、回復力ポリシーを選択します。
3. 「アクション」 を選択して、編集 を選択します。
4. 基本情報、RTO、RPO の各フィールドに適切な変更を入力します。次に、変更の保存 を選択します。

回復力ポリシー詳細で回復力ポリシーを削除するには

1. 左側のナビゲーションメニューで ポリシー を選択します。
2. 回復力ポリシーで、回復力ポリシーを開きます。
3. 削除 をクリックします。 削除 を選択し、確定します。

回復力ポリシー内の回復力ポリシーを削除するには

1. 左側のナビゲーションメニューで ポリシー を選択します。
2. 回復力ポリシーで、回復力ポリシーを開きます。
3. 「アクション」を選択して、「削除」 を選択します。
4. 削除 を選択し、確定します。

AWS Resilience Hub レジリエンス評価の実行と管理

アプリケーションが変更されたら、障害耐性評価を実行する必要があります。評価では、各アプリケーションコンポーネントの設定をポリシーと比較し、アラーム、SOP、テストの推奨事項を作成します。これらの推奨構成により、復旧手順の速度を向上させることができます。

アラームの推奨事項は、停止を検出するアラームの設定に役立ちます。SOP の推奨事項には、バックアップからの復旧など、一般的な復旧プロセスを管理するスクリプトが用意されています。テスト推奨事項には、構成が正しく動作していることを確認するための提案が記載されています。例えば、

ネットワークの問題による自動スケーリングや負荷分散などの自動復旧中にアプリケーションが復旧するかどうかをテストできます。また、リソースが上限に達したときにアプリケーションアラームがトリガーされるかどうか、指定した条件下で SOP がどの程度機能するかについても、テストできます。

障害耐性評価の実行

障害耐性評価レポートは、 AWS Resilience Hubの複数の場所から実行できます。アプリケーションの詳細については、「the section called “アプリケーション”」を参照してください。

アクションメニューから回復力評価を実行するには

1. 左側のナビゲーションメニューで、[アプリケーション] を選択します。
2. [アプリケーション] テーブルからアプリケーションを選択します。
3. [アクション] メニューで [障害耐性を評価] を選択します。
4. [耐障害性評価を実行] ダイアログでは、一意の名前を入力することも、生成された評価名を使用することもできます。
5. [実行] を選択します。

   評価レポートを確認するには、アプリケーションで [評価] を選択します。詳細については、「the section called “評価レポートのレビュー”」を参照してください。

評価タブから障害耐性評価を実行するには

アプリケーションまたは障害耐性ポリシーが変更されたときに、新しい障害耐性評価を実行できます。

1. 左側のナビゲーションメニューで、[アプリケーション] を選択します。
2. [アプリケーション] テーブルからアプリケーションを選択します。
3. [評価] タブを選択します。
4. [耐障害性評価を実行] を選択します。
5. [耐障害性評価を実行] ダイアログでは、一意の名前を入力することも、生成された評価名を使用することもできます。
6. [実行] を選択します。

   評価レポートを確認するには、アプリケーションで [評価] を選択します。詳細については、「the section called “評価レポートのレビュー”」を参照してください。

評価レポートのレビュー

評価レポートはアプリケーションの [評価] ビューにあります。

評価レポートを検索するには

1. 左側のナビゲーションメニューで、[アプリケーション] を選択します。
2. [アプリケーション] で、アプリケーションを選択します。
3. [評価] タブの [障害耐性評価] テーブルで評価レポートを選択します。

レポートを開くと、以下のようになります。

- 評価レポートの概要
- 障害耐性を向上させるための推奨事項。
- アラーム、SOP、テストの設定に関する推奨事項
- リソースを検索してフィルタリングするためのタグを作成および管理する方法 AWS

確認

このセクションでは、評価レポートの概要を説明します。 AWS Resilience Hub 各中断タイプと関連するアプリケーションコンポーネントを一覧表示します。また、実際の RTO ポリシーと RPO ポリシーを一覧表示し、アプリケーションコンポーネントがポリシー目標を達成できるかどうかを判断します。

概要

アプリケーションの名前、障害耐性ポリシーの名前、およびレポートの作成日が表示されます。

RTO

アプリケーションが障害耐性ポリシーの目標を満たす見込みがあるかどうかをグラフィカルに表示します。これは、組織に重大な損害を与えることなく、アプリケーションが停止できる時間に基づくものです。この評価により、推定ワークロードの RTO が算出されます。

RPO

アプリケーションが障害耐性ポリシーの目標を満たす見込みがあるかどうかをグラフィカルに表示します。これは、ビジネスに重大な損害が発生する前に、データが失われる可能性のある時間に基づくものです。この評価により、ワークロードの推定 RPO が算出されます。

詳細

[すべての結果] タブと [アプリケーションコンプライアンスドリフト] タブに、各中断タイプの詳細な説明が表示されます。[すべての結果] タブにはコンプライアンスドリフトを含むすべての中断が表示され、[アプリケーションコンプライアンスドリフト] タブにはコンプライアンスドリフトのみが表示されます。中断タイプには、[アプリケーション]、クラウドインフラストラクチャ ([インフラストラクチャ] と [アベイラビリティーゾーン])、[リージョン] があり、それらに関する以下の情報が表示されます。

- AppComponent

  アプリケーションを構成するリソース。例えば、アプリケーションにはデータベースやコンピュートコンポーネントが含まれる場合があります。

- 推定 RTO

  ポリシー設定がポリシー要件と一致しているかどうかを示します。[推定 RTO] と [目標 RTO] の 2 つの値が提供されます。例えば、[目標 RTO] に [2 時間]、[推定ワークロード RTO] に [40 分] という値が表示されている場合は、アプリケーションの現在の RTO が 2 時間であるのに対し、ワークロードの見積もり RTO は 40 分であることがわかります。推定ワークロード RTO の計算は、ポリシーではなく構成に基づいて行われます。その結果、選択したポリシーに関係なく、複数のアベイラビリティーゾーンのデータベースでは、アベイラビリティーゾーンの障害に対する推定ワークロード RTO は同じになります。

- RTO ドリフト

  前回の評価が成功した場合の推定ワークロード RTO からアプリケーションがずれている期間を示します。[推定 RTO] と [RTO ドリフト] という 2 つの値を提供しています。例えば、[推定 RTO] に [2 時間]、[RTO ドリフト]に [40 分] という値が表示される場合、アプリケーションが前回成功した評価の推定ワークロード RTO から 40 分ずれていることがわかります。

- 推定 RPO

  各アプリケーションコンポーネントに設定した [目標 RPO] ポリシーに基づいて、 AWS Resilience Hub が推定した実際の [推定ワークロード RPO] ポリシーを表示します。例えば、アベイラビリティーゾーンの障害に対する障害耐性ポリシーの RPO 目標を 1 時間に設定したとします。推定結果はほぼゼロと計算される可能性があります。これは、すべてのトランザクションをコミットする Amazon Aurora が、複数のアベイラビリティーゾーンにまたがる 6 つのノードのうち 4 つで成功することを前提としています。 point-in-time 復元には 5 分かかる場合があります。

指定しないで選択できる RTO と RPO の目標はリージョンだけです。一部のアプリケーションでは、AWS サービスに重大な依存関係があり、リージョン全体で使用できなくなる可能性がある場合に、復旧計画を立てておくと便利です。

リージョンの RTO や RPO の目標を設定するなど、このオプションを選択すると、そのような障害に対する推定復旧時間と運用上の推奨事項が表示されます。

- RPO ドリフト

  前回の評価で予測されたワークロードの RPO から、アプリケーションがどの程度ずれているかを示します。[推定 RPO] と [RPO ドリフト] という 2 つの値を提供しています。例えば、[推定 RTO] に [2 時間]、[RTO ドリフト] に [40 分] という値が表示される場合、アプリケーションが前回成功した評価の推定ワークロード RTO から 40 分ずれていることがわかります。

障害耐性に関する推奨事項の確認

障害耐性に関する推奨事項では、アプリケーションコンポーネントを評価し、推定ワークロードの RTO と推定ワークロードの RPO、コスト、最小限の変更によって最適化する方法を推奨しています。

では AWS Resilience Hub、「このオプションを選択すべき理由」に記載されている以下の推奨オプションのいずれかを使用して耐障害性を最適化できます。

> **Note**
>
> - AWS Resilience Hub 最大 3 AWS Resilience Hub つの推奨オプションが表示されます。
> - 地域の RTO と RPO の目標を設定すると、 AWS Resilience Hub 推奨オプションに [地域 RTO/RPO に合わせて最適化] が表示されます。リージョナル RTO と RPO 目標が設定されていない場合は、アベイラビリティーゾーン (AZ) の RTO/RPO に合わせた最適化が表示されます。障害耐性ポリシーを作成する際にリージョナル RTO/RPO 目標を設定する方法の詳細については、回復力ポリシーの作成 を参照してください。
> - アプリケーションとその構成の推定ワークロード RTO と推定ワークロード RPO 値は、データ量と個人を考慮して決定されます。 AppComponentsただし、これらの値は推定値にすぎません。アプリケーションの実際の復旧時間をテストするには、独自のテスト (Amazon Fault Injection Service など) を使用してください。

アベイラビリティーゾーン RTO/RPO に合わせて最適化する

アベイラビリティーゾーン (AZ) が停止している間の推定ワークロード復旧時間 (RTO/RPO) を可能な限り短くします。RTO と RPO の目標を満たすほど設定を変更できない場合は、ポリシーを満たす可能性に近づくために、ワークロード AZ の推定復旧時間の最短が通知されます。

リージョン RTO/RPO に合わせた最適化

リージョナル障害発生時のワークロードの推定復旧時間 (RTO/RPO) の最小値。RTO と RPO の目標を満たすほど構成を変更できない場合は、ポリシーを満たす可能性に近づくために、ワークロードのリージョンの推定復旧時間の最短が通知されます。

コストに合わせた最適化

発生する可能性のある、かつ耐障害性ポリシーを満たすことができる最低のコストです。最適化の目標を達成するために構成を十分に変更できない場合は、構成をポリシーを満たす可能性に近づけるために発生する可能性のある最低コストが通知されます。

最小化変更の最適化

ポリシー目標を達成するために最低限必要な変更。最適化の目標を達成するために構成を十分に変更できない場合は、構成をポリシーを満たす可能性に近づけるための推奨変更が通知されます。

最適化カテゴリの内訳には以下の項目が含まれます。

- 説明

  AWS Resilience Hubが提案する構成について説明します。
- 変更

  推奨構成に切り替えるために必要なタスクを説明するためのテキスト変更リスト。
- 基本コスト

  推奨された変更に伴う推定コスト。

  > **Note**
  >
  > 基本コストは使用状況によって異なる場合があり、エンタープライズ割引プログラム (EDP) による割引や特典は含まれていません。
- 推定ワークロード RTO と RPO

変更後の推定ワークロード RTO と推定ワークロード RPO。

AWS Resilience Hub は、アプリケーションコンポーネント (AppComponent) が耐障害性ポリシーに準拠できるかどうかを評価します。 AppComponent が耐障害性ポリシーに準拠しておらず、AWS Resilience Hub がコンプライアンスを促進するための推奨を行えない場合は、 AppComponent 選択したものの復旧時間がの制約内で満たされていないことが原因である可能性があります。 AppComponent AppComponent 制約の例としては、リソースタイプ、ストレージサイズ、リソース設定などがあります。

を耐障害性ポリシーに順守しやすくするには、 AppComponent のリソースの種類を変更するか、リソースが提供できる内容に合わせて耐障害性ポリシーを更新してください。 AppComponent

運用上の推奨事項のレビュー

運用上の推奨事項には、アラーム、SOP、 AWS FIS 実験をテンプレートを使って設定するための推奨事項が含まれています。 AWS CloudFormation

AWS Resilience Hub AWS CloudFormation アプリケーションのインフラストラクチャをコードとしてダウンロードして管理するためのテンプレートファイルが用意されています。そのため、アプリケーションコードに追加できるように、 AWS CloudFormation で推奨事項が提供されます。 AWS CloudFormation テンプレートファイルのサイズが 1 MB を超え、500 個を超えるリソースが含まれている場合は、各ファイルのサイズが 1 MB 以下で、最大 500 AWS Resilience Hub AWS CloudFormation 個のリソースを含む複数のテンプレートファイルが生成されます。 AWS CloudFormation テンプレートファイルが複数のファイルに分割されている場合、 AWS CloudFormation テンプレートファイル名にはが付加されます。はpartXofY、シーケンス内のファイル番号、X AWS CloudFormation テンプレートファイルが分割されたファイルの総数を示します。Y例えば、テンプレートファイル `big-app-template5-Alarm-104849185070-us-west-2.yaml` が 4 つのファイルに分割されている場合、ファイル名は次のようになります。

- `big-app-template5-Alarm-104849185070-us-west-2-part1of4.yaml`
- `big-app-template5-Alarm-104849185070-us-west-2-part2of4.yaml`
- `big-app-template5-Alarm-104849185070-us-west-2-part3of4.yaml`
- `big-app-template5-Alarm-104849185070-us-west-2-part4of4.yaml`

ただし、 AWS CloudFormation 大きなテンプレートの場合は、ローカルファイルを入力として CLI / API を使用する代わりに、Amazon Simple Storage Service URI を指定するように求められます。

では AWS Resilience Hub、以下のアクションを実行できます。

- 選択したアラーム、SOP、 AWS FIS テストをプロビジョニングできます。アラーム、SOP、AWS FIS テストをプロビジョニングするには、適切な推奨事項を選択し、一意の名前を入力します。 AWS Resilience Hub 選択した推奨事項に基づいてテンプレートを作成します。[テンプレート] では、Amazon Simple Storage Service (Amazon S3) URL を通じて作成したテンプレートにアクセスできます。
- アプリケーションに推奨されたアラーム、SOP、 AWS FIS テストをいつでも含めたり除外したりできます。詳細については、the section called “運用上の推奨事項を含めるまたは除外する” を参照してください。
- また、アプリケーションのタグを検索、作成、追加、削除、管理して、そのアプリケーションに関連するすべてのタグを確認することもできます。

運用上の推奨事項を含めるまたは除外する

AWS Resilience Hub アプリケーションの耐障害性スコアを向上させるために推奨されていたアラーム、SOP、 AWS FIS 実験 (テスト) をいつでも含めたり除外したりできます。運用上の推奨事項を含めたり除外したりしても、新しい評価を実行した後でのみ、アプリケーションの耐障害性スコアに影響します。そのため、評価を実施して最新の耐障害性スコアを取得し、アプリケーションへの影響を把握することをお勧めします。

アプリケーションごとに推奨事項を含めたり除外したりするためのアクセス許可の制限の詳細については、the section called “ AWS Resilience Hub 推奨事項を含めたり除外したりする権限の制限” を参照してください。

運用上の推奨事項をアプリケーションに含めたり除外したりするには

1. 左側のナビゲーションメニューで、[アプリケーション] を選択します。
2. [アプリケーション] で、アプリケーションを選択します。
3. [評価] を選択し、[障害耐性評価] 表から評価を選択します。評価を受けていない場合は、the section called “障害耐性評価の実行” の手順を完了してからこのステップに戻ってください。
4. [運用上の推奨事項] タブを選択します。
5. 運用上の推奨事項をアプリケーションに含める、またはアプリケーションから除外するには、以下のステップを実行します。

推奨アラームをアプリケーションに含めたり除外したりするには

1. アラームを除外するには、以下のステップを実行します。

   a. [アラーム] タブの [アラーム] テーブルから、除外するアラーム ([未実装] ステータス) をすべて選択します。アラームの現在の実装状況は、[ステータス] 列で確認できます。

   b. [アクション] から [選択項目を除外] を選択します。

   c. [推奨項目を除外] ダイアログから、以下のいずれかの理由 (オプション) を選択し、[選択項目を除外] を選択すると、選択したアラームがアプリケーションから除外されます。

      - すでに実装済み — AWS Amazonなどのサービスやその他のサードパーティのサービスプロバイダーにこれらのアラームをすでに実装している場合は CloudWatch、このオプションを選択してください。
      - [該当なし] — アラームがビジネス要件に合わない場合は、このオプションを選択してください。
      - [実装が複雑すぎる] — アラームが複雑すぎて実装できないと思われる場合は、このオプションを選択してください。
      - [その他] — 推奨項目を除外するその他の理由を指定する場合は、このオプションを選択してください。

2. アラームを含めるには、次のステップを実行します。

   a. [アラーム] タブの [アラーム] テーブルから、含めたいアラーム ([除外] ステータス) をすべて選択します。アラームの現在の実装状況は、[ステータス] 列で確認できます。

   b. [アクション] から [選択項目を含める] を選択します。

   c. [推奨項目を含める] ダイアログで [選択項目を含める] を選択すると、選択したすべてのアラームがアプリケーションに含められます。

推奨標準作業手順 (SOP) をアプリケーションに含めたり除外したりするには

1. 推奨 SOP を除外するには、以下のステップを実行します。

   a. [標準作業手順] タブの [SOP] テーブルから、除外するすべての SOP ([実施済み] または [未実装]) を選択します。SOP の現在の実施ステータスは、[ステータス] 列で確認できます。

   b. [アクション] から [選択項目を除外] を選択し、選択した SOP をアプリケーションから除外します。

c. [推奨項目を除外] ダイアログから、以下のいずれかの理由 (オプション) を選択し、[選択項目を除外] を選択して、選択した SOP をアプリケーションから除外します。

- [既に実装済み] — これらの SOP を AWS サービスまたは他のサードパーティのサービスプロバイダーですでに実装している場合は、このオプションを選択してください。
- [該当なし] — SOP がビジネス要件に合わない場合は、このオプションを選択してください。
- [実装が複雑すぎる] — これらの SOP が複雑すぎて実装できないと思われる場合は、このオプションを選択してください。
- [なし] — 理由を指定しない場合は、このオプションを選択してください。

2. SOP を含めるには、次のステップを実行します。

a. [標準作業手順書] タブの [SOP] テーブルから、含めたいアラーム ([除外] ステータス) をすべて選択します。アラームの現在の実装状況は、[ステータス] 列で確認できます。

b. [アクション] から [選択項目を含める] を選択します。

c. [レコメンデーションを含める] ダイアログで [選択したものを含める] を選択すると、選択したすべての SOP がアプリケーションに含められます。

推奨テストをアプリケーションに含めたり除外したりするには

1. 推奨テストを除外するには、以下のステップを実行します。

a. [故障注入実験テンプレート] タブの [故障注入実験テンプレート] テーブルから、除外したいテスト ([実装済み] または [未実装] ステータス) をすべて選択します。テストの現在の実装状況は、[ステータス] 列で確認できます。

b. [アクション] から [選択項目を除外] を選択します。

c. [推奨項目を除外] ダイアログから、以下のいずれかの理由 (オプション) を選択し、[選択項目を除外] を選択すると、選択した AWS FIS 実験がアプリケーションから除外されます。

- すでに実装済み — AWS これらのテストをサービスまたは他のサードパーティのサービスプロバイダーですでに実装している場合は、このオプションを選択してください。
- [該当なし] — テストがビジネス要件に合わない場合は、このオプションを選択してください。
- [実装が複雑すぎる] — テストが複雑すぎて実装できないと思われる場合は、このオプションを選択してください。

- [なし] — 理由を指定しない場合は、このオプションを選択してください。

2. 推奨テストを含めるには、以下のステップを実行します。

   a. [故障注入実験テンプレート] タブの [故障注入実験テンプレート] テーブルから、含めたいテスト ([除外] ステータス) をすべて選択します。テストの現在の実装状況は、[ステータス] 列で確認できます。
   b. [アクション] から [選択項目を含める] を選択します。
   c. [推奨項目を含める] ダイアログから [選択したものを含める] を選択すると、選択したすべてのテストがアプリケーションに含められます。

障害耐性評価の削除

アプリケーションの [評価] ビューで障害耐性評価を削除できます。

障害耐性評価を削除するには

1. 左側のナビゲーションメニューで、[アプリケーション] を選択します。
2. [アプリケーション] で、アプリケーションを選択します。
3. [評価] で、[障害耐性評価] 表から評価レポートを選択します。
4. 削除を確認するには、[削除] を選択します。

   レポートは [障害耐性評価] 表に表示されなくなります。

アラームの管理

耐障害性評価を実施する場合、運用上の推奨事項の一部として、Amazon AWS Resilience Hub CloudWatch アラームを設定してアプリケーションの耐障害性を監視することを推奨しています。これらのアラームは、現在のアプリケーション設定のリソースとコンポーネントに基づいて推奨されます。アプリケーション内のリソースやコンポーネントが変更された場合は、障害耐性評価を実行して、更新したアプリケーションに適したアラームが適用されていることを確認する必要があります。

AWS Resilience Hub には、 AWS Resilience Hub 内部（AmazonなどREADME.md） AWSまたは外部が推奨するアラームを作成できるテンプレートファイル AWS （ CloudWatch ）が用意されています。アラームに設定されているデフォルト値は、これらのアラームの作成に使用されたベストプラクティスに基づいています。

トピック

- 運用上の推奨事項に基づいてアラームを作成します。
- アラームを表示する

運用上の推奨事項に基づいてアラームを作成します。

AWS Resilience Hub Amazon AWS CloudFormation CloudWatch で選択したアラームを作成するための詳細を含むテンプレートを作成します。テンプレートが生成されたら、Amazon S3 のURL を介してテンプレートにアクセスし、ダウンロードしてコードパイプラインに配置するか、 AWS CloudFormation コンソールからスタックを作成できます。

AWS Resilience Hub 推奨事項に基づいてアラームを作成するには、 AWS CloudFormation 推奨アラームのテンプレートを作成し、コードベースに含める必要があります。

運用上の推奨事項にアラームを作成するには

1. 左側のナビゲーションメニューで、[アプリケーション] を選択します。
2. アプリケーションで、アプリケーションを選択します。
3. [評価] タブを選択します。

   [障害耐性評価] 表では、以下の情報を使用して評価を特定できます。

   - [名前] – 作成時に提供した評価の名前。
   - [ステータス] – 評価の実行状態を示します。
   - [コンプライアンスステータス] – 評価が障害耐性ポリシーに準拠しているかどうかを示します。
   - [障害耐性ドリフトステータス] – アプリケーションが前回の成功した評価から逸脱したかどうかを示します。
   - [アプリバージョン] – アプリケーションのバージョン。
   - [呼び出した人] – 評価を呼び出したロールを示します。
   - [開始時刻] – 評価の開始時刻を示します。
   - [終了時刻] – 評価の終了時刻を示します。
   - [ARN] - 評価の Amazon リソースネーム (ARN)。
4. [障害耐性評価] 表から評価を選択します。評価を受けていない場合は、the section called “障害耐性評価の実行” の手順を完了してからこのステップに戻ってください。
5. [運用上の推奨事項] を選択します。

6. デフォルトで選択されていない場合は、[アラーム] タブを選択します。

   [アラーム] テーブルでは、以下を使用して推奨アラームを識別できます。

   - [名前] – アプリケーションに設定したアラームの名前。
   - [説明] – アラームの目的を説明します。
   - 状態 — Amazon CloudWatch アラームの現在の実装状態を示します。

     この列には、次のいずれかの値が表示されます。

     - 実装済み — AWS Resilience Hub が推奨するアラームがアプリケーションに実装されていることを示します。以下の番号を選択すると、[アラーム] テーブルがフィルタリングされ、アプリケーションに実装されている推奨アラームがすべて表示されます。
     - 未実装 — AWS Resilience Hub が推奨するアラームがアプリケーションに含まれていても実装されていないことを示します。以下の番号を選択すると、[アラーム] テーブルがフィルタリングされ、アプリケーションに実装されていない推奨アラームがすべて表示されます。
     - 除外 — AWS Resilience Hub が推奨するアラームがアプリケーションから除外されていることを示します。以下の番号を選択すると、[アラーム] テーブルがフィルタリングされ、アプリケーションから除外されている推奨アラームがすべて表示されます。推奨アラームを含めるか除外するかについて詳しくは、「運用上の推奨事項を含める/除外する」を参照してください。
     - 非アクティブ — アラームは Amazon に配信されているが CloudWatch、Amazon ではステータスが INSUFFICIENT_DATA に設定されていることを示します。 CloudWatch以下の番号を選択すると、[アラーム] テーブルがフィルタリングされ、実装済みのアラームと非アクティブなアラームがすべて表示されます。
   - [構成] – 対処する必要のある保留中の構成の依存関係があるかどうかを示します。
   - [タイプ] – アラームの種類を示します。
   - AppComponent— このアラームに関連付けられているアプリケーションコンポーネント (AppComponents) を示します。
   - Reference ID — AWS CloudFormation 内のスタックイベントの論理識別子を示します AWS CloudFormation。
   - レコメンデーション ID — AWS CloudFormation 内のスタックリソースの論理識別子を示します AWS CloudFormation。

7. [アラーム] タブで、[アラーム] テーブル内のアラーム推奨事項を特定の状態に基づいてフィルタリングするには、その下にある番号を選択します。

8. アプリケーションに設定したい推奨アラームを選択し、「Create CloudFormation template」を選択します。
9. [CloudFormation テンプレートの作成] ダイアログでは、自動生成された名前を使用するか、[テンプレート名] AWS CloudFormation CloudFormation ボックスにテンプレートの名前を入力できます。
10. [作成] を選択します。 AWS CloudFormation テンプレートの作成には数分かかることがあります。

    コードベースに推奨事項を含めるには、以下の手順を実行します。

AWS Resilience Hub レコメンデーションをコードベースに含めるには

1. [テンプレート] タブを選択すると、作成したテンプレートが表示されます。テンプレートを特定するには、以下を使用します。

    - [名前] – 作成時に提供した評価の名前。
    - [ステータス] – 評価の実行状態を示します。
    - [タイプ] – 運用上の推奨事項の種類を示します。
    - [フォーマット] – テンプレートが作成されるフォーマット (JSON/テキスト) を示します。
    - [開始時刻] – 評価の開始時刻を示します。
    - [終了時刻] – 評価の終了時刻を示します。
    - ARN – テンプレートの ARN
2. [テンプレートの詳細] で、[テンプレート S3 パス] の下のリンクを選択し、Amazon S3 コンソールでテンプレートオブジェクトを開きます。
3. Amazon S3 のコンソールで、[オブジェクト] テーブルから SOP フォルダへのリンクを選択します。
4. Amazon S3 のパスをコピーするには、JSON ファイルの前にあるチェックボックスを選択し、[URL をコピー] を選択します。
5. AWS CloudFormation AWS CloudFormation コンソールからスタックを作成する。
   AWS CloudFormation スタックの作成について詳しくは、を参照してくださいhttps://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-console-create-stack.html。

    AWS CloudFormation スタックの作成時に、前のステップでコピーした Amazon S3 パスを指定する必要があります。

アラームを表示する

アプリケーションの耐障害性を監視するために設定したアクティブなアラームをすべて表示できます。 AWS Resilience Hub AWS CloudFormation テンプレートを使用してアラームの詳細を保存し、それを Amazon でアラームを作成する際に使用されます。 CloudWatchAmazon S3 URL AWS CloudFormation を使用してテンプレートにアクセスし、ダウンロードしてコードパイプラインに配置するか、 AWS CloudFormation コンソールからスタックを作成できます。

ダッシュボードからアラームを表示するには、左側のナビゲーションメニューから [ダッシュボード] を選択します。[アラーム] テーブルでは、以下を使用して実装されたアラームを識別できます。

- [影響を受けるアプリケーション] – このアラームを実装したアプリケーションの名前。
- [アクティブアラーム] – アプリケーションからトリガーされたアクティブなアラームの数を示します。
- FIS in progress — AWS FIS アプリケーションに対して現在実行中の実験を示します。

実装されたアラームをアプリケーションから確認するには

1. 左側のナビゲーションメニューで、[アプリケーション] を選択します。
2. [アプリケーション] テーブルからアプリケーションを選択します。
3. アプリケーション概要ページの [実装済みアラーム] テーブルには、アプリケーションに実装されている推奨アラームがすべて表示されます。

   [実装済みアラーム] テーブルで特定のアラームを検索するには、[テキスト、プロパティ、または値でアラームを検索] ボックスで、次のいずれかのフィールドを選択し、操作を選択して、値を入力します。

   - [アラーム名] – アプリケーションに設定したアラームの名前。
   - [説明] – アラームの目的を説明します。
   - 状態 — Amazon CloudWatch アラームの現在の実装状態を示します。

     この列には、次のいずれかの値が表示されます。

     - 実装済み — AWS Resilience Hub が推奨するアラームがアプリケーションに実装されていることを示します。以下の番号を選択すると、[運用上の推奨事項] タブに推奨アラームと実装済みアラームがすべて表示されます。

- 未実装 — AWS Resilience Hub が推奨するアラームがアプリケーションに含まれていても実装されていないことを示します。以下の番号を選択すると、[運用上の推奨事項] タブに推奨されているアラームと実装されていないアラームがすべて表示されます。
- 除外 — AWS Resilience Hub が推奨するアラームがアプリケーションから除外されていることを示します。以下の番号を選択すると、[運用上の推奨事項] タブに推奨アラームと除外アラームがすべて表示されます。推奨アラームを含めるか除外するかについて詳しくは、「運用上の推奨事項を含める/除外する」を参照してください。
- 非アクティブ — アラームは Amazon に配信されているが CloudWatch、Amazon ではステータスが INSUFFICIENT_DATA に設定されていることを示します。 CloudWatch以下の番号を選択すると、[運用上の推奨事項] タブに実装済みのアラームと非アクティブなアラームがすべて表示されます。

- ソーステンプレート — AWS CloudFormation アラームの詳細を含むスタックの Amazon リソースネーム (ARN) を提供します。
- [リソース] – このアラームがアタッチされ、かつ実装されたリソースを表示します。
- メトリック — アラームに割り当てられた Amazon CloudWatch メトリクスを表示します。Amazon メトリクスの詳細については、「Amazon CloudWatch CloudWatch メトリクス」を参照してください。
- [最終変更] – アラームが最後に変更された日付と時刻が表示されます。

評価から推奨されるアラームを確認するには

1. 左側のナビゲーションメニューで、[アプリケーション] を選択します。
2. [アプリケーション] テーブルからアプリケーションを選択します。

   アプリケーションを検索するには、[アプリケーションを検索] ボックスにアプリケーション名を入力します。
3. [評価] タブを選択します。

   [障害耐性評価] 表では、以下の情報を使用して評価を特定できます。

   - [名前] – 作成時に提供した評価の名前。
   - [ステータス] – 評価の実行状態を示します。
   - [コンプライアンスステータス] – 評価が障害耐性ポリシーに準拠しているかどうかを示します。

- [障害耐性ドリフトステータス] – アプリケーションが前回の成功した評価から逸脱したかどうかを示します。
- [アプリバージョン] – アプリケーションのバージョン。
- [呼び出した人] – 評価を呼び出したロールを示します。
- [開始時刻] – 評価の開始時刻を示します。
- [終了時刻] – 評価の終了時刻を示します。
- [ARN] - 評価の Amazon リソースネーム (ARN)。

4. [障害耐性評価] 表から評価を選択します。
5. [運用上の推奨事項] タブを選択します。
6. デフォルトで選択されていない場合は、[アラーム] タブを選択します。

   [アラーム] テーブルでは、以下を使用して推奨アラームを識別できます。

   - [名前] – アプリケーションに設定したアラームの名前。
   - [説明] – アラームの目的を説明します。
   - 状態 — Amazon CloudWatch アラームの現在の実装状態を示します。

     この列には、次のいずれかの値が表示されます。

     - [実装済み] – アラームがアプリケーションに実装されていることを示します。以下の番号を選択すると、[アラーム] テーブルがフィルタリングされ、アプリケーションに実装されている推奨アラームがすべて表示されます。
     - [未実装] – アラームがアプリケーションに実装されていないか、含まれていないことを示します。以下の番号を選択すると、[アラーム] テーブルがフィルタリングされ、アプリケーションに実装されていない推奨アラームがすべて表示されます。
     - [除外] – アラームがアプリケーションから除外されていることを示します。以下の番号を選択すると、[アラーム] テーブルがフィルタリングされ、アプリケーションから除外されている推奨アラームがすべて表示されます。推奨アラームを含める/除外する方法の詳細については、「the section called “運用上の推奨事項を含めるまたは除外する”」を参照してください。
     - 非アクティブ — アラームは Amazon に配信されているが CloudWatch、Amazon ではステータスが INSUFFICIENT_DATA に設定されていることを示します。 CloudWatch以下の番号を選択すると、[アラーム] テーブルがフィルタリングされ、実装済みのアラームと非アクティブなアラームがすべて表示されます。

   - [構成] – 対処する必要のある保留中の構成の依存関係があるかどうかを示します。

- [タイプ] – アラームの種類を示します。
- AppComponent— このアラームに関連付けられているアプリケーションコンポーネント (AppComponents) を示します。
- Reference ID — AWS CloudFormation 内のスタックイベントの論理識別子を示します AWS CloudFormation。
- レコメンデーション ID — AWS CloudFormation 内のスタックリソースの論理識別子を示します AWS CloudFormation。

標準操作手順

標準運用手順 (SOP) は、システム停止やアラームが発生した場合にアプリケーションを効率的に復旧するための規範的な一連の手順です。運用上の障害が発生した場合にタイムリーに復旧できるように、SOP を事前に準備、テスト、測定します。

アプリケーションコンポーネントに基づいて、AWS Resilience Hub は、準備すべき SOP を推奨します。AWS Resilience Hub は Systems Manager と連携して、SOP の基礎として使用できる多数の SSM ドキュメントを提供することで、SOP の手順を自動化します。

たとえば、AWS Resilience Hub は既存の SSM 自動化ドキュメントに基づいてディスク容量を追加するための SOP を推奨する場合があります。この SSM ドキュメントを実行するには、適切なアクセス許可を持つ特定の IAM ロールが必要です。AWS Resilience Hub は、ディスクが不足した場合に実行する SSM 自動化ドキュメントと、その SSM ドキュメントを実行するために必要な IAM ロールを示すメタデータをアプリケーションに作成します。その後、このメタデータは SSM パラメータに保存されます。

SSM 自動化を設定することに加えて、AWS FIS の実験を行ってテストすることもベストプラクティスです。そのため、AWS Resilience Hub は SSM 自動化ドキュメントを呼び出す AWS FIS の実験も行っています。こうすることで、事前にアプリケーションをテストして、作成したSOPが意図したとおりに機能することを確認できます。

AWS Resilience Hub は、アプリケーションのコードベースに追加できる AWS CloudFormation のテンプレートの形式で、その推奨事項を提供します。このテンプレートは以下を提供します。

- SOPの実行に必要な権限を持つ IAM ロール。
- SOPのテストに使える AWS FIS の実験。

- どの SSM ドキュメントと IAM ロールを SOP として実行するか、どのリソースで実行するかを示すアプリケーションメタデータを含む SSM パラメータ。例: `$(DocumentName) for SOP $(HandleCrisisA) on $(ResourceA)`。

SOP の作成には試行錯誤が必要な場合があります。まずは、アプリケーションに対して耐障害性評価を実行し、AWS Resilience Hub の推奨事項に基づいて AWS CloudFormation のテンプレートを生成することから始めるとよいでしょう。AWS CloudFormationのテンプレートを使用して AWS CloudFormation のスタックを生成し、次に SSM パラメータとそのデフォルト値をSOPで使用します。SOPを実行して、どのような改良が必要かを確認してください。

アプリケーションごとに要件が異なるため、AWS Resilience Hub によって提供されている SSM ドキュメントのデフォルトリストではすべてのニーズを満たすことはできません。ただし、デフォルトの SSM ドキュメントをコピーして、それを基にしてアプリケーションに合わせた独自のカスタムドキュメントを作成することはできます。独自のまったく新しい SSM ドキュメントを作成することもできます。デフォルトを変更する代わりに独自の SSM ドキュメントを作成する場合は、SOP の実行時に正しい SSM ドキュメントが呼び出されるように、それらを SSM パラメータに関連付ける必要があります。

必要な SSM ドキュメントを作成し、必要に応じてパラメータとドキュメントの関連付けを更新して SOP を完成させたら、SSM ドキュメントをコードベースに直接追加し、後で変更やカスタマイズを行います。そうすれば、アプリケーションをデプロイするたびに、最新の SOP もデプロイできます。

トピック

AWS Resilience Hub の推奨事項に基づいて SOP を構築する。

AWS Resilience Hub の推奨事項に基づいてSOPを構築するには、レジリエンスポリシーが適用された AWS Resilience Hub のアプリケーションが必要で、そのアプリケーションに対してレジリエンス評価を実行している必要があります。レジリエンス評価により、SOP の推奨事項が生成されます。

AWS Resilience Hub の推奨事項に基づいてSOPを構築するには、推奨SOPの AWS CloudFormation のテンプレートを作成し、コードベースに含める必要があります。

SOP 推奨事項の AWS CloudFormation のテンプレートを作成してください。

1. AWS Resilience Hub コンソールを開きます。
2. ナビゲーションペインで、アプリケーション を選択します。
3. アプリケーションのリストで、SOPを作成したいアプリケーションを選択します。
4. 評価 タブを選択します。
5. 「レジリエンス評価」表から評価を選択します。評価を受けていない場合は、the section called “障害耐性評価の実行” の手順を完了してからこのステップに戻ってください。
6. 「運用上の推奨事項」で、標準運用手順 を選択します。
7. 含めたい SOP 推奨事項をすべて選択します。
8. CloudFormation テンプレートの作成 を選択します。AWS CloudFormation のテンプレートの作成に数分かかることがあります。

   コードベースに SOP 推奨事項を含めるには、以下の手順を実行します。

AWS Resilience Hub の推奨事項をコードベースに含めるには

1. 「運用上の推奨事項」で テンプレート を選択します。
2. テンプレートのリストで、先ほど作成した SOP テンプレートの名前を選択します。

   以下の情報を使用して、アプリケーションに実装されている SOP を特定できます。

   - SOP 名 – アプリケーション用に定義した SOP の名前。
   - 説明 – SOP の目的を説明します。
   - SSM ドキュメント – SOP 定義を含む SSM ドキュメントの Amazon S3 のURL。
   - テスト実行 – 最新のテストの結果を含むドキュメントの Amazon S3 のURL。
   - ソーステンプレート – SOP の詳細を含む AWS CloudFormation のスタックの Amazon リソースネーム (ARN) を指定します。
3. テンプレートの詳細 で、テンプレート S3 パス のリンクを選択し、Amazon S3 のコンソールでテンプレートオブジェクトを開きます。
4. Amazon S3 のコンソールで、オブジェクトテーブルから SOP フォルダへのリンクを選択します。

5. Amazon S3 のパスをコピーするには、JSON ファイルの前にあるチェックボックスを選択し、URL をコピー を選択します。
6. コンソールで スタックを作成します。AWS CloudFormation ロールの作成の詳細については、「https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-console-create-stack.html」を参照してください。

   AWS CloudFormation のスタックの作成時に、前のステップでコピーした Amazon S3 のパスを指定する必要があります。

カスタム SSM ドキュメントの削除

アプリケーションのリカバリを完全に自動化するには、Systems Manager コンソールで SOP 用のカスタム SSM ドキュメントを作成する必要がある場合があります。既存の SSM ドキュメントをベースとして変更することも、新しい SSM ドキュメントを作成することもできます。

Systems Manager を使用して SSM ドキュメントを作成する方法の詳細については、「チュートリアル:ドキュメントビルダーを使用してカスタムランブックを作成する」を参照してください。

SSM ドキュメント構文について詳しくは、SSM ドキュメント構文を参照してください。

オートメーションアクションの詳細については、 の「 オートメーションのリファレンス」を参照してください。

デフォルトの代わりにカスタム SSM ドキュメントを使用する

SOP 用に提案された SSM ドキュメント AWS Resilience Hub を、作成したカスタムドキュメントに置き換えるには、コードベースで直接作業してください。新しいカスタム SSM 自動化ドキュメントを追加することに加えて、以下の作業も行います。

1. 自動化の実行に必要な IAM 権限を追加します。
2. SSM ドキュメントをテストする AWS FIS の実験を追加します。
3. SOP として使用したい自動化ドキュメントを指す SSM パラメータを追加します。

一般的には、AWS Resilience Hub の推奨デフォルト値をそのまま使用し、必要に応じてカスタマイズするのが最も効率的です。たとえば、IAM ロールに必要な権限を追加または削除したり、新しい SSM ドキュメントを指すように AWS FIS の実験設定を変更したり、新しい SSM ドキュメントを指すように SSM パラメータを変更したりします。

SOP のテスト

前述のように、ベストプラクティスは CI/CD パイプラインに AWS FIS の実験を追加して SOP を定期的にテストすることです。これにより、障害が発生した場合でも準備が整います。

AWS Resilience Hub によって提供された SOP とカスタム SOP の両方をテストします。

標準操作手順

実装された SOP をアプリケーションから確認するには

1. 左側のナビゲーションメニューで、アプリケーションを選択します。
2. アプリケーション で、アプリケーションを選択します。
3. 標準操作手順 タブを選択します。

   「標準運用手順の概要」セクションの「実施済み標準運用手順」表には、SOP の推奨事項から生成された SOP のリストが表示されます。

   SOP を特定するには、以下を使用します。

   - SOP 名 – アプリケーション用に定義した SOP の名前。
   - SSM ドキュメント – SOP 定義を含む Amazon EC2 Systems Manager ドキュメントの S3 の URL。
   - 説明 – SOP の目的を説明します。
   - テスト実行 – 最新のテストの結果を含むドキュメントの S3 のURL。
   - 参照 ID – 参照されている SOP 推奨事項の識別子。
   - リソース ID – SOP 勧告が実装されているリソースの識別子。

評価から推奨される SOP を確認するには

1. 左側のナビゲーションメニューで、アプリケーションを選択します。
2. 「アプリケーション」テーブルからアプリケーションを選択します。

   アプリケーションを検索するには、「アプリケーションを検索」ボックスにアプリケーション名を入力します。
3. 評価 タブを選択します。

   「レジリエンス評価」表では、以下の情報を使用して評価を特定できます。

- 名前 – 作成時に提供した評価の名前。
- ステータス – 評価の実行状態を示します。
- コンプライアンスステータス – 評価がレジリエンシーポリシーに準拠しているかどうかを示します。
- 耐障害性ドリフトステータス – アプリケーションが前回の成功した評価から逸脱したかどうかを示します。
- アプリバージョン – アプリケーションのバージョン。
- 呼び出した人 – 評価を呼び出したロールを示します。
- 開始時刻 – 評価の開始時刻を示します。
- 終了時刻 – 評価の終了時刻を示します。
- ARN - 評価の Amazon リソースネーム (ARN)。

4. 「レジリエンス評価」表から評価を選択します。
5. 運用上の推奨事項 タブを選択します。
6. 標準操作手順 タブを選択します。

   標準運用手順表では、以下の情報を参考に推奨SOPについてさらに理解を深めることができます。

   - 名前 – 推奨SOPの名前。
   - 説明 – SOP の目的を説明します。
   - 状態 – SOP の現在の実施状況を示します。表示は、「実装済み」、「未実装」、および「除外」です。
   - 構成 – 対処する必要のある保留中の構成の依存関係があるかどうかを示します。
   - タイプ – SOP のタイプを示します。
   - AppComponent – このSOPに関連するアプリケーションコンポーネント (AppComponents) を示します。サポートされている AppComponents について詳しくは、「AppComponent内のリソースのグループ化」を参照してください。
   - 参照 ID –AWS CloudFormation 内の AWS CloudFormation のスタックイベントの論理識別子を示します。
   - レコメンデーション ID – AWS CloudFormation 内の AWS CloudFormation のスタックリソースの論理識別子を示します。

Amazon Fault Injection Service の実験

このセクションでは、 AWS Resilience Hubで Amazon Fault Injection Service AWS FISの実験を作成して実行する方法について説明します。 AWS FIS 実験を実行して、 AWS リソースの回復力と、アプリケーション、インフラストラクチャ、アベイラビリティーゾーン、 AWS リージョン インシデントからの回復にかかる時間を測定します。

レジリエンスを測定するために、 AWS FIS これらの実験ではリソースの中断をシミュレートします。 AWS 中断の例としては、ネットワーク利用不可エラー、フェールオーバー、Amazon EC2 または AWS ASG でのプロセスの停止、Amazon RDS でのブートリカバリ、アベイラビリティーゾーンの問題などがあります。 AWS FIS 実験が終了すると、耐障害性ポリシーの RTO ターゲットで定義されている停止タイプからアプリケーションが復旧できるかどうかを見積もることができます。

この実験はすべて、を使用して構築され AWS FIS 、アクションを実行します AWS FIS 。 AWS Resilience Hub AWS FIS 実験の大半は、Systems Manager の自動化アクションを呼び出して中断を実行し、アラームを監視しますが、 AWS FIS 他の実験では、 AWS FIS AWS 特定のサービスに合わせてカスタマイズされた自動化アクション (Amazon EKS アクションなど) のみを使用します。 AWS FIS アクションの詳細については、「AWS FIS アクションのリファレンス」を参照してください。

AWS FIS テストはデフォルトの状態で使用することも、要件に基づいてカスタマイズすることもできます。 AWS FIS テストには AWS Resilience Hub (the section called “故障注入実験を表示する”) AWS FIS またはコンソール (AWS FIS) からアクセスできます。

トピック

- AWS FIS 運用上の推奨事項から実験を作成する
- AWS FIS から実験を実行します。 AWS Resilience Hub
- 故障注入実験を表示する
- Amazon Fault Injection Service の実験失敗/ステータスチェック

AWS FIS 運用上の推奨事項から実験を作成する

AWS Resilience Hub 評価レポートを実行した後でアプリケーションをテストすることを推奨します。これらの実験は、アプリケーションの評価レポートからアクセスして実行できます。

AWS Resilience Hub テストパラメータを含む Systems Manager AWS FIS ドキュメントである実験のリストが表示されます。 AWS FIS リストから実験を選択すると、Systems Manager AWS Resilience Hub AWS CloudFormation ドキュメントで定義したパラメータを使用してテンプレートが

作成されます。 AWS CloudFormation スタックの作成後、 AWS FIS アプリケーションにプロビジョニングされたテストを確認できます。

AWS CloudFormation テンプレートは、実行に必要な最小限の権限を持つ、各 Systems Manager ドキュメントの IAM ロールで構成されています。

AWS FIS AWS Resilience Hub 推奨事項に基づいてテストを作成するには、 AWS CloudFormation 推奨テストのテンプレートを作成し、コードベースに含める必要があります。

AWS CloudFormationAWS FIS 実験用のテンプレートを作成するには

1. AWS Resilience Hub コンソールを開きます。
2. ナビゲーションペインで、[アプリケーション] を選択します。
3. アプリケーションのリストで、テストを作成するアプリケーションを選択します。
4. [評価] タブを選択します。
5. [障害耐性評価] 表から評価を選択します。評価を受けていない場合は、the section called “障害耐性評価の実行” の手順を完了してからこのステップに戻ってください。
6. [運用上の推奨事項] で、[故障注入実験] を選択します。
7. 含めたいテストをすべて選択します。
8. [CloudFormation テンプレートを作成] を選択します。 AWS CloudFormation テンプレートの作成には数分かかることがあります。
9. テンプレートを選択します。

   AWS CloudFormation 新しく作成したテンプレートは Templates テーブルで確認できます。

   コードベースに推奨事項を含めるには、以下の手順を実行します。

AWS Resilience Hub レコメンデーションをコードベースに含めるには

1. [運用上の推奨事項] で [テンプレート] を選択します。
2. テンプレートのリストで、 AWS FIS 作成した実験テンプレートの名前を選択します。

   以下の情報を使用して、アプリケーションに実装されているテストを特定できます。

   - [テスト名] – アプリケーション用に作成したテストの名前。
   - [説明] – テストの目的を説明します。
   - [状態] – テストの現在の実装状態を示します。

この列には、次のいずれかの値が表示されます。

- [実装済み] – テストがアプリケーションに実装されていることを示します。
- [未実装] – テストがアプリケーションに実装されていないか、含まれていないことを示します。
- [除外] – テストがアプリケーションから除外されていることを示します。
- 非アクティブ — テストはデプロイされているが AWS FIS、過去 30 日間に実行されていないことを示します。

- [テスト実行] – 最新のテストの結果を含むドキュメントの Amazon S3 のURL。
- ソーステンプレート — AWS CloudFormation 実験の詳細を含むスタックの Amazon リソースネーム (ARN) を提供します。

3. [テンプレートの詳細] で、[テンプレート S3 パス] のリンクを選択し、Amazon S3 のコンソールでテンプレートオブジェクトを開きます。
4. Amazon S3 コンソールの [オブジェクト] テーブルで、テストフォルダのリンクを選択します。
5. Amazon S3 のパスをコピーするには、JSON ファイルの前にあるチェックボックスを選択し、[URL をコピー] を選択します。
6. AWS CloudFormation AWS CloudFormation コンソールからスタックを作成します。AWS CloudFormation スタックの作成について詳しくは、を参照してくださいhttps://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-console-create-stack.html。

   AWS CloudFormation スタックの作成時に、前のステップでコピーした Amazon S3 パスを指定する必要があります。

AWS FIS から実験を実行します。 AWS Resilience Hub

アプリケーションでは、 AWS FIS 実験を実行する前に AWS Resilience Hub 、 AWS FIS まず運用上の推奨事項から実験テンプレートを作成する必要があります。

AWS FIS 実験を開始するには

1. 左側のナビゲーションメニューで、[アプリケーション] を選択します。
2. [アプリケーション] テーブルから、アプリケーションを開きます。
3. [故障注入実験] タブを選択します。
4. [実験テンプレート] テーブルから実行する実験の作成に使用した実験テンプレートの前にあるラジオボタンを選択し、[実験を開始] を選択します。

AWS FIS 実験を中止するには

1. 左側のナビゲーションメニューで、[アプリケーション] を選択します。
2. [アプリケーション] テーブルから、アプリケーションを開きます。
3. [故障注入実験] タブを選択します。
4. 実験の前に [実験] テーブルからラジオボタンを選択し、[実験を停止] を選択します。

故障注入実験を表示する

で AWS Resilience Hub、 AWS リソースの耐障害性と、アプリケーション、インフラストラクチャ、アベイラビリティーゾーン、 AWS FIS インシデントからの回復にかかる時間を測定するために設定した実験を表示します。 AWS リージョン

AWS FIS ダッシュボードからテストを表示するには、左側のナビゲーションメニューから [Dashboard] を選択します。実験表では、 AWS FIS 以下の情報を使用して実施された実験を確認できます。

- [実験 ID] – AWS FIS の実験の識別子。
- 実験テンプレート ID — AWS FIS 実験の作成に使用された実験テンプレートの識別子。 AWS FIS
- ソーステンプレート — AWS CloudFormation AWS FIS 実験の詳細を含むスタックの Amazon リソースネーム (ARN) を提供します。
- 状態 — AWS FIS 実験が正常に完了したかどうかを示します。

AWS FIS 実装した実験をアプリケーションから表示するには

1. 左側のナビゲーションメニューで、[アプリケーション] を選択します。
2. [アプリケーション] テーブルから、アプリケーションを開きます。
3. [故障注入実験] を選択します。
4. 実験タブを選択します。

   Experiment タブでは、 AWS FIS Experiment テーブルにアクティブなテストのリストが表示されます。

   [実験] テーブルでは、以下の情報を使用して実施された AWS FIS の実験を確認できます。

   - テスト名 — AWS FIS 実験の作成に使用された AWS Resilience Hub 推奨テストの名前。

- [実験 ID] – AWS FIS の実験の識別子。
- 説明 — AWS FIS 実験の目的を説明します。
- [作成時間] – AWS FIS の実験が作成された日時。
- [最終更新日時] – AWS FIS の実験が最後に更新された日付と時刻。
- ソーステンプレート — AWS CloudFormation AWS FIS 実験の詳細を含むスタックの Amazon リソースネーム (ARN) を提供します。

評価から推奨された実験を確認するには

1. 左側のナビゲーションメニューで、[アプリケーション] を選択します。
2. [アプリケーション] テーブルからアプリケーションを選択します。

   アプリケーションを検索するには、[アプリケーションを検索] ボックスにアプリケーション名を入力します。
3. [評価] タブを選択します。

   [障害耐性評価] 表では、以下の情報を使用して評価を特定できます。

   - [名前] – 作成時に提供した評価の名前。
   - [ステータス] – 評価の実行状態を示します。
   - [コンプライアンスステータス] – 評価が障害耐性ポリシーに準拠しているかどうかを示します。
   - [障害耐性ドリフトステータス] – アプリケーションが前回の成功した評価から逸脱したかどうかを示します。
   - [アプリバージョン] – アプリケーションのバージョン。
   - [呼び出した人] – 評価を呼び出したロールを示します。
   - [開始時刻] – 評価の開始時刻を示します。
   - [終了時刻] – 評価の終了時刻を示します。
   - [ARN] - 評価の Amazon リソースネーム (ARN)。
4. [障害耐性評価] 表から評価を選択します。
5. [運用上の推奨事項] タブを選択します。
6. [故障注入実験] タブを選択します。

[フォールトインジェクション実験テンプレート] の表では、以下の情報を使用して推奨テストについて詳しく理解できます。

- [名前] – 推奨テストの名前。
- [説明] – テストの目的を説明します。
- [状態] – テストの現在の実装状態を示します。

  この列には、次のいずれかの値が表示されます。

  - [実装済み] – テストがアプリケーションに実装されていることを示します。
  - [未実装] – テストがアプリケーションに実装されていないか、含まれていないことを示します。
  - [除外] – テストがアプリケーションから除外されていることを示します。
  - Inactive — テストはデプロイされているが AWS FIS、過去 30 日間に実行されていないことを示します。
- [構成] – 対処する必要のある保留中の構成の依存関係があるかどうかを示します。
- [タイプ] – テストの種類を示します。
- AppComponent— このテストに関連するアプリケーションコンポーネント (AppComponents) を示します。サポート対象について詳しくは AppComponents、「リソースのグループ化」を参照してください。 AppComponent
- [リスク] – テスト失敗のリスクレベルを示します。「高」、「中」、「低」のリスクレベルは、それぞれ [高]、[中]、[低] で示されます。
- 参照 ID — AWS CloudFormation AWS CloudFormation内のスタックイベントの論理識別子を示します。
- レコメンデーション ID — AWS CloudFormation 内のスタックリソースの論理識別子を示します AWS CloudFormation。

Amazon Fault Injection Service の実験失敗/ステータスチェック

AWS Resilience Hub 開始したテストのステータスを追跡できます。詳細については、the section called “故障注入実験を表示する” の「推奨実験を評価から表示するには」の手順を参照してください。

トピック

- AWS Systems Manager AWS FIS を使用した実験実行の分析

- AWS FIS Amazon Elastic Kubernetes サービスクラスターで実行されている Kubernetes ポッドのテスト中に実験が失敗する

AWS Systems Manager AWS FIS を使用した実験実行の分析

AWS FIS 実験を実行すると、 AWS Systems Manager で実行の詳細を確認できます。

1. CloudTrail> [イベント履歴] に移動します。
2. 実験 ID を使用してユーザー名でイベントをフィルタリングします。
3. StartAutomationExecution エントリを表示します。リクエスト ID は SSM オートメーション ID です。
4. AWS システム・マネージャー > オートメーションに進みます。
5. SSM オートメーションID を使用して実行 ID でフィルタリングし、オートメーションの詳細を表示します。

   実行は、Systems Manager のどのオートメーションでも分析できます。詳細については、「ユーザーガイド」の「AWS Systems Manager Automation」を参照してください。実行入力パラメーターは実行詳細の「入力パラメーター」セクションに表示され、 AWS FIS 実験には表示されないオプションパラメーターも含まれています。

   実行ステップ内の特定のステップにドリルダウンすると、ステップステータスやその他のステップの詳細に関する情報が表示されます。

よくある失敗

評価レポートの実行中に発生する一般的な障害は次のとおりです。

- テスト/SOP 実験が実行される前に、アラームテンプレートがデプロイされませんでした。これにより、自動化ステップ中にエラーメッセージが表示されます。
  - 障害メッセージ: `The following parameters were not found: [/ResilienceHub/Alarm/3dee49a1-9877-452a-bb0c-a958479a8ef2/nat-gw-alarm-bytes-out-to-source-2020-09-21_nat-02ad9bc4fbd4e6135]. Make sure all the SSM parameters in automation document are created in SSM Parameter Store.`
  - 修正:フォールトインジェクション実験を再実行する前に、必ず関連するアラームをレンダリングし、結果のテンプレートをデプロイしてください。

- 実行ロールに権限がありません。このエラーメッセージは、指定した実行ロールに権限がない場合に発生し、ステップの詳細に表示されます。
  - 障害メッセージ: `An error occurred (Unauthorized Operation) when calling the DescribeInstanceStatus operation: You are not authorized to perform this operation. Please Refer to Automation Service Troubleshooting Guide for more diagnosis details。`
  - 修正: 正しい実行ロールを指定したことを確認してください。これが完了したら、必要な権限を追加して評価を再実行してください。
- 実行は成功しましたが、期待した結果にはなりませんでした。これは、パラメータが正しくないか、内部自動化の問題が原因です。
  - 失敗メッセージ: 実行に成功したため、エラーメッセージは表示されません。
  - 対策:Analyze AWS FIS 実験の実行で説明されているように、入力パラメーターを確認し、実行されたステップを確認してから、個々のステップで想定される入力と出力について調べます。

AWS FIS Amazon Elastic Kubernetes サービスクラスターで実行されている Kubernetes ポッドのテスト中に実験が失敗する

Amazon EKS クラスターで実行されている Kubernetes ポッドのテスト中に発生する Amazon Elastic Kubernetes Service (Amazon EKS) の障害は次のとおりです。

- AWS FIS 実験用の IAM ロールまたは Kubernetes サービスアカウントの設定が正しくない。
  - 障害メッセージ:
    - `Error resolving targets. Kubernetes API returned ApiException with error code 401.`
    - `Error resolving targets. Kubernetes API returned ApiException with error code 403.`
    - `Unable to inject AWS FIS Pod: Kubernetes API returned status code 403. Check Amazon EKS logs for more details.`
  - 修正: 以下を確認してください。
    - 「AWS FIS`aws:eks:pod`アクションを使用する」の指示に従っていることを確認してください。
    - 必要な RBAC 権限と正しい名前空間を持つ Kubernetes サービスアカウントを作成して設定したことを確認してください。

    - 提供された IAM ロール (AWS CloudFormation テストのスタックの出力を参照) を Kubernetes ユーザーにマッピングしたことを確認してください。
- AWS FIS Pod を起動できません:失敗したサイドカーコンテナの最大数に達しました。これは通常、 AWS FIS メモリがサイドカーコンテナを実行するのに十分でない場合に発生します。
    - 障害メッセージ: `Unable to heartbeat FIS Pod: Max failed sidecar containers reached`。
    - 修復: このエラーを回避する方法の 1 つは、使用可能なメモリまたは CPU に合わせて目標負荷率を下げることです。
- 実験の開始時にアラームアサーションが失敗しました。このエラーは、関連するアラームにデータポイントがないために発生します。
    - 障害メッセージ: `Assertion failed for the following alarms`。アサーションが失敗したすべてのアラームを一覧表示します。
    - 修復: Container Insights がアラーム用に正しくインストールされ、アラームがオンになっていない (`ALARM` の状態になっている) ことを確認します。

障害耐性スコアの理解

このセクションでは、 がさまざまな中断シナリオからのアプリケーションの準備状況を AWS Resilience Hub 定量化する方法について説明します。

AWS Resilience Hub は、アプリケーションの耐障害性体制を表す耐障害性スコアを提供します。このスコアは、アプリケーションがアプリケーションの障害耐性ポリシー、アラーム、標準作業手順書 (SOP)、テストを満たすための推奨事項にどの程度準拠しているかを反映します。アプリケーションが使用するリソースのタイプに基づいて、 はアラーム、SOPs、および中断タイプごとに一連のテスト AWS Resilience Hub を推奨します。

障害耐性の最高スコアは 100 ポイントです。最高のスコアまたは最高得点を達成するには、推奨されているアラーム、SOP、テストをすべてアプリケーションに実装する必要があります。例えば、 は 1 つのアラームと 1 つの TAK を含む 1 つのテスト AWS Resilience Hub を推奨します。テストを実行してアラームを起動し、関連する SOP を開始します。テストが正常に実行され、アプリケーションがレジリエンスポリシーを満たしていれば、100 ポイントに近い障害耐性スコアが与えられます。

最初の評価を実行した後、 は、運用上の推奨事項をアプリケーションから除外するオプション AWS Resilience Hub を提供します。除外された推奨事項が障害耐性スコアに与える影響を理解するには、新しい評価を実施する必要があります。ただし、除外された推奨事項をアプリケーションに含めて、

新しい評価を実行することはいつでも可能です。アラーム、SOP、テストの推奨事項を含めたり除外したりする方法の詳細については、the section called “運用上の推奨事項を含めるまたは除外する”を参照してください。

アプリケーションの障害耐性スコアへのアクセス

ナビゲーションメニューから [ダッシュボード] または [アプリケーション] を選択すると、アプリケーションの障害耐性スコアを表示できます。

ダッシュボードから障害耐性スコアにアクセスする

1. 左側のナビゲーションメニューで、[ダッシュボード] を選択します。
2. 時間の経過に伴うアプリケーションの障害耐性スコアで、最大 4 つのアプリケーションを選択ドロップダウンリストから 1 つ以上のアプリケーションを選択します。
3. [障害耐性スコア] チャートには、選択したすべてのアプリケーションの障害耐性スコアが表示されます。

アプリケーションから障害耐性スコアへのアクセス

1. 左側のナビゲーションメニューで、[アプリケーション] を選択します。
2. [アプリケーション] で、アプリケーションを選択します。
3. 概要を選択します。

   耐障害性スコアチャートには、アプリケーションの耐障害性スコアの傾向が最大 1 年間表示されます。 AWS Resilience Hub には、以下を使用して最大限の耐障害性スコアを改善および達成するために対処する必要があるアクション項目、耐障害性ポリシー違反、および運用上の推奨事項が表示されます。

   - 障害耐性スコアを可能な限り高め、達成するために完了する必要のあるアクションアイテムを確認するには、[アクションアイテム] タブを選択します。選択すると、以下 AWS Resilience Hub が表示されます。
     - [RTO/RPO] — アプリケーションの障害耐性ポリシーの違反を解決するために修正する必要がある復旧時間 (RTO/RPO) の数を示します。値を選択すると、アプリケーションの評価レポートに RTO/RPO の詳細が表示されます。
     - アラーム – アプリケーションに実装する必要がある推奨 Amazon CloudWatch アラームの数を示します。値を選択すると、アプリケーションの評価レポートで修正する必要がある Amazon CloudWatch アラームが表示されます。

- [SOP] — アプリケーションに実装する必要がある推奨 SOP の数を示します。値を選択すると、修正が必要な SOP がアプリケーションの評価レポートに表示されます。
- [FIS] — アプリケーションに実装する必要のある推奨テストの数を示します。値を選択すると、修正が必要なテストがアプリケーションの評価レポートに表示されます。

- 障害耐性スコアに影響する各コンポーネントのスコアを表示するには、[スコアの詳細] を選択します。選択すると、 AWS Resilience Hub には次の内容が表示されます。
  - RTO/RPO コンプライアンス — アプリケーションコンポーネント (AppComponents) が推定ワークロード回復時間と、アプリケーションの回復力ポリシーで定義されている目標復旧時間にどのように準拠しているかを示します。値を選択すると、アプリケーションの評価レポートに RTO/RPO の推定が表示されます。
  - 実装されたアラーム — 実装された Amazon CloudWatch アラームの実際の寄与度と、アプリケーションの耐障害性スコアに対する最大寄与率を比較したことを示します。値を選択すると、実装された Amazon CloudWatch アラームがアプリケーションの評価レポートに表示されます。
  - [実装済み SOP] — 実装された SOP の実際の寄与度を、アプリケーションの障害耐性スコアに対する最大貢献度と比較したものです。値を選択すると、実装された SOP がアプリケーションの評価レポートに表示されます。
  - [実施された FIS 実験] – 実装されたテストの実際の寄与度をアプリケーションの障害耐性スコアに対する最大寄与度と比較したものです。値を選択すると、実装されたテストがアプリケーションの評価レポートに表示されます。
- 障害耐性ポリシー違反と運用上の推奨事項を表示するには、右矢印を選択して [ポリシー違反と運用上の推奨事項] セクションを展開します。展開すると、以下 AWS Resilience Hub が表示されます。
  - [障害耐性ポリシー違反] — アプリケーションの障害耐性ポリシーに違反しているアプリケーションコンポーネントの数を示します。[RTO/RPO] の横にある値を選択すると、アプリケーションの評価レポートの [障害耐性に関する推奨事項] タブに詳細が表示されます。
  - [運用上の推奨事項] — [未処理] タブと [除外] タブを使用して、アプリケーションの障害耐性を高めるために実装または実行されていない運用上の推奨事項を示します。運用上の推奨事項には、使用されていない推奨事項と実装されていない推奨事項がすべて含まれます。

    実装が必要な運用上の推奨事項を確認するには、[未処理] タブを選択します。選択すると、以下 AWS Resilience Hub が表示されます。
    - アラーム – 実装する必要がある推奨 Amazon CloudWatch アラームの数を示します。
    - [SOP] — 実装する必要のある推奨 SOP の数を示します。

- [FIS] — 実施する必要のある推奨テストの数を示します。

アプリケーションから除外されている運用上の推奨事項を表示するには、[除外] タブを選択します。選択すると、以下 AWS Resilience Hub が表示されます。

- アラーム – アプリケーションから除外されている推奨 Amazon CloudWatch アラームの数を示します。
- [SOP] — アプリケーションから除外されている推奨 SOP の数を示します。
- [FIS] — アプリケーションから除外されている推奨テストの数を示します。

障害耐性スコアの計算

このセクションの表では、各レコメンデーションタイプのスコアリングコンポーネントとアプリケーションの耐障害性スコアを決定する AWS Resilience Hub ために で使用される式について説明します。各レコメンデーションタイプのスコアリングコンポーネントとアプリケーションの耐障害性スコア AWS Resilience Hub について によって決定された結果の値はすべて、最も近いポイントに丸められます。例えば、3 つのアラームのうち 2 つを実装した場合、スコアは 13.33 ((2/3) * 20) ポイントになります。この値は 13 ポイントに四捨五入されます。表内の計算式に使われているウェイトの詳細については、the section called “ AppComponents および 中断タイプの重み” セクションを参照してください。

一部のスコアリングコンポーネントは `ScoringComponentResiliencyScore` API を通じてのみ取得できます。この API の詳細については、「ScoringComponentResiliencyScore」を参照してください。

テーブル

- 各推奨タイプのスコアリングコンポーネントを計算する式
- 障害耐性スコアの計算式
- AppComponents および 中断タイプの回復性スコアを計算するための計算式

次の表は、各レコメンデーションタイプのスコアリングコンポーネントを計算する AWS Resilience Hub ために が使用する式について説明しています。

各推奨タイプのスコアリングコンポーネントを計算する式

スコアリングコンポーネント	説明	計算式	例
テストカバレッジ (T)	AWS Resilience Hub 推奨テストの総数のうち、正常に実装されたテストと除外されたテストの数に基づいて標準化されたスコア (0 ~ 100 ポイント)。 **Note** 回復性スコアを計算するには、がそれを実装済みと見なす AWS Resilience Hub ために、過去 30 日間に推奨テストが正常に実行されている必要があります。	`T = ((Total number of tests implemented) + (Total number of tests excluded)) / (Total number of tests recommended)` 計算式の一部は次のとおりです。 • 設定されたテストの合計数 — AWS CloudFormation テンプレートが作成およびアップロードされたときに設定されたテストの合計数を示します AWS CloudFormation 。 • 推奨されるテストの合計数 — アプリケーションリソース AWS Resilience Hub に基づいて、 によって推奨されるテストを示します。 • [除外されたテストの総数] — アプリケーションから除外された推奨テストの数を示します。	20 件の AWS Resilience Hub 推奨テストのうち 10 件を実装し、5 件を除外した場合、テストカバレッジは次のように計算されます。 `T = (10 + 5) / 20` つまり、`T = .75 or 75 points`
アラームカバレッジ (A)	AWS Resilience Hub 推奨される Amazon CloudWatch アラームの合計数のう	`A = ((Total number of alarms implemented) + (Total number`	20 個の AWS Resilience Hub 推奨 Amazon

スコアリングコンポーネント	説明	計算式	例
	ち、正常に実装され、除外された Amazon CloudWatch アラームの数に基づく正規化されたスコア (0 ~ 100 ポイント) 。 **Note** 障害耐性スコアを計算するには、AWS Resilience Hub が実装済みとみなせるように、推奨アラームが準備完了状態になっている必要があります。	`of alarms excluded) ) / (Total number of alarms recommended)` 計算式の一部は次のとおりです。 • 設定されたアラームの合計数 – AWS CloudFormation テンプレートの作成およびアップロード時に設定された Amazon CloudWatch アラームの合計数を AWS CloudFormation コンソールで示します。 • 推奨されるアラームの合計数 — アプリケーションリソース AWS Resilience Hub に基づいて、 によって推奨される Amazon CloudWatch アラームを示します。 • 除外されたアラームの合計数 — アプリケーションから除外した推奨 Amazon CloudWatch アラームの数を示します。	CloudWatch アラームのうち、10 個と除外された 5 個の Amazon CloudWatch アラームを実装した場合、Amazon CloudWatch アラームのカバレッジは次のように計算されます。 `A = (10 + 5) / 20` つまり、`A = .75 or 75 points`

スコアリングコンポーネント	説明	計算式	例
SOP カバレッジ (S)	AWS Resilience Hub が推奨する SOP の総数のうち、正常に実装されたものと除外された SOP の数に基づく標準化されたスコア (0 ~ 100 ポイント)。	`S = ((Total number of SOPs implemented) + (Total number of SOPs excluded)) / (Total number of SOPs recommended)` 計算式の一部は次のとおりです。 • 設定された SOPs の合計数 – AWS CloudFormation テンプレートが作成されて AWS CloudFormation コンソールにアップロードされたときに設定された SOPsの合計数を示します。 • 推奨される SOPs の合計数 — アプリケーションリソース AWS Resilience Hub に基づいて、 が推奨する SOPs を示します。 • [除外された SOP の総数] — アプリケーションから除外した推奨 SOP の数を示します。	20 個の AWS Resilience Hub 推奨 SOP のうち 10 個の SOP を実装し、5 個の SOP を除外した場合、SOP カバレッジは次のように計算されます。 `S = (10 + 5) / 20` つまり、`S = .75 or 75 points`

スコアリングコンポーネント	説明	計算式	例

RTO/RPO コンプライアンス (P)	アプリケーションが障害耐性ポリシーを満たしていることに基づく標準化されたスコア (0 ~ 100 ポイント)。	`P = Total weights of disruption types meeting the application's resiliency policy / Total weights of all disruption types .`	アプリケーションの障害耐性ポリシーがアベイラビリティーゾーン (AZ) とインフラストラクチャの中断タイプのみを満たす場合、障害耐性ポリシースコア (P) は次のように計算されます。
			• リージョナル RTO と RPO の目標を設定している場合、P は次のように計算されます。
			`P = (20 + 30)/ 100`
			つまり、`P = .5 or 50 points`
			• リージョナル RTO と RPO の目標を設定していない場合は、P のように計算されます。
			`P = (22.22 + 33.33)/ 99.9`

スコアリングコンポーネント	説明	計算式	例
			つまり、P = .55 or 55 points

次の表は、アプリケーション全体の耐障害性スコアを計算する AWS Resilience Hub ために が使用する式を示しています。

障害耐性スコアの計算式

スコアリングコンポーネント	説明	計算式	例
アプリケーションの障害耐性スコア (RS)	アプリケーションがその障害耐性ポリシーを満たしていることに基づく、標準化された障害耐性スコア (0 ~ 100 ポイント)。アプリケーションごとの障害耐性スコアは、すべての推奨タイプの加重平均です。つまり: RS = Weighted Average (T, A, S, P)	アプリケーションごとの障害耐性スコアは、次の式を使用して計算されます: RS = (T * Weight(T) + A * Weight(A) + S * Weight(S) + P * Weight(P)) / (Weight(T) + Weight(A) + Weight(S) + Weight(P))	各推奨タイプ表の対象範囲を計算する式は次のとおりです。 • Test coverage (T) = .75 • Alarms (A) = .75 • SOPs (S) = .75 • Meeting resiliency policy (P) = .5 アプリケーションごとの障害耐性ス

スコアリングコンポーネント	説明	計算式	例
			コアは次のように計算されます。 `RS = ((.75 * .2) + (.75 * .2) + (.75 * .2) + (.5 * .4)) /(.2 + .2 + .2 + .4)` つまり、`RS = .65 or 65 points`

次の表は、アプリケーションコンポーネント (AppComponents) と中断タイプの回復性スコアを計算する AWS Resilience Hub ために で使用される式を示しています。ただし、 AppComponents および 中断タイプの回復性スコアは、次の AWS Resilience Hub APIs を介してのみ取得できます。

- DescribeAppAssessment を取得するための RSo
- ListAppComponentCompliances RSaoと を取得するための RSA

AppComponents および 中断タイプの回復性スコアを計算するための計算式

スコアリングコンポーネント	説明	計算式	例

AppComponent 中断タイプごとの耐障害性スコア (RSao)	中断タイプごとの回復カポリシー AppComponent を満たすことに基づく正	AppComponent 中断タイプごとの回復性スコアは、次の式を使用して計算されます。
		
		`RSao = (T * Weight(T) +`
		
		`A * Weight(A) +`
			すべての推奨タイプの RSao の前提条件は次のとおりです。
			
			• `Test coverage (T) = .75`

スコアリングコンポーネント	説明	計算式	例
	規化されたスコア (0～100 ポイント) 。中断タイプ AppComponent ごとの耐障害性スコアは、すべてのレコメンデーションタイプの加重平均です。 つまり: RSao = Weighted Average (T, A, S, P) の値は、 および AppComponent 中断タイプの推奨テスト、アラーム、SOPs、会議耐障害性ポリシーすべてに対してT, A, S, P計算されます。	S * Weight(S) + P * Weight(P)) / (Weight(T) + Weight(A) + Weight(S) + Weight(P))	• Alarms (A) = .75 • SOPs (S) = .75 • Meeting resiliency policy (P) = .5 AppComponent および中断タイプごとの回復性スコアは、次のように計算されます。 RSao = ((.75 * .2) + (.75 * .2) + (.75 * .2) + (.5 * .4)) / (.2 + .2 + .2 + .4) つまり、RSao = .65 or 65 points

スコアリングコンポーネント	説明	計算式	例
あたりの耐障害性スコア AppComponent（RSa）	障害耐性ポリシーを満たしていることに基づく標準化されたスコア (0 ~ 100 ポイント)。あたりの回復性スコア AppComponent は、すべてのレコメンデーションタイプの加重平均です。つまり: RSa = Weighted Average（T, A, S, P） の値は、 のすべての推奨テスト、アラーム、SOPs、会議耐障害性ポリシーに対してT, A, S, P計算されます AppComponent。	ごとの回復性スコア AppComponent は、次の式を使用して計算されます。 RSa = (T * Weight(T) + A * Weight(A) + S * Weight(S) + P * Weight(P)) / (Weight(T) + Weight(A) + Weight(S) + Weight(P))	すべての推奨タイプの RSa の前提条件は次のとおりです。 • Test coverage (T) = .75 • Alarms (A) = .75 • SOPs (S) = .75 • Meeting resiliency policy (P) = .5 あたりの回復性スコア AppComponent は次のように計算されます。 RSa = ((.75 * .2) + (.75 * .2) + (.75 * .2) + (.5 * .4)) / (.2 + .2 + .2 + .4) つまり、RSa = .65 or 65 points

スコアリングコンポーネント	説明	計算式	例
中断タイプごとの障害耐性スコア (RSo)	障害耐性ポリシーを満たしていることに基づく標準化されたスコア (0 ~ 100 ポイント)。中断タイプごとの障害耐性スコアは、すべての推奨タイプの加重平均です。つまり: RSo = Weighted Average (T, A, S, P) T, A, S, P の値は、すべての推奨テスト、アラーム、SOP、および中断タイプの障害耐性ポリシーを満たすために計算されたものです。	中断タイプごとの障害耐性スコアは、次の式を使用して計算されます。 RSo = (T * Weight(T) + A * Weight(A) + S * Weight(S) + P * Weight(P)) / (Weight(T) + Weight(A) + Weight(S) + Weight(P))	すべての推奨タイプの RSo の前提条件は次のとおりです。 • Test coverage (T) = .75 • Alarms (A) = .75 • SOPs (S) = .75 • Meeting resiliency policy (P) = .5 中断タイプごとの障害耐性スコアは、次のように計算されます。 RSo = ((.75 * .2) + (.75 * .2) + (.75 * .2) + (.5 *.4)) / (.2 + .2 + .2 + .4) つまり、RSo = .65 or 65 points

重量

AWS Resilience Hub は、総回復性スコアの各レコメンデーションタイプに重みを割り当てます。

次の表は、アラーム、SOPs、会議耐障害性ポリシー、および中断タイプの重みを示しています。中断タイプには、アプリケーション、インフラストラクチャ、AZ、リージョンが含まれます。

> **Note**
>
> 保険契約でリージョナル RTO または RPO 目標を定義しないことを選択した場合、リージョンが定義されていない場合のウェイト例に示されているように、他の中断タイプのウェイトもそれに応じて増加します。

アラーム、SOP、テスト、ポリシーターゲットのウェイト

推奨事項の種類	(重量)
アラーム	20 ポイント
SOP	20 ポイント
テスト	20 ポイント
障害耐性ポリシーを満たす	40 ポイント

中断タイプ別のウェイト

中断タイプ	リージョンが定義された場合のウェイト	リージョンが定義されていない場合のウェイト
アプリケーション	40 ポイント	44.44 ポイント
インフラストラクチャ	30 ポイント	33.33 ポイント
アベイラビリティーゾーン	20 ポイント	22.22 ポイント
リージョン	10 ポイント	該当なし

AWS CloudFormation を使用して、運用上の推奨事項をアプリケーションに統合します

運用上の推奨事項ページで CloudFormation テンプレートの作成 を選択した後、AWS Resilience Hub は、アプリケーションの特定のアラーム、標準運用手順 (SOP)、または AWS FIS の実験を説明する AWS CloudFormation のテンプレートを作成します。AWS CloudFormation のテンプレートは Amazon S3 バケットに保存され、「運用上の推奨事項」ページの テンプレートの詳細 タブでテンプレートへの S3 パスを確認できます。

たとえば、以下のリストは JSON 形式の AWS CloudFormation のテンプレートを示しています。このテンプレートには、AWS Resilience Hub によってレンダリングされるアラーム推奨が記述されています。`Employees` という名前の DynamoDB テーブルの読み取りスロットリングアラームです。

テンプレートの `Resources` セクションでは、DynamoDB テーブルの読み取りスロットルイベントの数が 1 を超えたときにアクティブになる `AWS::CloudWatch::Alarm` のアラームについて説明しています。また、この 2 つの `AWS::SSM::Parameter` リソースは、実際のアプリケーションをスキャンしなくても AWS Resilience Hub がインストールされているリソースを識別できるようにするメタデータを定義します。

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

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

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

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

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

テンプレートの変更 AWS CloudFormation

アラーム、SOP、または AWS FIS リソースをメインアプリケーションに統合する最も簡単な方法は、アプリケーションテンプレートを記述するテンプレートに別のリソースとして追加することです。以下に示す JSON 形式のファイルは、DynamoDB テーブルが AWS CloudFormation のテンプレートでどのように記述されるかの基本的な概要を示しています。実際のアプリケーションには、追加のテーブルなど、さらにいくつかのリソースが含まれる可能性があります。

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

アラームリソースをアプリケーションとともにデプロイできるようにするには、ハードコーディングされたリソースをアプリケーションスタックの動的参照に置き換える必要があります。

そこで、AWS::CloudWatch::Alarm のリソース定義で以下を変更してください。

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

以下へ:

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

そこで、AWS::SSM::Parameter のリソース定義で以下を変更してください。

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

以下へ:

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

SOP や AWS FIS の実験用に AWS CloudFormation のテンプレートを変更する場合も、ハードコーディングされた参照 ID を、ハードウェアが変更されても動作し続ける動的参照に置き換えるという同じアプローチを取ります。

DynamoDB テーブルへの参照を使用することで、AWS CloudFormation によって次のことが可能になります。

- まず、データベーステーブルを作成します。
- 生成されたリソースの実際の ID を必ずアラームに使用し、AWS CloudFormation がリソースの交換を必要とする場合はアラームを動的に更新してください。

> **Note**
>
> スタックをネストしたり、別の AWS CloudFormation スタックにあるリソース出力を参照したりするなど、AWS CloudFormation を使用したアプリケーションリソースの管理にはより高度な方法を選択できます。(ただし、レコメンデーションスタックをメインスタックとは別にしておきたい場合は、2 つのスタック間で情報を渡す方法を設定する必要があります)。さらに、HashiCorp の Terraform などのサードパーティツールを使用して、Infrastructure as Code (IaC) をプロビジョニングすることもできます。

AWS Resilience HubAPI によるアプリケーションの記述と管理

AWS Resilience Hubコンソールを使用してアプリケーションを記述および管理する代わりに、AWS Resilience Hub ではAWS Resilience HubAPI を使用してアプリケーションを記述および管理できます。この章では、AWS Resilience Hub API を使用してアプリケーションを作成する方法について説明します。また、API を実行する順序や、適切な例とともに提供する必要があるパラメータ値についても定義しています。詳細については、次のトピックを参照してください。

- the section called “アプリケーションの準備”
- the section called “アプリケーションの実行と分析”
- the section called “アプリケーションの修正”

ステップ 1: アプリケーションの準備

アプリケーションを準備するには、まずアプリケーションを作成し、回復力ポリシーを割り当ててから、入力ソースからアプリケーションリソースをインポートする必要があります。アプリケーションの準備に使用される AWS Resilience Hub API の詳細については、次のトピックを参照してください。

- the section called “アプリケーションの作成”
- the section called “回復力ポリシーを作成します”
- the section called “アプリケーションリソースのインポートとインポートステータスの監視”
- the section called “アプリケーションの発行と回復力ポリシーの割り当て”

アプリケーションを作成する

AWS Resilience Hubで新しいアプリケーションを作成するには、`CreateApp`API を呼び出して一意のアプリケーション名を指定する必要があります。この API の詳細については、「https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_CreateApp.html」を参照してください。

次の例では、AWS Resilience Hub`CreateApp` API を使用して新しいアプリケーションnewAppを作成する方法を示しています。

リクエスト

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

レスポンス

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

回復力ポリシーの作成

アプリケーションを作成したら、CreateResiliencyPolicyAPI を使用してアプリケーションの回復力を把握できるようにする回復力ポリシーを作成する必要があります。この API の詳細については、「https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_CreateResiliencyPolicy.html」を参照してください。

次の例では、CreateResiliencyPolicyAPI を使用してAWS Resilience HubでアプリケーションのnewPolicyを作成する方法を示しています。

リクエスト

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

レスポンス

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

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

入力ソースからのリソースのインポートとインポートステータスの監視

AWS Resilience Hubには、リソースをアプリケーションにインポートするための次の API が用意されています。

- `ImportResourcesToDraftAppVersion`— この API を使用すると、さまざまな入力ソースからアプリケーションのドラフトバージョンにリソースをインポートできます。この API の詳細については、「https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_ImportResourcesToDraftAppVersion.html」を参照してください。
- `PublishAppVersion`— この API は、更新された AppComponents と共にアプリケーションの新しいバージョンを発行します。この API の詳細については、「https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_PublishAppVersion.html」を参照してください。
- `DescribeDraftAppVersionResourcesImportStatus`— この API を使用すると、リソースのアプリケーションバージョンへのインポートステータスを監視できます。この API の詳細については、「https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_DescribeDraftAppVersionResourcesImportStatus.html」を参照してください。

次の例では、ImportResourcesToDraftAppVersionAPI を使用してリソースをAWS Resilience Hubのアプリケーションにインポートする方法を示しています。

リクエスト

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

レスポンス

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

次の例は、CreateAppVersionResourceAPI を使用してAWS Resilience Hubのアプリケーションにリソースを手動で追加する方法を示しています。

リクエスト

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

レスポンス

```
{
    "appArn": "<App_ARN>",
```

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

次の例では、AWS Resilience HubでDescribeDraftAppVersionResourcesImportStatusAPIを使用して、リソースのインポートステータスを監視する方法を示しています。

リクエスト

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

レスポンス

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

アプリケーションのドラフトバージョンの発行と回復力ポリシーの割り当て

評価を実行する前に、まずアプリケーションのドラフトバージョンを発行し、リリースされたバージョンのアプリケーションに回復力ポリシーを割り当てる必要があります。

アプリケーションのドラフトバージョンを発行し、回復力ポリシーを割り当てるには

1. アプリケーションのドラフトバージョンを発行するには PublishAppVersion API を使用します。この API の詳細については、「https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_PublishAppVersion.html」を参照してください。

   次の例では、PublishAppVersion APIを使用してAWS Resilience Hubのアプリケーションのドラフトバージョンを発行する方法を示しています。

   リクエスト

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

   レスポンス

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

2. UpdateAppAPI を使用して、リリースされたバージョンのアプリケーションに回復力ポリシーを適用します。この API の詳細については、「https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_UpdateApp.html」を参照してください。

   次の例では、UpdateApp APIを使用してAWS Resilience Hubのアプリケーションのリリース済みバージョンに回復力ポリシーを適用する方法を示しています。

   リクエスト

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

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

レスポンス

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

ステップ 2: AWS Resilience Hub 回復力評価の実行と管理

アプリケーションの新しいバージョンを発行したら、新しい回復力評価を実行し、結果を分析して、アプリケーションが回復力ポリシーで定義されている推定ワークロード RTO と推定 RPO を満たしていることを確認する必要があります。評価では、各アプリケーションコンポーネントの設定をポリシーと比較し、アラーム、SOP、テストの推奨事項を作成します。

詳細については、次のトピックを参照してください。

- the section called “回復力評価の実行と監視”
- the section called “回復力ポリシーの作成”

AWS Resilience Hub 回復力評価の実行と監視

AWS Resilience Hubで回復力評価を実行し、そのステータスを監視するには、次の API を使用する必要があります。

- `StartAppAssessment`— この API はアプリケーションの新しい評価を作成します。この API の詳細については、「https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_StartAppAssessment.html」を参照してください。
- `DescribeAppAssessment`— この API は、アプリケーションの評価について説明し、評価の完了ステータスを提供します。この API の詳細については、「https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_DescribeAppAssessment.html」を参照してください。

次の例では、`StartAppAssessment` APIを使用して AWS Resilience Hub で新しい評価の実行を開始する方法を示します。

リクエスト

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

レスポンス

```
{
    "assessment": {
        "appArn": "<App_ARN>",
        "appVersion": "release",
        "invoker": "User",
        "assessmentStatus": "Pending",
        "startTime": "2022-10-27T08:15:10.452000+03:00",
        "assessmentName": "first-assessment",
        "assessmentArn": "<Assessment_ARN>",
        "policy": {
            "policyArn": "<Policy_ARN>",
            "policyName": "newPolicy",
            "dataLocationConstraint": "AnyLocation",
            "policy": {
                "AZ": {
                    "rtoInSecs": 172800,
                    "rpoInSecs": 86400
                },
                "Hardware": {
                    "rtoInSecs": 172800,
                    "rpoInSecs": 86400
                },
```

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

次の例では、DescribeAppAssessment APIを使用して AWS Resilience Hub で評価のステータスを監視する方法を示しています。assessmentStatus変数から評価のステータスを抽出できます。

リクエスト

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

レスポンス

```
{
    "assessment": {
        "appArn": "<App_ARN>",
        "appVersion": "release",
        "cost": {
            "amount": 0.0,
            "currency": "USD",
            "frequency": "Monthly"
        },
        "resiliencyScore": {
            "score": 0.27,
            "disruptionScore": {
                "AZ": 0.42,
                "Hardware": 0.0,
                "Region": 0.0,
                "Software": 0.38
            }
        },
        "compliance": {
            "AZ": {
                "achievableRtoInSecs": 0,
                "currentRtoInSecs": 4500,
```

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

```
        "tags": {}
    }
}
```

評価結果の確認

評価が正常に完了したら、次の API を使用して評価結果を調べることができます。

- `DescribeAppAssessment`— この API では、回復力ポリシーと照らし合わせてアプリケーションの現在のステータスを追跡することができます。さらに、`complianceStatus`変数からコンプライアンスステータスを抽出したり、`resiliencyScore`構造から各中断タイプの回復力スコアを抽出したりすることもできます。この API の詳細については、「https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_DescribeAppAssessment.html」を参照してください。
- `ListAlarmRecommendations`— この API では、評価の Amazon リソースネーム (ARN) を使用してアラームの推奨事項を取得することができます。この API の詳細については、「https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_ListAlarmRecommendations.html」を参照してください。

> **Note**
>
> SOP と FIS テストの推奨事項を取得するには、`ListSopRecommendations`と`ListTestRecommendations`API を使用してください。

次の例では、`ListAlarmRecommendations` API を使用して評価の Amazon リソースネーム (ARN) を使用してアラームレコメンデーションの取得方法を示します。

> **Note**
>
> SOP と FIS テストの推奨事項を取得するには、`ListSopRecommendations`または`ListTestRecommendations`に置き換えてください。

リクエスト

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

レスポンス


```
{
    "alarmRecommendations": [
        {
            "recommendationId": "78ece7f8-c776-499e-baa8-b35f5e8b8ba2",
            "referenceId": "app_common:alarm:synthetic_canary:2021-04-01",
            "name": "AWSResilienceHub-SyntheticCanaryInRegionAlarm_2021-04-01",
            "description": "A monitor for the entire application, configured to
 constantly verify that the application API/endpoints are available",
            "type": "Metric",
            "appComponentName": "appcommon",
            "items": [
                {
                    "resourceId": "us-west-2",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ],
            "prerequisite": "Make sure CloudWatch Synthetics is setup to monitor the
 application (see the <a href=\"https://docs.aws.amazon.com/AmazonCloudWatch/latest/
monitoring/CloudWatch_Synthetics_Canaries.html\" target=\"_blank\">docs</a>). \nMake
 sure that the Synthetics Name passed in the alarm dimension matches the name of the
 Synthetic Canary. It Defaults to the name of the application.\n"
        },
        {
            "recommendationId": "d9c72c58-8c00-43f0-ad5d-0c6e5332b84b",
            "referenceId": "efs:alarm:percent_io_limit:2020-04-01",
            "name": "AWSResilienceHub-EFSHighIoAlarm_2020-04-01",
            "description": "Alarm by AWS ResilienceHub that reports when EFS I/O load
 is more than 90% for too much time",
            "type": "Metric",
            "appComponentName": "storageappcomponent-rlb",
            "items": [
                {
                    "resourceId": "fs-0487f945c02f17b3e",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ]
        },
```

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

```
            "recommendationId": "15f49b10-9bac-4494-b376-705f8da252d7",
            "referenceId": "rds:alarm:health-storage:2020-04-01",
            "name": "AWSResilienceHub-RDSInstanceLowStorageAlarm_2020-04-01",
            "description": "Reports when database free storage is low",
            "type": "Metric",
            "appComponentName": "databaseappcomponent-hji",
            "items": [
                {
                    "resourceId": "terraform-20220623141426115800000001",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ]
        },
        {
            "recommendationId": "c1906101-cea8-4f77-be7b-60abb07621f5",
            "referenceId": "rds:alarm:health-connections:2020-04-01",
            "name": "AWSResilienceHub-RDSInstanceConnectionSpikeAlarm_2020-04-01",
            "description": "Reports when database connection count is anomalous",
            "type": "Metric",
            "appComponentName": "databaseappcomponent-hji",
            "items": [
                {
                    "resourceId": "terraform-20220623141426115800000001",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ]
        },
        {
            "recommendationId": "f169b8d4-45c1-4238-95d1-ecdd8d5153fe",
            "referenceId": "rds:alarm:health-cpu:2020-04-01",
            "name": "AWSResilienceHub-RDSInstanceOverUtilizedCpuAlarm_2020-04-01",
            "description": "Reports when database used CPU is high",
            "type": "Metric",
            "appComponentName": "databaseappcomponent-hji",
            "items": [
                {
                    "resourceId": "terraform-20220623141426115800000001",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
```

```
                }
            ]
        },
        {
            "recommendationId": "69da8459-cbe4-4ba1-a476-80c7ebf096f0",
            "referenceId": "rds:alarm:health-memory:2020-04-01",
            "name": "AWSResilienceHub-RDSInstanceLowMemoryAlarm_2020-04-01",
            "description": "Reports when database free memory is low",
            "type": "Metric",
            "appComponentName": "databaseappcomponent-hji",
            "items": [
                {
                    "resourceId": "terraform-20220623141426115800000001",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ]
        },
        {
            "recommendationId": "67e7902a-f658-439e-916b-251a57b97c8a",
            "referenceId": "ecs:alarm:health-service_cpu_utilization:2020-04-01",
            "name": "AWSResilienceHub-ECSServiceHighCpuUtilizationAlarm_2020-04-01",
            "description": "Alarm by AWS ResilienceHub that triggers when CPU
utilization of ECS tasks of Service exceeds the threshold",
            "type": "Metric",
            "appComponentName": "computeappcomponent-nrz",
            "items": [
                {
                    "resourceId": "aws_ecs_service_terraform-us-east-1-demo",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ]
        },
        {
            "recommendationId": "fb30cb91-1f09-4abd-bd2e-9e8ee8550eb0",
            "referenceId": "ecs:alarm:health-service_memory_utilization:2020-04-01",
            "name": "AWSResilienceHub-ECSServiceHighMemoryUtilizationAlarm_2020-04-01",
            "description": "Alarm by AWS ResilienceHub for Amazon ECS that indicates if
the percentage of memory that is used in the service, is exceeding specified threshold
limit",
            "type": "Metric",
```

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

次の例では、ListAppComponentRecommendations API を使用して推奨構成「現在の回復力を向上させるための推奨事項」を取得する方法を示しています。

リクエスト

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

レスポンス


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

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

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

```
                    "description": "Stateful ECS service with launch type EC2 and EFS
storage, deployed in multiple AZs. AWS Backup is used to backup EFS and copy snapshots
in-region.",
                    "suggestedChanges": [
                        "Add Auto Scaling Groups and Capacity Providers in multiple
AZs",
                        "Change desired count of the setup",
                        "Remove EBS volume"
                    ],
                    "haArchitecture": "BackupAndRestore",
                    "referenceId": "ecs:config:ec2-multi_az-efs-backups:2022-02-16"
                }
            ]
        },
        {
            "appComponentName": "databaseappcomponent-hji",
            "recommendationStatus": "MetCanImprove",
            "configRecommendations": [
                {
                    "cost": {
                        "amount": 0.0,
                        "currency": "USD",
                        "frequency": "Monthly"
                    },
                    "appComponentName": "databaseappcomponent-hji",
                    "recommendationCompliance": {
                        "AZ": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": "Estimated time to restore from
an RDS backup. (Estimates are averages based on size, real time may vary greatly from
estimate).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Estimate based on the backup
schedule. (Estimates are calculated from backup schedule, real time restore may
vary)."
                        },
                        "Hardware": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": "Estimated time to restore from
snapshot. (Estimates are averages based on size, real time may vary greatly from
estimate).",
                            "expectedRpoInSecs": 86400,
```

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

```
                            "expectedRtoDescription": "Estimated time to restore from
snapshot. (Estimates are averages based on size, real time may vary greatly from
estimate).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Estimate based on the backup
schedule. (Estimates are calculated from backup schedule, real time restore may
vary)."
                        },
                        "Software": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": "Estimated time to restore from
snapshot. (Estimates are averages based on size, real time may vary greatly from
estimate).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Estimate based on the backup
schedule. (Estimates are calculated from backup schedule, real time restore may
vary)."
                        }
                    },
                    "optimizationType": "LeastChange",
                    "description": "Current Configuration",
                    "suggestedChanges": [],
                    "haArchitecture": "BackupAndRestore",
                    "referenceId": "original"
                },
                {
                    "cost": {
                        "amount": 76.73,
                        "currency": "USD",
                        "frequency": "Monthly"
                    },
                    "appComponentName": "databaseappcomponent-hji",
                    "recommendationCompliance": {
                        "AZ": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 120,
                            "expectedRtoDescription": "Estimated time to promote a
secondary instance.",
                            "expectedRpoInSecs": 0,
                            "expectedRpoDescription": "Aurora data is automatically
replicated across multiple Availability Zones in a Region."
                        },
                        "Hardware": {
```

```
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 120,
                            "expectedRtoDescription": "Estimated time to promote a
secondary instance.",
                            "expectedRpoInSecs": 0,
                            "expectedRpoDescription": "Aurora data is automatically
replicated across multiple Availability Zones in a Region."
                        },
                        "Software": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 900,
                            "expectedRtoDescription": "Estimate time to backtrack to a
stable state.",
                            "expectedRpoInSecs": 300,
                            "expectedRpoDescription": "Estimate for latest restorable
time for point in time recovery."
                        }
                    },
                    "optimizationType": "BestAZRecovery",
                    "description": "Aurora database cluster with one read replica, with
backtracking window of 24 hours.",
                    "suggestedChanges": [
                        "Add read replica in the same region",
                        "Change DB instance to a supported class (db.t3.small)",
                        "Change to Aurora",
                        "Enable cluster backtracking",
                        "Enable instance backup with retention period 7"
                    ],
                    "haArchitecture": "WarmStandby",
                    "referenceId": "rds:config:aurora-backtracking"
                }
            ]
        },
        {
            "appComponentName": "storageappcomponent-rlb",
            "recommendationStatus": "BreachedUnattainable",
            "configRecommendations": [
                {
                    "cost": {
                        "amount": 0.0,
                        "currency": "USD",
                        "frequency": "Monthly"
                    },
                    "appComponentName": "storageappcomponent-rlb",
```

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

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

ステップ 3: アプリケーションプログラムを変更する

AWS Resilience Hub ではアプリケーションのドラフトバージョンを編集し、その変更を新しい「発行済みの」バージョンに発行することで、アプリケーションリソースを変更できます。AWS Resilience Hub は、回復力評価を実行するために、更新されたリソースを含むアプリケーションの発行済みバージョンを使用します。

詳細については、次のトピックを参照してください。

- the section called “リソースの手動追加”
- the section called “リソースを 1 つのアプリケーションコンポーネントにグループ化”
- the section called “AppComponent からのリソースの除外”

リソースのアプリケーションへの手動追加

リソースが入力ソースの一部としてデプロイされていない場合は、AWS Resilience Hub では`CreateAppVersionResource`API を使用してリソースをアプリケーションに手動で追加できます。この API の詳細については、「https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_CreateAppVersionResource.html」を参照してください。

に以下のパラメータを提供する必要があります。

- アプリケーションの Amazon リソースネーム (ARN)。
- リソースの論理的な ID。
- リソースの物理 ID
- AWS CloudFormation type

次の例では、`CreateAppVersionResource` APIを使用してAWS Resilience Hubのアプリケーションにリソースを手動で追加する方法を示しています。

リクエスト

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

レスポンス

```
{
    "appArn": "<App_ARN>",
    "appVersion": "draft",
    "physicalResource": {
```

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

リソースを 1 つのアプリケーションコンポーネントにグループ化

アプリケーションコンポーネント (AppComponent) は、1 つのユニットとして機能し、障害が発生する AWS 関連リソースのグループです。たとえば、スタンバイデプロイメントとして使用されるクロスリージョンのワークロードがある場合です。AWS Resilience Hub には、どの AWS リソースをどの種類の AppComponent に属させることができるかを管理するルールがあります。AWS Resilience Hub では以下のリソース管理 API を使用して、リソースを単一の AppComponent にグループ化できます。

- `UpdateAppVersionResource`— この API はアプリケーションのリソース詳細を更新します。この API の詳細については、UpdateAppVersionResourceを参照してください。
- `DeleteAppVersionAppComponent`— この API はアプリケーションから AppComponent を削除します。この API の詳細については、DeleteAppVersionAppComponentを参照してください。

次の例では、`DeleteAppVersionAppComponent`API を使用してAWS Resilience Hubのアプリケーションのリソース詳細を更新する方法を示しています。

リクエスト

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

```
--id new-app-component
```

レスポンス

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

次の例では、AWS Resilience HubでUpdateAppVersionResourceAPI を使用して、前の例で作成した空の AppComponent を削除する方法を示しています。

リクエスト

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

レスポンス

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

AppComponent からのリソースの除外

AWS Resilience Hub ではUpdateAppVersionResource API を使用してリソースを評価から除外できます。これらのリソースは、アプリケーションの回復力を計算する際には考慮されません。

この API の詳細については、「https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_UpdateAppVersionResource.html」を参照してください。

> **Note**
>
> 入力ソースからインポートされたリソースのみを除外できます。

次の例は、UpdateAppVersionResource APIを使用する際にAWS Resilience Hubのアプリケーションのリソースを除外する方法を示しています。

リクエスト

```
aws resiliencehub update-app-version-resource \
--app-arn <App_ARN> \
--resource-name "ec2instance-nvz" \
--excluded
```

レスポンス

```
{
    "appArn": "<App_ARN>",
    "appVersion": "draft",
    "physicalResource": {
        "resourceName": "ec2instance-nvz",
        "logicalResourceId": {
            "identifier": "ec2",
            "terraformSourceName": "test.state.file"
        },
        "physicalResourceId": {
            "identifier": "i-0b58265a694e5ffc1",
            "type": "Native",
            "awsRegion": "us-west-2",
            "awsAccountId": "123456789101"
        },
        "resourceType": "AWS::EC2::Instance",
        "appComponents": [
            {
                "name": "computeappcomponent-nrz",
                "type": "AWS::ResilienceHub::ComputeAppComponent"
            }
```

```
            ]
        }
}
```

のセキュリティ AWS Resilience Hub

AWS クラウドセキュリティは最優先事項です。 AWS お客様は、最もセキュリティに敏感な組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャの恩恵を受けることができます。

セキュリティは、 AWS お客様とお客様との間で共有される責任です。責任共有モデルではこれを、クラウドのセキュリティ、およびクラウド内でのセキュリティと説明しています:

- クラウドのセキュリティ — AWS AWS AWS クラウド内でサービスを実行するインフラストラクチャを保護する責任があります。 AWS また、安全に使用できるサービスも提供します。第三者監査人は、AWS、当社のセキュリティの有効性を定期的にテストおよび検証しています。に適用されるコンプライアンスプログラムについては AWS Resilience Hub、「AWS コンプライアンスプログラム別の対象サービス」「」を参照してください。
- クラウドにおけるセキュリティ — お客様の責任は、 AWS 使用するサービスによって決まります。また、お客様は、データの機密性、会社の要件、適用される法律や規制など、その他の要因についても責任を負います。

このドキュメントは、利用時に責任分担モデルを適用する方法を理解するのに役立ちます AWS Resilience Hub。以下のトピックでは、 AWS Resilience Hub セキュリティとコンプライアンスの目標を満たすように構成する方法を示しています。また、 AWS AWS Resilience Hub リソースの監視と保護に役立つ他のサービスの使い方についても学びます。

コンテンツ

におけるデータ保護 AWS Resilience Hub

AWS のデータ保護には、https://aws.amazon.com/compliance/shared-responsibility-model/、 (責任分担モデル) が適用されます AWS Resilience Hub。このモデルで説明したように、 AWS は、 AWS クラウドすべてを支えるグローバルインフラストラクチャを保護する責任があります。お客様は、このインフラストラクチャでホストされているコンテンツに対する管理を維持する責任があります。また、使用する AWS のサービス のセキュリティ設定と管理タスクもユーザーの責任となります。

データプライバシーの詳細については、「データプライバシーのよくある質問」を参照してください。欧州でのデータ保護の詳細については、AWS セキュリティブログに投稿された記事「AWS 責任共有モデルおよび GDPR」を参照してください。

データ保護のため、 AWS アカウント 認証情報を保護し、 AWS IAM Identity Center または AWS Identity and Access Management (IAM) を使用して個々のユーザーを設定することをお勧めします。この方法により、それぞれのジョブを遂行するために必要な権限のみが各ユーザーに付与されます。また、次の方法でデータを保護することもお勧めします:

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用してリソースと通信します。 AWS TLS 1.2 は必須であり TLS 1.3 がお勧めです。
- を使用して API とユーザーアクティビティのロギングを設定します。 AWS CloudTrail
- AWS 暗号化ソリューションと、 AWS のサービスその中に含まれるデフォルトのセキュリティコントロールをすべて使用してください。
- Amazon Macie などの高度なマネージドセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- コマンドラインインターフェイスまたは API AWS を介してアクセスするときに FIPS 140-2 で検証された暗号モジュールが必要な場合は、FIPS エンドポイントを使用してください。利用可能な FIPS エンドポイントの詳細については、「連邦情報処理規格 (FIPS) 140-2」を参照してください。

お客様の E メールアドレスなどの極秘または機密情報は、タグ、または名前フィールドなどの自由形式のテキストフィールドに配置しないことを強くお勧めします。これには、コンソール、API、または SDK AWS のサービス を使用して Resilience Hub などと連携する場合も含まれます。 AWS CLI AWS 名前に使用する自由記述のテキストフィールドやタグに入力したデータは、課金や診断ログに使用される場合があります。外部サーバーへの URL を提供する場合は、そのサーバーへのリクエストを検証するための認証情報を URL に含めないように強くお勧めします。

保管中の暗号化

AWS Resilience Hub 保存中のデータを暗号化します。 AWS Resilience Hub 保存中のデータは、透過的なサーバー側の暗号化を使用して暗号化されます。これは、機密データの保護における負担と複雑な作業を減らすのに役立ちます。保管時に暗号化することで、セキュリティを重視したアプリケーションを構築して、暗号化のコンプライアンスと規制の要件を満たすことができます。

転送中の暗号化

AWS Resilience Hub サービスと他の統合サービス間で転送中のデータを暗号化します。 AWS AWS Resilience Hub サービスと統合サービス間でやり取りされるすべてのデータは、トランスポート層セキュリティ (TLS) を使用して暗号化されます。 AWS Resilience Hub AWS サービス全体で特定の種類のターゲットに対して事前設定されたアクションを提供し、ターゲットリソースに対するアクションをサポートします。

AWS レジリエンスハブのIdentity and Access Management

AWS Identity and Access Management (IAM) は、 AWS のサービス 管理者がリソースへのアクセスを安全に制御できるようにするものです。 AWS IAM 管理者は、 AWS Resilience Hub リソースを使用するユーザーを認証 (サインイン) および許可 (権限の付与) できるユーザーを制御します。IAM AWS のサービス は追加料金なしで使用できるアプリです。

トピック

対象者

AWS Identity and Access Management (IAM) の使用方法は、 AWS レジリエンスハブで行う作業によって異なります。

サービスユーザー — AWS Resilience Hub サービスを使用して業務を行う場合、管理者は必要な認証情報と権限を提供します。 AWS Resilience Hub の機能を業務に使用すればするほど、追加の権限が必要になることがあります。アクセスの管理方法を理解しておくと、管理者に適切な許可をリクエストするうえで役立ちます。 AWS Resilience Hub の機能にアクセスできない場合は、を参照してください。AWS Resilience Hub の ID とアクセスのトラブルシューティング

サービス管理者 — AWS 社内でレジリエンスハブのリソースを担当している場合は、 AWS おそらくレジリエンスハブへのフルアクセス権を持っているでしょう。サービスユーザーがアクセスすべき AWS Resilience Hub の機能とリソースを決定するのはあなたの仕事です。その後、IAM 管理者にリクエストを送信して、サービスユーザーの権限を変更する必要があります。このページの情報を点検して、IAM の基本概念を理解してください。会社が AWS Resilience Hub で IAM をどのように使用できるかについての詳細は、を参照してください。AWS レジリエンスハブと IAM の連携の仕組み

IAM 管理者 — IAM 管理者の方は、Resilience Hub へのアクセスを管理するポリシーを作成する方法の詳細を知りたいと思うかもしれません。 AWS IAM で使用できる AWS Resilience Hub アイデンティティベースのポリシーの例を確認するには、を参照してください。レジリエンスハブのアイデンティティベースのポリシー例 AWS

アイデンティティを使用した認証

認証とは、ID AWS 認証情報を使用してサインインする方法です。IAM ユーザーとして AWS アカウントのルートユーザー、または IAM ロールを引き受けて認証 (サインイン AWS) する必要があります。

ID ソースを通じて提供された認証情報を使用して、フェデレーション ID AWS としてサインインできます。 AWS IAM Identity Center フェデレーテッド ID の例としては、(IAM Identity Center) ユーザー、会社のシングルサインオン認証、Google や Facebook の認証情報などがあります。フェデレーティッドアイデンティティとしてサインインする場合、IAM ロールを使用して、前もって管理者により ID フェデレーションが設定されています。 AWS フェデレーションを使用してアクセスすると、間接的にロールを引き継ぐことになります。

ユーザーのタイプによっては、 AWS Management Console AWS またはアクセスポータルにサインインできます。へのサインインについて詳しくは AWS、『AWS サインイン ユーザーガイド』の「AWS アカウントにサインインする方法」を参照してください。

AWS プログラムでアクセスする場合は、認証情報を使用してリクエストに暗号署名するためのソフトウェア開発キット (SDK) とコマンドラインインターフェイス (CLI) AWS を提供します。 AWS ツールを使用しない場合は、リクエストに自分で署名する必要があります。推奨方法を使用して自分

でリクエストに署名する方法の詳細については、IAM ユーザーガイドの「 AWS API リクエストへの署名」を参照してください。

使用する認証方法を問わず、追加セキュリティ情報の提供をリクエストされる場合もあります。たとえば、アカウントのセキュリティを強化するために多要素認証 (MFA) AWS を使用することを推奨しています。詳細については、『AWS IAM Identity Center ユーザーガイド』の「Multi-factor authentication」(多要素認証) および『IAM ユーザーガイド』の「AWSにおける多要素認証 (MFA) の使用」を参照してください。

AWS アカウント root ユーザー

を作成するときは AWS アカウント、 AWS のサービス アカウント内のすべてのリソースに完全にアクセスできる 1 つのサインイン ID から始めます。この ID は AWS アカウント root ユーザーと呼ばれ、アカウントの作成に使用したメールアドレスとパスワードでサインインすることでアクセスされます。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザーの認証情報は保護し、ルートユーザーでしか実行できないタスクを実行するときに使用します。ルートユーザーとしてサインインする必要があるタスクの完全なリストについては、『IAM ユーザーガイド』の「ルートユーザー認証情報が必要なタスク」を参照してください。

フェデレーティッドアイデンティティ

ベストプラクティスとして、管理者アクセスを必要とするユーザーを含む人間のユーザーに、ID AWS のサービス プロバイダーとのフェデレーションを使用して一時的な認証情報を使用してアクセスするように要求します。

フェデレーテッド ID とは、エンタープライズユーザーディレクトリ、ウェブ ID プロバイダー、Identity Center ディレクトリのユーザー、または ID AWS のサービス ソースを通じて提供された認証情報を使用してアクセスする任意のユーザーです。 AWS Directory Serviceフェデレーテッド ID がアクセスすると AWS アカウント、そのユーザーがロールを引き受け、そのロールが一時的な認証情報を提供します。

アクセスを一元管理する場合は、 AWS IAM Identity Centerを使用することをお勧めします。IAM Identity Center でユーザーとグループを作成したり、独自のアイデンティティソース内のユーザーやグループに接続して同期したりして、すべてのアプリケーションで使用することができます。 AWS アカウント IAM Identity Center の詳細については、『AWS IAM Identity Center ユーザーガイド』の「What is IAM Identity Center?」(IAM Identity Center とは) を参照してください。

IAM ユーザーとグループ

IAM ユーザーは、1 人のユーザーまたはアプリケーションに対して特定の権限を持つ社内の AWS アカウント ID です。可能であれば、パスワードやアクセスキーなどの長期的な認証情報を保有する IAM ユーザーを作成する代わりに、一時認証情報を使用することをお勧めします。ただし、IAM ユーザーでの長期的な認証情報が必要な特定のユースケースがある場合は、アクセスキーをローテーションすることをお勧めします。詳細については、『IAM ユーザーガイド』の「長期的な認証情報を必要とするユースケースのためにアクセスキーを定期的にローテーションする」を参照してください。

IAM グループは、IAM ユーザーの集団を指定するアイデンティティです。グループとしてサインインすることはできません。グループを使用して、複数のユーザーに対して一度に権限を指定できます。多数のユーザーグループがある場合、グループを使用することで権限の管理が容易になります。例えば、IAMAdmins という名前のグループを設定して、そのグループに IAM リソースを管理する権限を与えることができます。

ユーザーは、ロールとは異なります。ユーザーは 1 人の人または 1 つのアプリケーションに一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。ユーザーには永続的な長期の認証情報がありますが、ロールでは一時的な認証情報が提供されます。詳細については、『IAM ユーザーガイド』の「IAM ユーザー (ロールではなく) の作成が適している場合」を参照してください。

IAM ロール

IAM ロールは、 AWS アカウント 特定の権限を持つ社内の ID です。これは IAM ユーザーに似ていますが、特定のユーザーには関連付けられていません。 AWS Management Console ロールを切り替えることで、の IAM ロールを一時的に引き受けることができます。 AWS CLI または AWS API オペレーションを呼び出すか、カスタム URL を使用してロールを引き受けることができます。ロールを使用する方法の詳細については、『IAM ユーザーガイド』の「IAM ロールの使用」を参照してください。

IAM ロールと一時的な認証情報は、次の状況で役立ちます:

- フェデレーションユーザーアクセス – フェデレーティッドアイデンティティに権限を割り当てるには、ロールを作成してそのロールの権限を定義します。フェデレーティッドアイデンティティが認証されると、そのアイデンティティはロールに関連付けられ、ロールで定義されている権限が付与されます。フェデレーションの詳細については、『IAM ユーザーガイド』の「サードパーティーアイデンティティプロバイダー向けロールの作成」 を参照してください。IAM アイデンティティセンターを使用する場合、権限セットを設定します。アイデンティティが認証後にアク

セスできるものを制御するため、IAM Identity Center は、権限セットを IAM のロールに関連付けます。権限セットの詳細については、『AWS IAM Identity Center ユーザーガイド』の「権限セット」を参照してください。

- 一時的な IAM ユーザー権限 - IAM ユーザーまたはロールは、特定のタスクに対して複数の異なる権限を一時的に IAM ロールで引き受けることができます。
- クロスアカウントアクセス - IAM ロールを使用して、自分のアカウントのリソースにアクセスすることを、別のアカウントの人物 (信頼済みプリンシパル) に許可できます。クロスアカウントアクセス権を付与する主な方法は、ロールを使用することです。ただし、ロールをプロキシとして使用する代わりに AWS のサービス、ポリシーをリソースに直接アタッチできるものもあります。クロスアカウントアクセスにおけるロールとリソースベースのポリシーの違いについては、『IAM ユーザーガイド』の「IAM ロールとリソースベースのポリシーとの相違点」を参照してください。
- クロスサービスアクセス — AWS のサービス AWS のサービス他の機能を使用するものもあります。例えば、あるサービスで呼び出しを行うと、通常そのサービスによって Amazon EC2 でアプリケーションが実行されたり、Amazon S3 にオブジェクトが保存されたりします。サービスでは、呼び出し元プリンシパルの権限、サービスロール、またはサービスにリンクされたロールを使用してこれを行う場合があります。
  - 転送アクセスセッション (FAS) — IAM ユーザーまたはロールを使用してアクションを実行する場合 AWS、あなたはプリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 AWS のサービス を呼び出したプリンシパルの権限をリクエスト元と組み合わせて使用して AWS のサービス、ダウンストリームサービスにリクエストを行います。FASリクエストは、AWS のサービス サービスが他のユーザーとのやりとりやリソースとのやり取りを必要とするリクエストを受信したときにのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。
  - サービスロール - サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、『IAM ユーザーガイド』の「AWS のサービスに権限を委任するロールの作成」を参照してください。
  - サービスにリンクされたロール — サービスにリンクされたロールは、にリンクされているサービスロールの一種です。 AWS のサービスサービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。 AWS アカウント サービスにリンクされたロールはに表示され、そのサービスが所有します。IAM 管理者は、サービスにリンクされたロールの権限を表示できますが、編集することはできません。

- Amazon EC2 で実行されるアプリケーション — IAM ロールを使用して、EC2 インスタンスで実行され、 AWS API AWS CLI リクエストを行うアプリケーションの一時的な認証情報を管理できます。これは、EC2 インスタンス内でのアクセスキーの保存に推奨されます。EC2 AWS インスタンスにロールを割り当て、そのロールをそのすべてのアプリケーションで使用できるようにするには、インスタンスにアタッチされるインスタンスプロファイルを作成します。インスタンスプロファイルにはロールが含まれ、EC2 インスタンスで実行されるプログラムは一時的な認証情報を取得できます。詳細については、『IAM ユーザーガイド』の「Amazon EC2 インスタンスで実行されるアプリケーションに IAM ロールを使用して権限を付与する」を参照してください。

IAM ロールと IAM ユーザーのどちらを使用するかについては、『IAM ユーザーガイド』の「(IAM ユーザーではなく) IAM ロールをいつ作成したら良いのか?」を参照してください。

ポリシーを使用したアクセスの管理

AWS ポリシーを作成して AWS ID またはリソースにアタッチすることで、アクセスを制御します。ポリシーとは、ID またはリソースに関連付けると権限を定義するオブジェクトです。 AWS AWS プリンシパル (ユーザー、ルートユーザー、またはロールセッション) がリクエストを行うと、これらのポリシーを評価します。ポリシーでの権限により、リクエストが許可されるか拒否されるかが決まります。ほとんどのポリシーは JSON AWS ドキュメントとして保存されます。JSON ポリシードキュメントの構造と内容の詳細については、『IAM ユーザーガイド』の「JSON ポリシー概要」を参照してください。

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどんなリソースにどんな条件でアクションを実行できるかということです。

デフォルトでは、ユーザーやロールに権限はありません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き継ぐことができます。

IAM ポリシーは、オペレーションの実行方法を問わず、アクションの権限を定義します。例えば、`iam:GetRole` アクションを許可するポリシーがあるとします。そのポリシーを持つユーザは AWS Management Console、、 AWS CLI、または AWS API からロール情報を取得できます。

アイデンティティベースのポリシー

アイデンティティベースポリシーは、IAM ユーザー、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 権限ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティ

ベースのポリシーを作成する方法については、『IAM ユーザーガイド』の「IAM ポリシーの作成」を参照してください。

アイデンティティベースポリシーは、さらにインラインポリシーまたはマネージドポリシーに分類できます。インラインポリシーは、単一のユーザー、グループ、またはロールに直接埋め込まれています。管理ポリシーは、内の複数のユーザー、グループ、およびロールにアタッチできるスタンドアロンポリシーです。 AWS アカウント管理ポリシーには、 AWS 管理ポリシーと顧客管理ポリシーが含まれます。マネージドポリシーまたはインラインポリシーのいずれかを選択する方法については、『IAM ユーザーガイド』の「マネージドポリシーとインラインポリシーの比較」を参照してください。

リソースベースのポリシー

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザ、ロール、フェデレーティッドユーザ、またはを含めることができます。 AWS のサービス

リソースベースのポリシーは、そのサービス内にあるインラインポリシーです。IAM AWS の管理ポリシーをリソースベースのポリシーで使用することはできません。

アクセスコントロールリスト (ACL)

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするための権限を持つかをコントロールします。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

ACL をサポートするサービスの例としては AWS WAF、Amazon S3、、および Amazon VPC があります。ACL の詳細については、『Amazon Simple Storage Service デベロッパーガイド』の「アクセスコントロールリスト (ACL) の概要」を参照してください。

その他のポリシータイプ

AWS あまり一般的ではないポリシータイプもサポートしています。これらのポリシータイプでは、より一般的なポリシータイプで付与された最大の権限を設定できます。

- アクセス許可の境界 - アクセス許可の境界は、アイデンティティベースのポリシーによって IAM エンティティ (IAM ユーザーまたはロール) に付与できる権限の上限を設定する高度な機能です。エンティティにアクセス許可の境界を設定できます。結果として得られる権限は、エンティティのアイデンティティベースポリシーとそのアクセス許可の境界の共通部分になります。Principal フィールドでユーザーまたはロールを指定するリソースベースのポリシーでは、アクセス許可の境界は制限されません。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。アクセス許可の境界界の詳細については、『IAM ユーザーガイド』の「IAM エンティティのアクセス許可の境界」を参照してください。
- サービスコントロールポリシー (SCP) — SCP は、組織または組織単位 (OU) の最大権限を指定する JSON ポリシーです。 AWS Organizations AWS Organizations は、 AWS アカウント 企業が所有する複数のものをグループ化して一元管理するためのサービスです。組織内のすべての機能を有効にすると、サービスコントロールポリシー (SCP) を一部またはすべてのアカウントに適用できます。SCP は、メンバーアカウントのエンティティ (各エンティティを含む) の権限を制限します。 AWS アカウントのルートユーザー Organizations と SCP の詳細については、『AWS Organizations ユーザーガイド』の「SCP の仕組み」を参照してください。
- セッションポリシー - セッションポリシーは、ロールまたはフェデレーションユーザーの一時的なセッションをプログラムで作成する際にパラメータとして渡す高度なポリシーです。結果としてセッションの権限は、ユーザーまたはロールのアイデンティティベースポリシーとセッションポリシーの共通部分になります。また、リソースベースのポリシーから権限が派生する場合もあります。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。詳細については、『IAM ユーザーガイド』の「セッションポリシー」を参照してください。

複数のポリシータイプ

1 つのリクエストに複数のタイプのポリシーが適用されると、結果として作成される権限を理解するのがさらに難しくなります。 AWS 複数のポリシータイプが関係している場合にリクエストを許可するかどうかを決定する方法については、IAM ユーザーガイドの「ポリシー評価ロジック」を参照してください。

AWS レジリエンスハブと IAM の連携の仕組み

IAM を使用してレジリエンスハブへのアクセスを管理する前に、 AWS レジリエンスハブで使用できる IAM 機能について確認してください。 AWS

レジリエンスハブで使用できる IAM 機能 AWS

IAM 機能	AWS レジリエンスハブのサポート
アイデンティティベースのポリシー	Yes
リソースベースのポリシー	No
ポリシーアクション	Yes
ポリシーリソース	はい
ポリシー条件キー (サービス固有)	はい
ACL	No
ABAC (ポリシー内のタグ)	部分的
一時的な認証情報	はい
転送アクセスセッション (FAS)	はい
サービスロール	はい

AWS Resilience Hub AWS やその他のサービスがほとんどの IAM 機能でどのように機能するかを大まかに把握するには、IAM ユーザーガイドの「IAM AWS と連携するサービス」を参照してください。

レジリエンスハブのアイデンティティベースのポリシー AWS

アイデンティティベースポリシーをサポートする	Yes

アイデンティティベースポリシーは、IAM ユーザー、ユーザーグループ、ロールなど、アイデンティティにアタッチできる JSON 権限ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースのポリシーを作成する方法については、『IAM ユーザーガイド』の「IAM ポリシーの作成」を参照してください。

IAM アイデンティティベースのポリシーでは、許可または拒否するアクションとリソース、およびアクションを許可または拒否する条件を指定できます。プリンシパルは、それが添付されているユーザーまたはロールに適用されるため、アイデンティティベースのポリシーでは指定できません。JSON ポリシーで使用できるすべての要素については、「IAM ユーザーガイド」の「IAM JSON ポリシーの要素のリファレンス」を参照してください。

レジリエンスハブのアイデンティティベースのポリシー例 AWS

AWS Resilience Hub の ID ベースのポリシーの例については、を参照してください。レジリエンスハブのアイデンティティベースのポリシー例 AWS

レジリエンスハブ内のリソースベースのポリシー AWS

リソースベースのポリシーのサポート	No

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザ、ロール、フェデレーティッドユーザ、またはを含めることができます。 AWS のサービス

クロスアカウントアクセスを有効にするには、アカウント全体、または別のアカウントの IAM エンティティをリソースベースのポリシーのプリンシパルとして指定します。リソースベースのポリシーにクロスアカウントのプリンシパルを追加しても、信頼関係は半分しか確立されない点に注意してください。プリンシパルとリソースが異なる場合 AWS アカウント、信頼されたアカウントの IAM 管理者は、プリンシパルエンティティ (ユーザーまたはロール) にリソースへのアクセス権限を付与する必要もあります。IAM 管理者は、アイデンティティベースのポリシーをエンティティにアタッチすることで権限を付与します。ただし、リソースベースのポリシーで、同じアカウントのプリンシパルへのアクセス権が付与されている場合は、アイデンティティベースのポリシーを追加する必要はありません。詳細については、『IAM ユーザーガイド』の「IAM ロールとリソースベースのポリシーとの相違点」を参照してください。

AWS レジリエンスハブのポリシーアクション

ポリシーアクションに対するサポート	はい

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどんなリソースにどんな条件でアクションを実行できるかということです。

JSON ポリシーのAction要素には、ポリシー内のアクセスを許可または拒否するために使用できるアクションが記述されます。ポリシーアクションは通常、関連する AWS API オペレーションと同じ名前です。一致する API オペレーションのない権限のみのアクションなど、いくつかの例外があります。また、ポリシーに複数アクションが必要なオペレーションもあります。これらの追加アクションは、 依存アクション と呼ばれます。

このアクションは、関連付けられたオペレーションを実行するための権限を付与するポリシーで使用されます。

AWS Resilience Hub アクションのリストについては、『サービス認証リファレンス』の「AWS Resilience Hub で定義されているアクション」を参照してください。

AWS Resilience Hub のポリシーアクションは、アクションの前に次のプレフィックスを使用します。

```
resiliencehub
```

単一のステートメントで複数のアクションを指定するには、アクションをカンマで区切ります。

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

AWS Resilience Hub の ID ベースのポリシーの例を表示するには、を参照してください。レジリエンスハブのアイデンティティベースのポリシー例 AWS

レジリエンスハブのポリシーリソース AWS

ポリシーリソースに対するサポート	はい

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどんなリソースにどんな条件でアクションを実行できるかということです。

Resource JSON ポリシー要素は、アクションが適用されるオブジェクトを指定します。ステートメントには、Resource または NotResource要素を含める必要があります。ベストプラクティスとして、Amazon リソースネーム (ARN) を使用してリソースを指定します。これは、リソースレベルの権限と呼ばれる特定のリソースタイプをサポートするアクションに対して実行できます。

オペレーションのリスト化など、リソースレベルの権限をサポートしないアクションの場合は、ステートメントがすべてのリソースに適用されることを示すために、ワイルドカード (*) を使用します。

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

AWS Resilience Hub のリソースタイプとその ARN のリストについては、『サービス認証リファレンス』の「AWS Resilience Hub によって定義されたリソース」を参照してください。各リソースの ARN を指定できるアクションについては、「AWS Resilience Hub によって定義されたアクション」を参照してください。

AWS Resilience Hub の ID ベースのポリシーの例については、を参照してください。レジリエンスハブのアイデンティティベースのポリシー例 AWS

レジリエンスハブのポリシー条件キー AWS

サービス固有のポリシー条件キーのサポート	はい

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどんなリソースにどんな条件でアクションを実行できるかということです。

Condition 要素 (または Condition ブロック) を使用すると、ステートメントが有効な条件を指定できます。Condition 要素はオプションです。イコールや未満などの 条件演算子 を使用して条件式を作成することで、ポリシーの条件とリクエスト内の値を一致させることができます。

1 つのステートメントに複数の Condition 要素を指定するか、1 つの Condition 要素に複数のキーを指定すると、 AWS は AND 論理演算子を使用してそれらを評価します。1 つの条件キーに複

数の値を指定すると、 AWS 0R論理演算を使用して条件を評価します。ステートメントの権限が付与される前にすべての条件が満たされる必要があります。

条件を指定する際にプレースホルダー変数も使用できます。例えば IAM ユーザーに、IAM ユーザー名がタグ付けされている場合のみリソースにアクセスできる権限を付与することができます。詳細については、『IAM ユーザーガイド』の「IAM ポリシーの要素: 変数およびタグ」を参照してください。

AWS グローバル条件キーとサービス固有の条件キーをサポートします。 AWS すべてのグローバル条件キーを確認するには、IAM ユーザーガイドの「AWS グローバル条件コンテキストキー」を参照してください。

AWS Resilience Hub の条件キーのリストについては、『サービス認証リファレンス』の「 AWS Resilience Hub の条件キー」を参照してください。条件キーを使用できるアクションとリソースについては、「AWS Resilience Hub で定義されるアクション」を参照してください。

AWS Resilience Hub の ID ベースのポリシーの例については、を参照してください。レジリエンスハブのアイデンティティベースのポリシー例 AWS

レジリエンスハブの ACL AWS

ACL のサポート	No

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするための権限を持つかを制御します。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

ABAC とレジリエンス・ハブ AWS

ABAC (ポリシー内のタグ) のサポート	部分的

属性ベースのアクセスコントロール (ABAC) は、属性に基づいて権限を定義する認可戦略です。では AWS、これらの属性はタグと呼ばれます。IAM エンティティ (ユーザーまたはロール) AWS や多くのリソースにタグを付けることができます。エンティティとリソースのタグ付けは、ABAC の最初の手順です。その後、プリンシパルのタグがアクセスしようとしているリソースのタグと一致した場合に操作を許可するように ABAC ポリシーを設計します。

ABAC は、急成長する環境やポリシー管理が煩雑になる状況で役立ちます。

タグに基づいてアクセスを管理するには、aws:ResourceTag/*key-name*、aws:RequestTag/*key-name*、または aws:TagKeys の条件キーを使用して、ポリシーの条件要素でタグ情報を提供します。

サービスがすべてのリソースタイプに対して 3 つの条件キーすべてをサポートする場合、そのサービスの値ははいです。サービスが一部のリソースタイプに対してのみ 3 つの条件キーのすべてをサポートする場合、値は「部分的」になります。

ABAC の詳細については、『IAM ユーザーガイド』の「ABAC とは?」を参照してください。ABAC をセットアップするステップを説明するチュートリアルについては、「IAM ユーザーガイド」の「属性に基づくアクセスコントロール (ABAC) を使用する」を参照してください。

AWS Resilience Hub で一時的な認証情報を使用する

一時的な認証情報のサポート	はい

AWS のサービス 一時的な認証情報を使用してサインインすると機能しないものもあります。 AWS のサービス 一時的な認証情報で機能するものなど、追加情報については、『IAM ユーザーガイド』の「IAM と連携する」を参照してくださいAWS のサービス 。

ユーザー名とパスワード以外の方法でにサインインすると、 AWS Management Console 一時的な認証情報が使用されることになります。たとえば、会社のシングルサインオン (SSO) AWS リンクを使用してアクセスすると、そのプロセスによって一時的な認証情報が自動的に作成されます。また、ユーザーとしてコンソールにサインインしてからロールを切り替える場合も、一時的な認証情報が自動的に作成されます。ロールの切り替えに関する詳細については、『IAM ユーザーガイド』の「ロールへの切り替え (コンソール)」を参照してください。

または API を使用して一時的な認証情報を手動で作成できます。 AWS CLI AWS その後、その一時的な認証情報を使用してアクセスできます AWS。 AWS 長期アクセスキーを使用する代わりに、一時的な認証情報を動的に生成することをおすすめします。詳細については、「IAM の一時的セキュリティ認証情報」を参照してください。

AWS Resilience Hub へのアクセスセッションを転送する

フォワードアクセスセッション (FAS) をサポート	はい

IAM ユーザーまたはロールを使用してアクションを実行する場合 AWS、そのユーザーはプリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FASは、を呼び出したプリンシパルの権限と AWS のサービス、 AWS のサービス ダウンストリームサービスにリクエストを行うリクエストを組み合わせて使用します。FASリクエストは、 AWS のサービス サービスが他のユーザーとのやりとりやリソースとのやり取りを必要とするリクエストを受信したときにのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。

AWS レジリエンスハブのサービスロール

サービスロールに対するサポート	あり

サービスロールとは、サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、『IAM ユーザーガイド』の「AWS のサービスに権限を委任するロールの作成」を参照してください。

> **Warning**
>
> サービスロールの権限を変更すると、 AWS Resilience Hub の機能が損なわれる可能性があります。 AWS Resilience Hub がガイダンスを提供している場合にのみ、サービスロールを編集してください。

レジリエンスハブのアイデンティティベースのポリシー例 AWS

デフォルトでは、ユーザーとロールには AWS Resilience Hub リソースを作成または変更する権限がありません。また、、 AWS Management Console、 AWS Command Line Interface (AWS CLI)、AWS API を使用してタスクを実行することもできません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き受けることができます。

これらサンプルの JSON ポリシードキュメントを使用して、IAM アイデンティティベースのポリシーを作成する方法については、『IAM ユーザーガイド』の「IAM ポリシーの作成」を参照してください。

各リソースタイプの ARN の形式など、 AWS Resilience Hub によって定義されるアクションとリソースタイプの詳細については、『サービス認証リファレンス』の「AWS Resilience Hub のアクション、リソース、および条件キー」を参照してください。

トピック

- ポリシーのベストプラクティス
- レジリエンスハブコンソールを使用する AWS
- 自分の権限の表示をユーザーに許可する
- 利用可能なアプリケーションの一覧が表示されます。 AWS Resilience Hub
- アプリケーションアセスメントの開始
- アプリケーションアセスメントを削除する。
- 特定のアプリケーション用のレコメンデーションテンプレートの作成
- 特定のアプリケーションの推奨テンプレートを削除する。
- 特定の耐障害性ポリシーを使用してアプリケーションを更新します。

ポリシーのベストプラクティス

ID ベースのポリシーは、アカウント内の AWS Resilience Hub リソースを誰かが作成、アクセス、削除できるかどうかを決定します。これらのアクションを実行すると、 AWS アカウントに料金が発生する可能性があります。アイデンティティベースポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください:

- AWS 管理ポリシーから始めて、最小権限の権限に移行する — ユーザーとワークロードへのアクセス権限の付与を開始するには、AWS 多くの一般的なユースケースで権限を付与する管理ポリシーを使用してください。これらのポリシーは、で利用できます。 AWS アカウント AWS ユースケースに固有のカスタマー管理ポリシーを定義して、権限をさらに減らすことをお勧めします。詳細については、『IAM ユーザーガイド』の「AWS マネージドポリシー」または「AWS ジョブ機能の管理ポリシー」を参照してください。
- 最小特権を適用する – IAM ポリシーで権限を設定するときは、タスクの実行に必要な権限のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、最小特権権限とも呼ばれています。IAM を使用して権限を適用する方法の詳細については、『IAM ユーザーガイド』の「IAM でのポリシーと権限」を参照してください。
- IAM ポリシーで条件を使用してアクセスをさらに制限する - ポリシーに条件を追加して、アクションやリソースへのアクセスを制限できます。例えば、ポリシー条件を記述して、すべてのリクエストを SSL を使用して送信するように指定できます。サービスアクションがなどの特定の用途で

使用された場合は AWS のサービス、条件を使用してサービスアクションへのアクセスを許可することもできます AWS CloudFormation。詳細については、『IAM ユーザーガイド』の [IAM JSON policy elements: Condition] (IAM JSON ポリシー要素：条件) を参照してください。

- IAM Access Analyzer を使用して IAM ポリシーを検証し、安全で機能的な権限を確保する - IAM Access Analyzer は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語 (JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライザーは 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサポートします。詳細については、『IAM ユーザーガイド』の「IAM Access Analyzer ポリシーの検証」を参照してください。
- 多要素認証 (MFA) が必要 — IAM ユーザーまたは root ユーザーを必要とするシナリオがある場合は AWS アカウント、セキュリティを強化するために MFA をオンにしてください。API オペレーションが呼び出されるときに MFA を必須にするには、ポリシーに MFA 条件を追加します。詳細については、『IAM ユーザーガイド』の「MFA 保護 API アクセスの設定」を参照してください。

IAM でのベストプラクティスの詳細については、『IAM ユーザーガイド』の「IAM でのセキュリティのベストプラクティス」を参照してください。

レジリエンスハブコンソールを使用する AWS

AWS Resilience Hub コンソールにアクセスするには、最低限の権限が必要です。これらの権限により、内の AWS Resilience Hub リソースの詳細を一覧表示して表示できる必要があります。 AWS アカウント最小限必要な許可よりも制限が厳しいアイデンティティベースのポリシーを作成すると、そのポリシーを持つエンティティ (ユーザーまたはロール) に対してコンソールが意図したとおりに機能しません。

AWS CLI または AWS API のみを呼び出すユーザーには、最低限のコンソール権限を付与する必要はありません。代わりに、実行しようとしている API オペレーションに一致するアクションのみへのアクセスが許可されます。

ユーザーとロールが引き続き AWS Resilience Hub コンソールを使用できるようにするには、 AWS Resilience Hub *ConsoleAccess* *ReadOnly* AWS または管理ポリシーをエンティティにアタッチします。詳細については、「IAM ユーザーガイド」の「ユーザーへのアクセス許可の追加」を参照してください。

次のポリシーは、 AWS Resilience Hub コンソール内のすべてのリソースを一覧表示して表示する権限をユーザーに付与しますが、作成、更新、削除は許可しません。

```
{
```

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

自分の権限の表示をユーザーに許可する

この例では、ユーザーアイデンティティにアタッチされたインラインおよびマネージドポリシーの表示を IAM ユーザーに許可するポリシーの作成方法を示します。このポリシーには、コンソールで、またはまたは API AWS CLI を使用してこのアクションをプログラムで実行する権限が含まれています。 AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
```

```
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

利用可能なアプリケーションの一覧が表示されます。 AWS Resilience Hub

次のポリシーでは、利用可能な AWS Resilience Hub アプリケーションを一覧表示するアクセス許可をユーザーに付与します。

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

アプリケーションアセスメントの開始

次のポリシーでは、 AWS Resilience Hub 特定のアプリケーションの評価を開始する権限をユーザーに付与します。

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

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

アプリケーションアセスメントを削除する。

次のポリシーは、 AWS Resilience Hub 特定のアプリケーションの評価を削除する権限をユーザーに付与します。

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

特定のアプリケーション用のレコメンデーションテンプレートの作成

次のポリシーは、 AWS Resilience Hub 特定のアプリケーション用の推奨テンプレートを作成する権限をユーザーに付与します。

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

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

特定のアプリケーションの推奨テンプレートを削除する。

次のポリシーは、 AWS Resilience Hub 特定のアプリケーションの推奨テンプレートを削除する権限をユーザーに付与します。

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

特定の耐障害性ポリシーを使用してアプリケーションを更新します。

次のポリシーは、特定の障害耐性ポリシーを使用して AWS Resilience Hub アプリケーションを更新する権限をユーザーに付与します。

```
{
  "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/*" }
      }
    }
  ]
}
```

IAM ロールおよび権限の設定

AWS Resilience Hub アプリケーションの評価を実行する際に使用したい IAM ロールを設定できます。アプリケーションリソースへの読み取り専用アクセス権を取得するように AWS Resilience Hub を設定する方法は複数あります。ただし、 AWS Resilience Hub は以下の方法を推奨しています。

- ロールベースのアクセス — このロールは現在のアカウントで定義され、使用されます。 AWS Resilience Hub この役割を引き受け、アプリケーションのリソースにアクセスします。

  ロールベースのアクセスを提供するには、ロールに次のものが含まれている必要があります。

  - リソースを読み取る読み取り専用権限 (AWS Resilience Hub `AwsResilienceHubAssessmentPolicy`管理ポリシーの使用を推奨します)。
  - この役割を引き受ける信頼ポリシー。これにより、 AWS Resilience Hub サービスプリンシパルがこの役割を引き受けることができます。アカウントにそのようなロールが設定されていない場合は、 AWS Resilience Hub そのロールを作成する手順が表示されます。詳細については、「the section called “ステップ 6: アクセス許可の設定”」を参照してください。

  > **Note**
  >
  > 呼び出し元ロール名のみを指定し、リソースが別のアカウントにある場合は、 AWS Resilience Hub 他のアカウントでもこのロール名を使用してクロスアカウントリソースにアクセスします。オプションで、呼び出しロール名の代わりに使用される他のアカウントのロール ARN を設定できます。

- 現在の IAM ユーザーアクセス — AWS Resilience Hub は、現在の IAM ユーザーを使用してアプリケーションリソースにアクセスします。リソースが別のアカウントにある場合は、次の IAM AWS Resilience Hub ロールを引き受けてリソースにアクセスします。
  - 現在のアカウントでの `AwsResilienceHubAdminAccountRole`

- 他のアカウントでの AwsResilienceHubExecutorAccountRole

また、 AWS Resilience Hub 定期評価を設定すると、AwsResilienceHubPeriodicAssessmentRoleがその役割を引き受けます。ただし、ロールと権限を手動で設定する必要があり、一部の機能 ([レジリエンシードリフト] 検出など) が期待どおりに動作しない場合があるため、AwsResilienceHubPeriodicAssessmentRole の使用はお勧めしません。

AWS Resilience Hub の ID とアクセスのトラブルシューティング

以下の情報を参考にして、 AWS Resilience Hub と IAM を使用する際に発生する可能性のある一般的な問題の診断と修正に役立ててください。

トピック

- 私にはレジリエンスハブでアクションを実行する権限がありません。 AWS
- 私にはiam を実行する権限がありません:PassRole
- AWS アカウントAWS 自分以外の人にもレジリエンスハブのリソースへのアクセスを許可したい

私にはレジリエンスハブでアクションを実行する権限がありません。 AWS

「I am not authorized to perform an action in Amazon Bedrock」というエラーが表示された場合、そのアクションを実行できるようにポリシーを更新する必要があります。

次のエラー例は、mateojackson IAM ユーザーがコンソールを使用して、ある *my-example-widget* リソースに関する詳細情報を表示しようとしたことを想定して、その際に必要なresiliencehub:*GetWidget* アクセス許可を持っていない場合に発生するものです。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 resiliencehub:GetWidget on resource: my-example-widget
```

この場合、resiliencehub:*GetWidget* アクションを使用して *my-example-widget*リソースへのアクセスを許可するように、mateojackson ユーザーのポリシーを更新する必要があります。

サポートが必要な場合は、 AWS 管理者に問い合わせてください。サインイン資格情報を提供した担当者が管理者です。

私にはiam を実行する権限がありません:PassRole

`iam:PassRole`アクションを実行する権限がないというエラーが表示された場合は、 AWS Resilience Hub にロールを渡せるようにポリシーを更新する必要があります。

新しいサービスロールやサービスにリンクされたロールを作成する代わりに、 AWS のサービス 既存のロールをそのサービスに渡すことができるものもあります。そのためには、サービスにロールを渡す権限が必要です。

以下のエラー例は、という名前の IAM ユーザーが Resilience `marymajor` Hub AWS でコンソールを使用してアクションを実行しようとしたときに発生します。ただし、このアクションをサービスが実行するには、サービスロールから付与された権限が必要です。Mary には、ロールをサービスに渡す権限がありません。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

この場合、Mary のポリシーを更新してメアリーに `iam:PassRole` アクションの実行を許可する必要があります。

サポートが必要な場合は、管理者に問い合わせてください。 AWS サインイン資格情報を提供した担当者が管理者です。

AWS アカウントAWS 自分以外の人にもレジリエンスハブのリソースへのアクセスを許可したい

他のアカウントのユーザーや組織外の人が、リソースにアクセスするために使用できるロールを作成できます。ロールの引き受けを委託するユーザーを指定できます。リソースベースのポリシーまたはアクセス制御リスト (ACL) をサポートするサービスの場合、それらのポリシーを使用して、リソースへのアクセスを付与できます。

詳細については、以下を参照してください:

- AWS Resilience Hub がこれらの機能をサポートしているかどうかについては、を参照してください。AWS レジリエンスハブと IAM の連携の仕組み
- AWS アカウント 所有しているリソース全体のリソースへのアクセスを提供する方法については、『IAM ユーザーガイド』の「AWS アカウント 所有する別の IAM ユーザーへのアクセスを提供する」を参照してください。
- リソースへのアクセスを第三者に提供する方法については AWS アカウント、IAM ユーザーガイドの「AWS アカウント 第三者が所有するリソースへのアクセスの提供」を参照してください。

- ID フェデレーションを介してアクセスを提供する方法については、『IAM ユーザーガイド』の「外部で認証されたユーザー (ID フェデレーション) へのアクセス権限」を参照してください。
- クロスアカウントアクセスでのロールとリソースベースのポリシーの使用の違いの詳細については、『IAM ユーザーガイド』の「IAM ロールとリソースベースのポリシーとの相違点」を参照してください。

AWS Resilience Hub アクセス権限リファレンス

AWS Identity and Access Management (IAM) を使用してアプリケーションリソースへのアクセスを管理し、ユーザー、グループ、またはロールに適用される IAM ポリシーを作成できます。

AWS Resilience Hub すべてのアプリケーションは、the section called “呼び出しロール” (IAM ロール) を使用するか、現在の IAM ユーザー権限 (およびクロスアカウントおよび定期評価用の定義済みロールのセット) を使用するように設定できます。このロールには、 AWS Resilience Hub AWS 他のリソースやアプリケーションリソースへのアクセスに必要な権限を定義するポリシーをアタッチできます。呼び出し側ロールには、 AWS Resilience Hub Service Principal に追加された信頼ポリシーが必要です。

アプリケーションの権限を管理するには、the section called “AWS 管理ポリシー”を使用することをお勧めします。これらの管理ポリシーは、何も変更せずに使用することができます。また、これらを基にして独自の制限ポリシーを作成することもできます。ポリシーでは、任意の追加条件を使用して、さまざまなアクションに対するユーザーのアクセス許可をリソースレベルで制限できます。

アプリケーションリソースが異なるアカウント (セカンダリアカウントとリソースアカウント) にある場合は、アプリケーションリソースを含む各アカウントに新しいロールを設定する必要があります。

トピック

- the section called “IAM ロールを使用する”
- the section called “現在の IAM ユーザーア権限を使用する”

IAM ロールを使用する

AWS Resilience Hub 事前定義された既存の IAM ロールを使用して、プライマリアカウントまたはセカンダリアカウント/リソースアカウントのリソースにアクセスします。これはリソースにアクセスするための推奨権限オプションです。

トピック

- the section called “呼び出しロール”
- the section called “ AWS 異なるアカウントのロール (クロスアカウントアクセス用)”

呼び出しロール

AWS Resilience Hub 呼び出し元ロールは、サービスとリソースへのアクセスを前提とする AWS Identity and Access Management (IAM) ロールです。 AWS Resilience Hub AWS 例えば、CFN テンプレートとそれによって作成されるリソースにアクセス許可を持つ呼び出しロールを作成することができます。このページでは、アプリケーション呼び出しロールを作成、表示、および管理する方法について説明します。

アプリケーションを作成するときは、呼び出しロールを指定します。 AWS Resilience Hub は、リソースをインポートしたり評価を開始したりするときに、このロールを引き受けてリソースにアクセスします。 AWS Resilience Hub 呼び出し側ロールを正しく引き受けるには、 AWS Resilience Hub ロールの信頼ポリシーでサービスプリンシパル (resiliencehub.amazonaws.com) を信頼できるサービスとして指定する必要があります。

アプリケーションの呼び出しロールを表示するには、ナビゲーションペインから [アプリケーション] を選択し、[アプリケーション] ページの [アクション] メニューから [権限の更新] を選択します。

権限は、アプリケーション呼び出しロールからいつでも追加または削除できます。別のロールを使用してアプリケーションリソースにアクセスすることもできます。

トピック

- the section called “IAM コンソールで呼び出しロールを作成する”
- the section called “IAM API によるロールの管理”
- the section called “JSON ファイルを使用した信頼ポリシーの定義”

IAM コンソールで呼び出しロールを作成する

AWS Resilience Hub AWS サービスとリソースにアクセスできるようにするには、IAM コンソールを使用してプライマリアカウントで呼び出し側ロールを作成する必要があります。IAM コンソールを使用してロールを作成する方法の詳細については、「AWS サービス (コンソール) のロールの作成」を参照してください。

IAM コンソールを使用してプライマリアカウントに呼び出しロールを作成するには

1. IAM コンソール (`https://console.aws.amazon.com/iam/`) を開きます。

2. ナビゲーションペインから [ロール] を選択し、[ロールの作成] を選択します。
3. [カスタム信頼ポリシー] を選択し、[カスタム信頼ポリシー] ウィンドウに次のポリシーをコピーして、[次へ] を選択します。

> **Note**
>
> リソースが異なるアカウントにある場合は、それらのアカウントごとにロールを作成し、他のアカウントにはセカンダリアカウントの信頼ポリシーを使用する必要があります。

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

4. [権限の追加] ページの [権限ポリシー] セクションで、[プロパティまたはポリシー名でポリシーを絞り込み、エンターキーを押す] ボックスに AWSResilienceHubAsssessmentExecutionPolicy を入力します。
5. ポリシーを選択し、[次へ] を選択します。
6. [ロールの詳細] セクションの [ロール名] ボックスに、一意のロール名 (AWSResilienceHubAssessmentRole など) を入力します。

   このフィールドには英数字と '+=,.@-_/' 文字のみを入力できます。
7. (オプション) [説明] ボックスにリポジトリの説明を入力します。
8. [ロールの作成] を選択します。

   ユースケースと権限を編集するには、ステップ 6 で、[ステップ 1: 信頼済みエンティティの選択] セクションまたは [ステップ 2: 権限の追加] セクションの右側にある [編集] ボタンを選択します。

呼び出しロールとリソースロール (該当する場合) を作成したら、これらのロールを使用するようにアプリケーションを設定できます。

> **Note**
>
> アプリケーションを作成または更新するときは、現在の IAM ユーザー/ロールに呼び出しロールに対する `iam:passRole` 権限が必要です。ただし、評価を実行するのにこの権限は必要ありません。

IAM API によるロールの管理

ロールの信頼ポリシーでは、指定したプリンシパルに、ロールを引き受けるための許可を付与します。 AWS Command Line Interface (AWS CLI) を使用してロールを作成するには、`create-role`コマンドを使用します。このコマンドを使用するときに、信頼ポリシーインラインを指定することもできます。次の例は、 AWS Resilience Hub ロールを引き受けるプリンシパル権限をサービスに付与する方法を示しています。

> **Note**
>
> JSON 文字列で引用符 (' ') をエスケープするための要件は、シェルのバージョンに応じて異なる場合があります。

サンプル **create-role**

```
aws iam create-role --role-name AWSResilienceHubAssessmentRole --assume-role-policy-
document '{
  "Version": "2012-10-17","Statement":
  [
    {
      "Effect": "Allow",
      "Principal": {"Service": "resiliencehub.amazonaws.com"},
      "Action": "sts:AssumeRole"
    }
  ]
}'
```

JSON ファイルを使用した信頼ポリシーの定義

個別の JSON ファイルを使用してロールの信頼ポリシーを定義し、create-role コマンドを実行できます。次の例では、**trust-policy.json** は現在のディレクトリにある信頼ポリシーを含むファイルです。このポリシーは、**create-role** コマンドを実行することでロールにアタッチされます。**create-role** コマンドの出力はサンプル出力に示されています。ロールに権限を追加するには、attach-policy-to-roleコマンドを使用します。AWSResilienceHubAsssessmentExecutionPolicy管理ポリシーを追加することから始めることができます。このマネージドポリシーの情報については、「the section called “AWSResilienceHubAsssessmentExecutionPolicy”」を参照してください。

サンプル**trust-policy.json**

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

サンプル**create-role**

```
aws iam create-role --role-name AWSResilienceHubAssessmentRole --assume-role-policy-document file://trust-policy.json
```

サンプル出力

```
{
    "Role": {
        "Path": "/",
        "RoleName": "AWSResilienceHubAssessmentRole",
        "RoleId": "AROAQFOXMPL6TZ6ITKWND",
        "Arn": "arn:aws:iam::123456789012:role/AWSResilienceHubAssessmentRole",
        "CreateDate": "2020-01-17T23:19:12Z",
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [{
```

```
                "Effect": "Allow",
                "Principal": {
                    "Service": "resiliencehub.amazonaws.com"
                },
                "Action": "sts:AssumeRole"
            }]
        }
    }
}
```

サンプル**attach-policy-to-role**

```
aws iam attach-role-policy --role-name AWSResilienceHubAssessmentRole --
policy-arn arn:aws:iam::aws:policy/
AWSResilienceHubAsssessmentExecutionPolicy
```

AWS クロスアカウントアクセス用の異なるアカウントのロール (オプション)

リソースがセカンダリアカウントまたはリソースアカウントにある場合、 AWS Resilience Hub アプリケーションを正しく評価できるようにするには、これらのアカウントごとにロールを作成する必要があります。ロールの作成手順は、信頼ポリシーの設定を除いて、呼び出しロールの作成プロセスと似ています。

> **Note**
>
> リソースが存在するセカンダリアカウントでロールを作成する必要があります。

トピック

- the section called “IAM コンソールでのセカンダリ/リソースアカウントのロールの作成”
- the section called “IAM API によるロールの管理”
- the section called “JSON ファイルを使用した信頼ポリシーの定義”

IAM コンソールでのセカンダリ/リソースアカウントのロールの作成

AWS Resilience Hub AWS AWS 他のアカウントのサービスやリソースにアクセスできるようにするには、それぞれのアカウントにロールを作成する必要があります。

IAM コンソールを使用してセカンダリ/リソースアカウントのロールを IAM コンソールに作成するには

1. IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. ナビゲーションペインから [ロール] を選択し、[ロールの作成] を選択します。
3. [カスタム信頼ポリシー] を選択し、[カスタム信頼ポリシー] ウィンドウに次のポリシーをコピーして、[次へ] を選択します。

> **Note**
>
> リソースが異なるアカウントにある場合は、それらのアカウントごとにロールを作成し、他のアカウントにはセカンダリアカウントの信頼ポリシーを使用する必要があります。

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

4. [権限の追加] ページの [権限ポリシー] セクションで、[プロパティまたはポリシー名でポリシーを絞り込み、エンターキーを押す] ボックスに AWSResilienceHubAsssessmentExecutionPolicy を入力します。
5. ポリシーを選択し、[次へ] を選択します。
6. [ロールの詳細] セクションの [ロール名] ボックスに、一意のロール名 (AWSResilienceHubAssessmentRole など) を入力します。
7. (オプション) [説明] ボックスにリポジトリの説明を入力します。
8. [ロールの作成] を選択します。

ユースケースと権限を編集するには、ステップ 6 で、[ステップ 1: 信頼済みエンティティの選択] セクションまたは [ステップ 2: 権限の追加] セクションの右側にある [編集] ボタンを選択します。

さらに、呼び出しロールに sts:assumeRole 権限を追加して、セカンダリアカウントでそのロールを引き受けられるようにする必要もあります。

作成した各セカンダリロールの呼び出しロールに次のポリシーを追加します。

```
{
    "Effect": "Allow",
    "Resource": [
      "arn:aws:iam::secondary_account_id_1:role/RoleInSecondaryAccount_1",
      "arn:aws:iam::secondary_account_id_2:role/RoleInSecondaryAccount_2",
      ...
      ],
      "Action": [
        "sts:AssumeRole"
      ]
}
```

IAM API によるロールの管理

ロールの信頼ポリシーでは、指定したプリンシパルに、ロールを引き受けるための許可を付与します。 AWS Command Line Interface (AWS CLI) を使用してロールを作成するには、create-roleコマンドを使用します。このコマンドを使用するときに、信頼ポリシーインラインを指定することもできます。次の例は、 AWS Resilience Hub ロールを引き受ける権限をサービスプリンシパルに付与する方法を示しています。

> **Note**
>
> JSON 文字列で引用符 (' ') をエスケープするための要件は、シェルのバージョンに応じて異なる場合があります。

サンプル**create-role**

```
aws iam create-role --role-name AWSResilienceHubAssessmentRole --assume-role-policy-
document '{"Version": "2012-10-17","Statement": [{"Effect": "Allow","Principal":
```

```
 {"AWS": ["arn:aws:iam::primary_account_id:role/InvokerRoleName"]},"Action":
 "sts:AssumeRole"}]}'
```

また、個別の JSON ファイルを使用してロールの信頼ポリシーを定義することもできます。次の例では、trust-policy.json は現在のディレクトリにあるファイルです。

JSON ファイルを使用した信頼ポリシーの定義

個別の JSON ファイルを使用してロールの信頼ポリシーを定義し、create-role コマンドを実行できます。次の例では、**trust-policy.json** は現在のディレクトリにある信頼ポリシーを含むファイルです。このポリシーは、**create-role** コマンドを実行することでロールにアタッチされます。**create-role** コマンドの出力はサンプル出力に示されています。ロールに権限を追加するには、attach-policy-to-roleコマンドを使用します。AWSResilienceHubAsssessmentExecutionPolicy管理ポリシーを追加することから始めることができます。このマネージドポリシーの情報については、「the section called “AWSResilienceHubAsssessmentExecutionPolicy”」を参照してください。

サンプル**trust-policy.json**

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

サンプル**create-role**

```
aws iam create-role --role-name AWSResilienceHubAssessmentRole --assume-role-policy-
document file://trust-policy.json
```

サンプル出力

```
{
    "Role": {
        "Path": "/",
        "RoleName": "AWSResilienceHubAssessmentRole2",
        "RoleId": "AROAT2GICMEDJML6EVQRG",
        "Arn": "arn:aws:iam::262412591366:role/AWSResilienceHubAssessmentRole2",
        "CreateDate": "2023-08-02T07:49:23+00:00",
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Effect": "Allow",
                    "Principal": {
                        "AWS": [
                            "arn:aws:iam::262412591366:role/
AWSResilienceHubAssessmentRole"
                        ]
                    },
                    "Action": "sts:AssumeRole"
                }
            ]
        }
    }
}
```

サンプル**attach-policy-to-role**

```
aws iam attach-role-policy --role-name AWSResilienceHubAssessmentRole --
policy-arn arn:aws:iam::aws:policy/
AWSResilienceHubAsssessmentExecutionPolicy.
```

現在の IAM ユーザーア権限を使用する

現在の IAM ユーザー権限を使用して評価を作成および実行する場合は、この方法を使用してください。IAM ユーザーまたはユーザーに関連付けられるロールに、AWSResilienceHubAsssessmentExecutionPolicy 管理ポリシーをアタッチできます。

単一アカウントの設定

IAM ユーザーと同じアカウントで管理されているアプリケーションで評価を実行するには、上記の管理ポリシーを使用するだけで十分です。

スケジュールされた評価の設定

AWS Resilience Hub がスケジュールされた評価の関連タスクを実行できるようにするには、新しいロール AwsResilienceHubPeriodicAssessmentRole を作成する必要があります。

> **Note**
>
> - ロールベースのアクセス (前述の呼び出しロールを使用) を使用する場合、このステップは不要です。
> - ロールタイプは、AwsResilienceHubPeriodicAssessmentRole である必要があります。

AWS Resilience Hub スケジュールされた評価関連のタスクを実行できるようにするには

1. AWSResilienceHubAsssessmentExecutionPolicy 管理ポリシーをロールにアタッチします。
2. 次のポリシーを追加します。ここで、primary_account_idはアプリケーションが定義され、 AWS 評価を実行するアカウントです。さらに、定期評価の役割に関連する信頼ポリシー (AwsResilienceHubPeriodicAssessmentRole) を追加する必要があります。これにより、AWS Resilience Hub サービスが定期評価の役割を引き受ける権限が付与されます。

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

```
        "arn:aws:iam::primary_account_id:role/
AwsResilienceHubAssessmentEKSAccessRole"
      ]
    }
  ]
}
```

スケジュールされたのロールに関する信頼ポリシー (**AwsResilienceHubPeriodicAssessmentRole**)

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

クロスアカウントの設定

複数のアカウントで AWS Resilience Hub を使用している場合は、次の IAM 権限ポリシーが必要です。ユースケースによっては、 AWS アカウントごとに異なる権限が必要になる場合があります。クロスアカウントアクセス用に AWS Resilience Hub を設定する際、以下のアカウントとロールが考慮されます。

- プライマリアカウント — AWS アプリケーションを作成して評価を実行するアカウント。
- AWS セカンダリ/リソースアカウント — リソースが置かれているアカウント。

> **Note**
>
> - ロールベースのアクセス (前述の呼び出しロールを使用) を使用する場合、このステップは不要です。

- Amazon Elastic Kubernetes Service にアクセスするためのアクセス権限の設定の詳細については、the section called “Amazon EKS AWS Resilience Hub クラスターへのアクセスを有効にする”を参照してください。

プライマリアカウントの設定

プライマリアカウントに新しいロールを作成し、AwsResilienceHubAdminAccountRole AWS Resilience Hub そのロールを引き継ぐためのアクセスを有効にする必要があります。このロールは、AWS アカウント内のリソースを含む別のロールにアクセスするために使用されます。リソースを読み取る権限があってはなりません。

Note

- ロールタイプは、AwsResilienceHubAdminAccountRole である必要があります。
- プライマリアカウントで作成する必要があります。
- 現在の IAM ユーザー/ロールには、このロールを引き受けるiam:assumeRole権限が必要です。
- secondary_account_id_1/2/... を関連するセカンダリアカウント識別子に置き換えます。

以下のポリシーでは、 AWS アカウント内の別のロールのリソースにアクセスするための実行権限をロールに付与します。

```
{
  {
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Resource": [
        "arn:aws:iam::secondary_account_id_1:role/AwsResilienceHubExecutorAccountRole",
        "arn:aws:iam::secondary_account_id_2:role/AwsResilienceHubExecutorAccountRole",
        ...
      ],
      "Action": [
        "sts:AssumeRole"
      ]
```

```
    }
  ]
}
```

管理者ロール (AwsResilienceHubAdminAccountRole) の信頼ポリシーは次のとおりです。

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

セカンダリ/リソースアカウントの設定

このロールを引き受けるには、各セカンダリアカウントで AwsResilienceHubExecutorAccountRole を新規作成し、上記で作成した管理者ロールを有効にする必要があります。このロールはアプリケーションリソースのスキャンと評価に使用されるため、適切な権限も必要です。 AWS Resilience Hub

ただし、AWSResilienceHubAsssessmentExecutionPolicy 管理ポリシーをロールにアタッチし、執行者ロールポリシーをアタッチする必要があります。

執行者ロールの信頼ポリシーは次のとおりです。

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

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

AWS の管理ポリシー AWS Resilience Hub

AWS 管理ポリシーは、によって作成および管理されるスタンドアロンのポリシーです。 AWS AWS 管理ポリシーは、ユーザー、グループ、ロールにアクセス権限を割り当てることができるように、多くの一般的な使用事例にアクセス許可を与えるように設計されています。

AWS 管理ポリシーでは、 AWS すべての顧客が使用できるようになっているため、特定のユースケースでは最小権限のアクセス権限が付与されない場合があることに注意してください。ユースケース別にカスタマーマネージドポリシーを定義して、マネージドポリシーを絞り込むことをお勧めします。

AWS 管理ポリシーで定義されている権限は変更できません。 AWS 管理ポリシーで定義されている権限を更新すると AWS 、その更新はポリシーがアタッチされているすべてのプリンシパル ID (ユーザー、グループ、ロール) に影響します。 AWS AWS 管理ポリシーが更新される可能性が最も高いのは、新しい API 操作が既存のサービスで開始されたときや、新しい API AWS のサービス 操作が使用可能になったときです。

詳細については、「IAM ユーザーガイド」の「AWS マネージドポリシー」を参照してください。

AWSResilienceHubAsssessmentExecutionPolicy

`AWSResilienceHubAsssessmentExecutionPolicy` は IAM ID にアタッチできます。評価の実行中、このポリシーは、 AWS 評価を実行するための他のサービスへのアクセス権限を付与します。

アクセス許可の詳細

このポリシーは、Amazon Simple Storage Service (Amazon S3) AWS FIS バケットにアラームと SOP テンプレートを発行するための適切なアクセス権限を提供します。Amazon S3 バケット名の先頭は`aws-resilience-hub-artifacts-`にする必要があります。別の Amazon S3 バケットに公開したい場合は、`CreateRecommendationTemplate` API を呼び出している間に発行できます。詳細については、「」を参照してください。CreateRecommendationTemplate

このポリシーには、以下の権限が含まれています。

- Amazon CloudWatch (CloudWatch) — CloudWatch アプリケーションを監視するために Amazon で設定した、実装済みのアラームをすべて取得します。さらに、`cloudwatch:PutMetricData` CloudWatch 名前空間内のアプリケーションの耐障害性スコアのメトリクスを公開するためにも使用します`ResilienceHub`。
- Amazon Data Lifecycle Manager — AWS アカウントに関連付けられている Amazon Data Lifecycle Manager `Describe` リソースのアクセス権限を取得および付与します。
- Amazon DevOps Guru — AWS お客様のアカウントに関連付けられている Amazon DevOps Guru リソースを一覧表示し、`Describe`アクセス権限を提供します。
- Amazon DynamoDB (DynamoDB) — AWS アカウントに関連付けられている Amazon DynamoDB リソースの`Describe`権限を一覧表示して提供します。
- Amazon ElastiCache (ElastiCache) — `Describe` ElastiCache AWS アカウントに関連付けられているリソースにアクセス許可を与えます。
- Amazon Elastic Compute Cloud (Amazon EC2) — AWS アカウントに関連付けられている Amazon EC2 リソースの`Describe`権限を一覧表示して提供します。
- Amazon Elastic Container Registry (Amazon ECR) — AWS アカウントに関連付けられている Amazon ECR `Describe` リソースにアクセス権限を提供します。
- Amazon Elastic Container Service (Amazon ECS) — AWS アカウントに関連付けられている Amazon ECS `Describe` リソースにアクセス権限を提供します。
- Amazon Elastic File System (Amazon EFS) — AWS お客様のアカウントに関連付けられている Amazon EFS `Describe` リソースにアクセス権限を提供します。
- Amazon Elastic Kubernetes Service (Amazon EKS) — AWS アカウントに関連付けられている Amazon EKS リソースの`Describe`権限を一覧表示して提供します。
- Amazon EC2 Auto Scaling — AWS アカウントに関連付けられている Amazon EC2 Auto Scaling リソースを一覧表示し、`Describe`アクセス権限を提供します。

- Amazon EC2 Systems Manager (SSM) — AWS アカウントに関連付けられている SSM `Describe` リソースにアクセス権限を提供します。
- Amazon Fault Injection Service (AWS FIS) — `Describe` AWS FIS AWS アカウントに関連付けられている実験と実験テンプレートを一覧表示して許可します。
- Windows ファイルサーバー用 Amazon FSx (Amazon FSx) — お客様のアカウントに関連付けられている Amazon FSx `Describe` リソースに対するアクセス権限を一覧表示して提供します。 AWS
- Amazon RDS — AWS アカウントに関連付けられている Amazon RDS リソースを一覧表示し、`Describe`アクセス権限を提供します。
- Amazon Route 53 (Route 53) — AWS アカウントに関連付けられている Route 53 リソースの `Describe` 権限を一覧表示して提供します。
- Amazon Route 53 Resolver — Amazon Route 53 Resolver AWS アカウントに関連付けられているリソースを一覧表示し、`Describe`アクセス権限を提供します。
- Amazon Simple Notification Service (Amazon SNS) — AWS アカウントに関連付けられている Amazon SNS リソースの`Describe`権限を一覧表示して提供します。
- Amazon Simple Queue Service (Amazon SQS) — AWS アカウントに関連付けられている Amazon SQS リソースの`Describe`権限を一覧表示して提供します。
- Amazon Simple Storage Service (Amazon S3) — AWS アカウントに関連付けられている Amazon S3 リソースの`Describe`権限を一覧表示して提供します。

> **Note**
>
> 評価の実行中に、管理ポリシーから更新する必要のある不足している権限がある場合は、AWS Resilience Hub s3: GetBucketLogging permissions を使用して評価を正常に完了します。ただし、 AWS Resilience Hub 不足している権限を一覧表示する警告メッセージが表示され、その権限を追加するための猶予期間が与えられます。指定した猶予期間内に不足している権限を追加しないと、評価は失敗します。

- AWS Backup — AWS アカウントに関連付けられている Amazon EC2 Auto Scaling `Describe` リソースを一覧表示してアクセス権限を取得します。
- AWS CloudFormation — `Describe` AWS CloudFormation AWS アカウントに関連付けられているスタック上のリソースを一覧表示してアクセス権限を取得します。
- AWS DataSync — AWS DataSync AWS アカウントに関連付けられているリソースを一覧表示し、`Describe`権限を提供します。
- AWS Directory Service — AWS Directory Service AWS アカウントに関連付けられているリソースを一覧表示し、`Describe`権限を提供します。

- AWS Elastic Disaster Recovery (Elastic Disaster Recovery) — AWS アカウントに関連付けられているElastic Disaster `Describe` Recoveryリソースにアクセス権限を付与します。
- AWS Lambda (Lambda) — アカウントに関連付けられている Lambda リソースを一覧表示し、`Describe`アクセス権限を提供します。 AWS
- AWS Resource Groups (Resource Groups) — AWS アカウントに関連付けられているResource Groups を一覧表示し、`Describe`権限を提供します。
- AWS Service Catalog (Service Catalog) — AWS アカウントに関連付けられているService Catalog `Describe` リソースの権限を一覧表示して提供します。
- AWS Step Functions — AWS Step Functions AWS アカウントに関連付けられているリソースを一覧表示し、`Describe`権限を提供します。
- Elastic Load Balancing — AWS アカウントに関連付けられている Elastic Load Balancing `Describe` リソースの権限を一覧表示して提供します。
- `ssm:GetParametersByPath`— この権限を使用して、 CloudWatch アプリケーションに設定されたアラーム、テスト、または SOP を管理します。

AWS 評価の実行中にチームがサービスにアクセスするために必要な権限を付与するユーザー、ユーザーグループ、 AWS およびロールの権限をアカウントに追加するには、以下のIAMポリシーが必要です。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "application-autoscaling:DescribeScalableTargets",
        "autoscaling:DescribeAutoScalingGroups",
        "backup:DescribeBackupVault",
        "backup:GetBackupPlan",
        "backup:GetBackupSelection",
        "backup:ListBackupPlans",
        "backup:ListBackupSelections",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "cloudformation:ValidateTemplate",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
```

```
        "datasync:DescribeTask",
        "datasync:ListLocations",
        "datasync:ListTasks",
        "devops-guru:ListMonitoredResources",
        "dlm:GetLifecyclePolicies",
        "dlm:GetLifecyclePolicy",
        "drs:DescribeJobs",
        "drs:DescribeSourceServers",
        "drs:GetReplicationConfiguration",
        "ds:DescribeDirectories",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListTagsOfResource",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeFastSnapshotRestores",
        "ec2:DescribeFleets",
        "ec2:DescribeHosts",
        "ec2:DescribeInstances",
        "ec2:DescribeNatGateways",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRegions",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcEndpoints",
        "ecr:DescribeRegistry",
        "ecs:DescribeCapacityProviders",
        "ecs:DescribeClusters",
        "ecs:DescribeContainerInstances",
        "ecs:DescribeServices",
        "ecs:DescribeTaskDefinition",
        "ecs:ListContainerInstances",
        "ecs:ListServices",
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeNodegroup",
        "eks:ListFargateProfiles",
        "eks:ListNodegroups",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeGlobalReplicationGroups",
```

```
        "elasticache:DescribeReplicationGroups",
        "elasticache:DescribeSnapshots",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "fis:GetExperimentTemplate",
        "fis:ListExperimentTemplates",
        "fis:ListExperiments",
        "fsx:DescribeFileSystems",
        "lambda:GetFunctionConcurrency",
        "lambda:GetFunctionConfiguration",
        "lambda:ListAliases",
        "lambda:ListVersionsByFunction",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeDBInstances",
        "rds:DescribeDBProxies",
        "rds:DescribeDBProxyTargets",
        "rds:DescribeDBSnapshots",
        "rds:DescribeGlobalClusters",
        "resource-groups:GetGroup",
        "resource-groups:ListGroupResources",
        "route53-recovery-control-config:ListClusters",
        "route53-recovery-control-config:ListControlPanels",
        "route53-recovery-control-config:ListRoutingControls",
        "route53-recovery-readiness:GetReadinessCheckStatus",
        "route53-recovery-readiness:GetResourceSet",
        "route53-recovery-readiness:ListReadinessChecks",
        "route53:GetHealthCheck",
        "route53:ListHealthChecks",
        "route53:ListHostedZones",
        "route53:ListResourceRecordSets",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:ListResolverEndpointIpAddresses",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketTagging",
```

```
        "s3:GetBucketVersioning",
        "s3:GetMultiRegionAccessPointRoutes",
        "s3:GetReplicationConfiguration",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListMultiRegionAccessPoints",
        "servicecatalog:GetApplication",
        "servicecatalog:ListAssociatedResources",
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptionsByTopic",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "ssm:DescribeAutomationExecutions",
        "states:DescribeStateMachine",
        "states:ListStateMachineVersions",
        "states:ListStateMachineAliases",
        "tag:GetResources"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "apigateway:GET"
      ],
      "Resource": [
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/usageplans"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:CreateBucket",
        "s3:PutObject",
        "s3:GetObject"
      ],
      "Resource": "arn:aws:s3:::aws-resilience-hub-artifacts-*"
    },
    {
      "Effect": "Allow",
      "Action": [
```

```
        "cloudwatch:PutMetricData"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "cloudwatch:namespace": "ResilienceHub"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "ssm:GetParametersByPath"
      ],
      "Resource": "arn:aws:ssm:*:*:parameter/ResilienceHub/*"
    }
  ]
}
```

AWS Resilience Hub 管理ポリシーの更新 AWS

AWS AWS Resilience Hub このサービスが変更の追跡を開始してからの管理ポリシーの更新に関する詳細が表示されます。このページへの変更に関する自動通知を受け取るには、 AWS Resilience Hub ドキュメント履歴ページの RSS フィードを購読してください。

変更	説明	日付
AWSResilienceHubAssessmentExecutionPolicy— Windows ファイルサーバー用 Amazon FSx AWS Resilience Hub のサポートを拡張します。	AWS Resilience Hub このポリシーにより、Windows 用 Amazon FSx ファイルサーバーの設定を読み取ることができます。	2024 年 3 月 26 日
AWSResilienceHubAssessmentExecutionPolicy— AWS Resilience Hub のサポートを拡張します。 AWS Step Functions	AWS Resilience Hub このポリシーでは、 AWS Step Functions 設定を読み取ることができます。	2023 年 10 月 30 日

変更	説明	日付
AWSResilienceHubAssessmentExecutionPolicy—Amazon Relational Database Service (Amazon RDS) AWS Resilience Hub のサポートを改善します。	AWS Resilience Hub このポリシーにより、評価の実行中に Amazon RDS のリソースにアクセスできます。	2023 年 10 月 5 日
AWSResilienceHubAssessmentExecutionPolicy - 新しいポリシー	AWS Resilience Hub このポリシーは、 AWS 評価を実施するための他のサービスへのアクセスを提供します。	2023 年 6 月 26 日
AWS Resilience Hub 変更の追跡を開始しました。	AWS Resilience Hub AWS 管理ポリシーの変更の追跡を開始しました。	2023 年 6 月 15 日

Terraform ステートファイルをにインポート中 AWS Resilience Hub

AWS Resilience Hub Amazon シンプルストレージサービスのマネージドキー (SSE-S3) またはマネージドキー (SSE-KMS) を使用してサーバー側暗号化 (SSE) を使用して暗号化された Terraform ステートファイルのインポートをサポートします。 AWS Key Management Service Terraform ステートファイルがお客様が用意した暗号化キー (SSE-C) を使用して暗号化されている場合、 AWS Resilience Hubを使用してインポートすることはできません。

Terraform ステートファイルをにインポートするには、ステートファイルの場所に応じて次の IAM AWS Resilience Hub ポリシーが必要です。

プライマリアカウントにある Amazon S3 バケットから Terraform ステートファイルをインポートする

プライマリアカウントの Amazon S3 バケットにある Terraform ステータスファイルへの読み取りアクセスを AWS Resilience Hub に許可するには、以下の Amazon S3 バケットポリシーと IAM ポリシーが必要です。

- バケットポリシー — プライマリアカウントにあるターゲット Amazon S3 バケットのバケットポリシー。詳細については、次の例を参照してください。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<primary-account>:role/<invoker-role-or-current-iam-
role>"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::<s3-bucket-name>/<path-to-state-file>"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<primary-account>:role/<invoker-role-or-current-iam-
role>"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::<s3-bucket-name>"
    }
  ]
}
```

- ID ポリシー — このアプリケーションに定義されている Invoker ロール、 AWS またはプライマリアカウントの現在の IAM ロールに関連するアイデンティティポリシー。 AWS Resilience Hub AWS 詳細については、次の例を参照してください。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::<s3-bucket-name>/<path-to-state-file>"
    },
    {
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::<s3-bucket-name>"
    }
  ]
```

```
}
```

> **Note**
>
> AWSResilienceHubAsssessmentExecutionPolicy管理ポリシーを使用している場合、ListBucket権限は必要ありません。

> **Note**
>
> Terraform ステートファイルが KMS を使用して暗号化されている場合は、次のkms:Decrypt権限を追加する必要があります。
>
> ```
> {
>       "Effect": "Allow",
>       "Action": [
>               "kms:Decrypt",
>       ],
>       "Resource": "<arn_of_kms_key>"
> }
> ```

セカンダリアカウントにある Amazon S3 バケットから Terraform ステートファイルをインポートする

- バケットポリシー — 1 つのセカンダリアカウントにあるターゲット Amazon S3 バケットのバケットポリシー。詳細については、次の例を参照してください。

```
 {
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<primary-account>:role/<invoker-role-or-current-iam-
role>"
      },
      "Action": "s3:GetObject",
```

```
      "Resource": "arn:aws:s3:::<bucket-with-statefile-in-secondary-account>/<path-
to-state-file>"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<primary-account>:role/<invoker-role-or-current-iam-
role>"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::<bucket-with-statefile-in-secondary-account>"
    }
  ]
}
```

- ID ポリシー — AWS Resilience Hub プライマリアカウントで実行される、 AWS アカウントロールに関連付けられた ID ポリシー。 AWS 詳細については、次の例を参照してください。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<primary-account>:role/<invoker-role-or-current-iam-
role>"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::<bucket-with-statefile-in-secondary-account>/<path-
to-state-file>"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<primary-account>:role/<invoker-role-or-current-iam-
role>"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::<bucket-with-statefile-in-secondary-account>"
    }
  ]
}
```

> **Note**
>
> AWSResilienceHubAsssessmentExecutionPolicy管理ポリシーを使用している場合、ListBucket権限は必要ありません。

> **Note**
>
> Terraform ステートファイルが KMS を使用して暗号化されている場合は、次のkms:Decrypt権限を追加する必要があります。

```
{
      "Effect": "Allow",
      "Action": [
              "kms:Decrypt",
      ],
      "Resource": "<arn_of_kms_key>"
}
```

Amazon Elastic Kubernetes Service AWS Resilience Hub スクラスターへのアクセスを有効にする

AWS Resilience Hub Amazon Elastic Kubernetes Service S クラスターのインフラストラクチャを分析することにより、Amazon EKS クラスターの耐障害性を評価します。 AWS Resilience Hub Kubernetes のロールベースアクセスコントロール (RBAC) 設定を使用して、Amazon EKS クラスターの一部としてデプロイされている他の Kubernetes (K8s) ワークロードを評価します。Amazon EKS AWS Resilience Hub クラスターをクエリしてワークロードの分析と評価を行うには、以下を完了する必要があります。

- Amazon EKS クラスターと同じアカウントで既存の AWS Identity and Access Management (IAM) ロールを作成または使用します。
- IAM ユーザーとロールが Amazon EKS クラスターにアクセスできるようにし、Amazon EKS クラスター内の K8s リソースに追加の読み取り専用アクセス権限を付与します。Amazon EKS クラス

ターへの IAM ユーザーとロールのアクセスを有効にする方法の詳細については、「クラスターへの IAM ユーザーとロールのアクセスを有効にする - Amazon EKS」を参照してください。

IAM エンティティを使用した Amazon EKS クラスターへのアクセスは、Amazon EKS コントロールプレーンで実行されるAWS IAM Authenticator for Kubernetes によって有効になります。オーセンティケーターは、その設定情報を `aws-auth ConfigMap` から取得します。

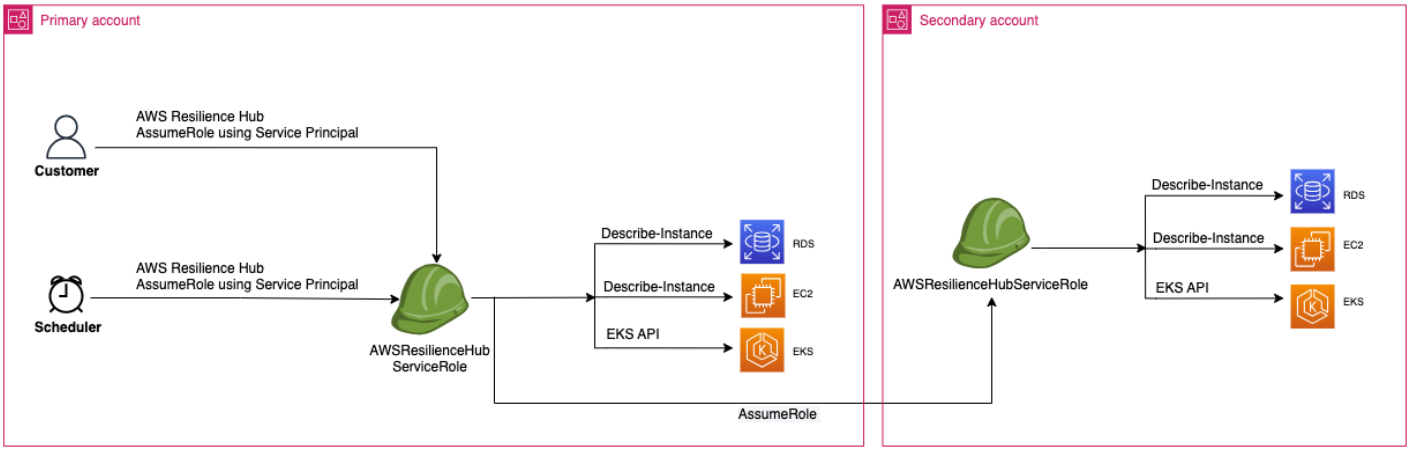
> **Note**
>
> - すべての設定の詳細については、の「`aws-auth ConfigMap`フル設定フォーマット」を参照してください。 GitHub
> - さまざまな IAM アイデンティティの詳細については、IAM ユーザーガイドの「アイデンティティ (ユーザー、グループ、ロール)」を参照してください。
> - Kubernetes のロールベースアクセスコントロール (RBAC) 設定の詳細については、「RBAC 認可の使用」を参照してください。

AWS Resilience Hub アカウントの IAM ロールを使用して Amazon EKS クラスター内のリソースをクエリします。Amazon EKS AWS Resilience Hub クラスター内のリソースにアクセスするには、が使用する IAM ロールを、Amazon EKS クラスター内のリソースへの十分な読み取り専用アクセス権限を持つ Kubernetes AWS Resilience Hub グループにマップする必要があります。

AWS Resilience Hub 次の IAM ロールオプションのいずれかを使用して Amazon EKS クラスターリソースにアクセスできます。

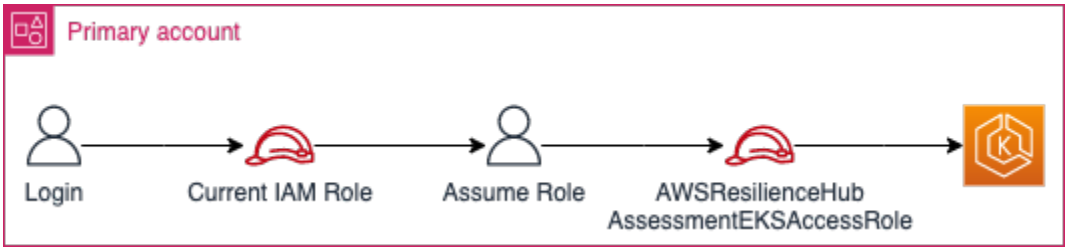
- リソースへのアクセスにロールベースのアクセスを使用するようにアプリケーションが設定されている場合、アプリケーションの作成中に AWS Resilience Hub に渡された呼び出しロールまたはセカンダリアカウントロールは、評価時に Amazon EKS クラスターにアクセスするために使用されます。

  次の概念図は、アプリケーションがロールベースのアプリケーションとして設定されている場合に Amazon AWS Resilience Hub EKS クラスターにアクセスする方法を示しています。

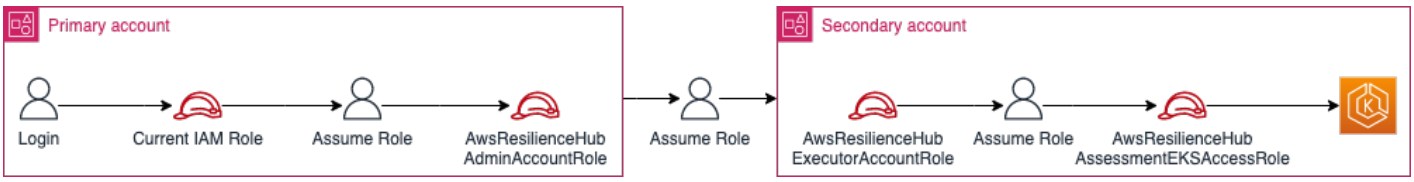


- 現在の IAM ユーザーを使用してリソースにアクセスするようにアプリケーションが設定されている場合、Amazon EKS クラスターと同じアカウントに`AwsResilienceHubAssessmentEKSAccessRole`という名前の新しい IAM ロールを作成する必要があります。その後、この IAM ロールは Amazon EKS クラスターへのアクセスに使用されます。

  次の概念図は、アプリケーションが現在の IAM ユーザー権限を使用するように設定されている場合に、プライマリアカウントにデプロイされた Amazon AWS Resilience Hub EKS クラスターにアクセスする方法を示しています。



  次の概念図は、アプリケーションが現在の IAM ユーザー権限を使用するように設定されている場合に、セカンダリアカウントにデプロイされた Amazon AWS Resilience Hub EKS クラスターにアクセスする方法を示しています。



Amazon EKS AWS Resilience Hub クラスター内のリソースへのアクセス権の付与

AWS Resilience Hub 必要な権限を設定していれば、Amazon EKS クラスターにあるリソースにアクセスできます。

Amazon EKS クラスター内のリソースの検出と評価に必要なアクセス権限を付与するには AWS Resilience Hub

1. Amazon EKS クラスターにアクセスするための IAM ロールを設定します。

   ロールベースのアクセスを使用してアプリケーションを設定した場合は、このステップをスキップしてステップ 2 に進み、アプリケーションの作成に使用したロールを使用できます。 AWS Resilience Hub でこの IAM ロールを使用する方法については、the section called “AWS レジリエンスハブと IAM の連携の仕組み” を参照してください。

   現在の IAM ユーザー権限を使用してアプリケーションを設定した場合は、Amazon EKS クラスターと同じアカウントで `AwsResilienceHubAssessmentEKSAccessRole` IAM ロールを作成する必要があります。その後、この IAM ロールは Amazon EKS クラスターにアクセスする際に使用されます。

   アプリケーションをインポートして評価する際、IAM AWS Resilience Hub ロールを使用して Amazon EKS クラスター内のリソースにアクセスします。このロールは Amazon EKS クラスターと同じアカウントで作成する必要があります。また、Amazon EKS クラスターの評価に必要なアクセス権限を含む Kubernetes グループにマッピングされます AWS Resilience Hub 。

   Amazon EKS AWS Resilience Hub クラスターが呼び出し元アカウントと同じアカウントにある場合、ロールは次の IAM 信頼ポリシーを使用して作成する必要があります。この IAM 信頼ポリシーでは、`caller_IAM_role`が現在のアカウントで API を呼び出すために使用されます。 AWS Resilience Hub

   > **Note**
   >
   > `caller_IAM_role` AWS はユーザーアカウントに関連付けられているロールです。

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

```
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::eks_cluster_account_id:role/caller_IAM_role"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Amazon EKS クラスターがクロスアカウント (AWS Resilience Hub 呼び出し元アカウントとは異なるアカウント) にある場合は、次の AwsResilienceHubAssessmentEKSAccessRole IAM 信頼ポリシーを使用して IAM ロールを作成する必要があります。

> **Note**
>
> 前提条件として、 AWS Resilience Hub ユーザーのアカウントとは別のアカウントにデプロイされている Amazon EKS クラスターにアクセスするには、マルチアカウントアクセスを設定する必要があります。詳細については、以下を参照してください。

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

2. ClusterRoleアプリケーションのロールと ClusterRoleBinding (またはRoleBinding) ロールを作成します。 AWS Resilience Hub

   Amazon ClusterRoleBinding EKS クラスター内の特定の名前空間に含まれるリソースを分析および評価するために必要な読み取り専用アクセス権限を作成しClusterRole、付与します。 AWS Resilience Hub

AWS Resilience Hub 以下のいずれかを完了することで、耐障害性評価を生成するための名前空間へのアクセスを制限できます。

a. すべての名前空間の読み取りアクセス権を AWS Resilience Hub アプリケーションに付与します。

Amazon EKS AWS Resilience Hub クラスター内のすべての名前空間におけるリソースの耐障害性を評価するには、次のとを作成する必要があります。`ClusterRole` `ClusterRoleBinding`

- `resilience-hub-eks-access-cluster-role`(`ClusterRole`) — Amazon EKS AWS Resilience Hub クラスターを評価するために必要なアクセス権限を定義します。
- `resilience-hub-eks-access-cluster-role-binding` (`ClusterRoleBinding`) — Amazon EKS クラスターに `resilience-hub-eks-access-group` という名前のグループを定義し、そのユーザーに AWS Resilience Hubで障害耐性評価を実行するために必要なアクセス権限を付与します。

すべての名前空間の読み取りアクセスを AWS Resilience Hub アプリケーションに付与するテンプレートは次のとおりです。

```
cat << EOF | kubectl apply -f -
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: resilience-hub-eks-access-cluster-role
rules:
- apiGroups:
    - ""
  resources:
    - pods
    - replicationcontrollers
    - nodes
  verbs:
    - get
    - list
- apiGroups:
    - apps
  resources:
    - deployments
```

```
    - replicasets
  verbs:
    - get
    - list
- apiGroups:
    - policy
  resources:
    - poddisruptionbudgets
  verbs:
    - get
    - list
- apiGroups:
    - autoscaling.k8s.io
  resources:
    - verticalpodautoscalers
  verbs:
    - get
    - list
- apiGroups:
    - autoscaling
  resources:
    - horizontalpodautoscalers
  verbs:
    - get
    - list
- apiGroups:
    - karpenter.sh
  resources:
    - provisioners
  verbs:
    - get
    - list
- apiGroups:
    - karpenter.k8s.aws
  resources:
    - awsnodetemplates
  verbs:
    - get
    - list
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: resilience-hub-eks-access-cluster-role-binding
```

```
subjects:
  - kind: Group
    name: resilience-hub-eks-access-group
    apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
  name: resilience-hub-eks-access-cluster-role
  apiGroup: rbac.authorization.k8s.io
---
EOF
```

b. AWS Resilience Hub 特定の名前空間を読み取るためのアクセス権を付与します。

を使用して、 AWS Resilience Hub 特定の名前空間セット内のリソースへのアクセスを制限できます。RoleBindingこれを実現するには、次のロールを作成する必要があります。

- ClusterRole— Amazon EKS クラスター内の特定の名前空間のリソースにアクセスし、その耐障害性を評価するには、次のロールを作成する必要があります。 AWS Resilience Hub ClusterRole
  - resilience-hub-eks-access-cluster-role— 特定の名前空間内のリソースを評価するために必要な権限を指定します。
  - resilience-hub-eks-access-global-cluster-role— Amazon EKS クラスター内の特定の名前空間に関連付けられていない、クラスタースコープのリソースを評価するために必要なアクセス権限を指定します。 AWS Resilience Hub アプリケーションの耐障害性を評価するには、Amazon EKS クラスター上のクラスタースコープのリソース (ノードなど) にアクセスする権限が必要です。

  ClusterRoleロールを作成するためのテンプレートは次のとおりです。

```
cat << EOF | kubectl apply -f -
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: resilience-hub-eks-access-cluster-role
rules:
  - apiGroups:
      - ""
    resources:
      - pods
      - replicationcontrollers
```

```
    verbs:
      - get
      - list
  - apiGroups:
      - apps
    resources:
      - deployments
      - replicasets
    verbs:
      - get
      - list
  - apiGroups:
      - policy
    resources:
      - poddisruptionbudgets
    verbs:
      - get
      - list
  - apiGroups:
      - autoscaling.k8s.io
    resources:
      - verticalpodautoscalers
    verbs:
      - get
      - list
  - apiGroups:
      - autoscaling
    resources:
      - horizontalpodautoscalers
    verbs:
      - get
      - list

---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: resilience-hub-eks-access-global-cluster-role
rules:
  - apiGroups:
      - ""
    resources:
      - nodes
    verbs:
```

```
      - get
      - list
  - apiGroups:
      - karpenter.sh
    resources:
      - provisioners
    verbs:
      - get
      - list
  - apiGroups:
      - karpenter.k8s.aws
    resources:
      - awsnodetemplates
    verbs:
      - get
      - list

---
EOF
```

- RoleBindingロール — このロールは、 AWS Resilience Hub 特定の名前空間内のリソースにアクセスするために必要なアクセス権限を付与します。つまり、RoleBinding各名前空間にロールを作成して、 AWS Resilience Hub 特定の名前空間内のリソースにアクセスできるようにする必要があります。

  > **Note**
  >
  > ClusterAutoscalerを自動スケーリングに使用する場合は、kube-systemに追加でRoleBindingを作成する必要があります。これは、kube-system名前空間の一部であるClusterAutoscalerを評価するために必要です。
  > これにより、Amazon EKS AWS Resilience Hub kube-system クラスターを評価する際に名前空間内のリソースを評価するために必要なアクセス権限が付与されます。

  RoleBindingロールを作成するためのテンプレートは次のとおりです。

```
cat << EOF | kubectl apply -f -
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
```

```
metadata:
  name: resilience-hub-eks-access-cluster-role-binding
  namespace: <namespace>
subjects:
  - kind: Group
    name: resilience-hub-eks-access-group
    apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
  name: resilience-hub-eks-access-cluster-role
  apiGroup: rbac.authorization.k8s.io

---
EOF
```

- ClusterRoleBindingロール — このロールは、 AWS Resilience Hub クラスタースコープのリソースにアクセスするために必要なアクセス権限を付与します。

  ClusterRoleBindingロールを作成するためのテンプレートは次のとおりです。

```
cat << EOF | kubectl apply -f -
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: resilience-hub-eks-access-global-cluster-role-binding
subjects:
  - kind: Group
    name: resilience-hub-eks-access-group
    apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
  name: resilience-hub-eks-access-global-cluster-role
  apiGroup: rbac.authorization.k8s.io

---
EOF
```

3. aws-auth ConfigMapを更新して、Amazon EKS クラスターへのアクセスに使用される IAM ロールでresilience-hub-eks-access-groupをマップします。

このステップでは、ステップ 1 で使用した IAM ロールとステップ 2 で作成した Kubernetes グループとのマッピングを作成します。このマッピングは、Amazon EKS クラスター内のリソースにアクセスするためのアクセス権限を IAM ロールに付与します。

> **Note**
>
> - ROLE-NAME はAmazon EKS クラスターへのアクセスに使用される IAM ロールを指します。
>   - アプリケーションがロールベースのアクセスを使用するように設定されている場合、ロールはアプリケーションの作成時に渡される呼び出し側ロールまたはセカンダリアカウントロールのいずれかである必要があります。 AWS Resilience Hub
>   - アプリケーションがリソースへのアクセスに、現在の IAM ユーザーを使用するように構成されている場合、それはAwsResilienceHubAssessmentEKSAccessRoleである必要があります。
> - ACCOUNT-IDAmazon EKS AWS クラスターのアカウント ID である必要があります。

次のいずれかの方法で aws-auth ConfigMap を作成できます。

- eksctl を使用する

  次のコマンドを実行して aws-auth ConfigMap を更新します。

  ```
  eksctl create iamidentitymapping \
   --cluster <cluster-name> \
   --region=<region-code> \
   --arn arn:aws:iam::<ACCOUNT-ID>:role/<ROLE-NAME>\
   --group resilience-hub-eks-access-group \
   --username AwsResilienceHubAssessmentEKSAccessRole
  ```

- データ下の ConfigMap の mapRoles セクションに IAM ロールの詳細を追加することで、aws-auth ConfigMap を手動で編集できます。次のコマンドを使用して、aws-auth ConfigMap を編集します。

  ```
  kubectl edit -n kube-system configmap/aws-auth
  ```

  mapRoles セクションは次のパラメータで構成されます。

- `rolearn` - 追加される IAM ロールの Amazon リソースネーム (ARN)。
  - ARN 構文 — `arn:aws:iam::<ACCOUNT-ID>:role/<ROLE-NAME>`。
- `username` — IAM ロール `AwsResilienceHubAssessmentEKSAccessRole` にマップされる Kubernetes 内のユーザー名。
- `groups`— グループ名はステップ 2 (`resilience-hub-eks-access-group`) で作成したグループ名と一致する必要があります。

> **Note**
>
> `mapRoles`セクションが存在しない場合は、このセクションを手動で追加する必要があります。

以下のテンプレートを使用して IAM ロールの詳細をデータ下の`ConfigMap`の `mapRoles` セクションに追加します。

```
- groups:
  - resilience-hub-eks-access-group
  rolearn: arn:aws:iam::<ACCOUNT-ID>:role/<ROLE-NAME>
  username: AwsResilienceHubAssessmentEKSAccessRole
```

Amazon AWS Resilience Hub 簡易通知サービストピックへの公開を有効にする

このセクションでは、 AWS Resilience Hub アプリケーションに関する通知を Amazon Simple Notification Service (Amazon SNS) トピックに発行できるようにする方法について説明します。Amazon SNS トピックに通知をプッシュするには、次のものが揃っていることを確認します。

- AWS Resilience Hub アクティブなアプリケーション。
- AWS Resilience Hub 通知を送信する必要がある既存の Amazon SNS トピック。Amazon SNS トピックの作成の詳細については、「Amazon SNS トピックの作成」を参照してください。

Amazon SNS AWS Resilience Hub トピックに通知を発行できるようにするには、Amazon SNS トピックのアクセスポリシーを次のように更新する必要があります。

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowResilienceHubPublish",
      "Effect": "Allow",
      "Principal": {
        "Service": "resiliencehub.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:account-id:topic-name"
    }
  ]
}
```

> **Note**
>
> AWS Resilience Hub を使用して、デフォルトで有効になっているリージョンにあるトピックにオプトインリージョンからメッセージを発行する場合、Amazon SNS トピック用に作成されたリソースポリシーを変更する必要があります。プリンシパルの値を `resiliencehub.amazonaws.com` から `resiliencehub.<opt-in-region>.amazonaws.com` に変更します。

サーバー側暗号化 (SSE) の Amazon SNS トピックを使用している場合は、 AWS Resilience Hub が Amazon SNS 暗号化キーへの `Decrypt` および `GenerateDataKey*` アクセス権を持っていることを確認する必要があります。

`DecryptGenerateDataKey*`を提供してアクセスするには AWS Resilience Hub、 AWS Key Management Service 以下のアクセス権限ポリシーを含める必要があります。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowResilienceHubDecrypt",
      "Effect": "Allow",
      "Principal": {
        "Service": "resiliencehub.amazonaws.com"
      },
      "Action": [
        "kms:GenerateDataKey*",
```

```
        "kms:Decrypt"
      ],
      "Resource": "arn:aws:kms:region:account-id:key/key-id"
    }
  ]
}
```

AWS Resilience Hub 権限を制限してレコメンデーションを含めたり除外したりします。

AWS Resilience Hub アプリケーションごとにレコメンデーションを含めたり除外したりする権限を制限できます。次の IAM 信頼ポリシーを使用して、アプリケーションごとに推奨事項を含めたり除外したりする権限を制限できます。この IAM 信頼ポリシーでは、現在のアカウントで `caller_IAM_role` (AWS ユーザーアカウントに関連付けられている) を使用して API を呼び出します。 AWS Resilience Hub

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "resiliencehub:BatchUpdateRecommendationStatus",
      "Resource": "arn:aws:resiliencehub:us-west-2:12345678900:app/0e6237b7-23ba-4103-
adb2-91811326b703"
    }
  ]
}
```

のインフラストラクチャー・ セキュリティ AWS Resilience Hub

マネージド型サービスとして、 AWS Resilience Hub 「Amazon Web Services: セキュリティプロセスの概要」 AWS ホワイトペーパーに記載されているグローバルネットワークセキュリティ手順によって保護されています。

AWS 公開されている API AWS Resilience Hub 呼び出しを使用してネットワーク経由でアクセスします。クライアントは、Transport Layer Security (TLS) 1.2 以降をサポートする必要があります。TLS 1.3 以降が推奨されます。また、一時的ディフィー・ ヘルマン Ephemeral Diffie-Hellman (DHE) や Elliptic Curve Ephemeral Diffie-Hellman (ECDHE) などの Perfect Forward Secrecy (PFS)

を使用した暗号スイートもクライアントでサポートされている必要があります。これらのモードは、Java 7 以降など、最近のほとんどのシステムでサポートされています。

また、リクエストには、アクセスキー ID と、IAM プリンシパルに関連付けられているシークレットアクセスキーを使用して署名する必要があります。または、AWS Security Token ServiceAWS STS を使用して、一時的なセキュリティ認証情報を生成し、リクエストに署名することもできます。

他の サービスでの使用

このセクションでは、 AWS と相互作用するサービスについて説明します AWS Resilience Hub。

トピック

- AWS CloudFormation
- AWS CloudTrail
- AWS Systems Manager
- AWS Trusted Advisor

AWS CloudFormation

AWS Resilience Hub は、リソースとインフラストラクチャの作成と管理の所要時間を短縮できるように AWS リソースをモデル化して設定するためのサービスである AWS CloudFormation と統合されています。必要なすべてのAWS リソース (AWS:: ResilienceHub:: ResilienceHub:: ResiliencyHub::: App など) を説明するテンプレートを作成し、AWS CloudFormation はそれらのリソースをプロビジョニングして設定します。

AWS CloudFormation を使用すると、テンプレートを再利用して AWS Resilience Hub リソースを同じように繰り返してセットアップできます。リソースを一度記述すると、同じリソースを複数の AWS アカウントおよびリージョンで何度でも繰り返してプロビジョニングできます。

AWS Resilience Hub および AWS CloudFormation のテンプレート

AWS Resilience Hub および関連サービスのリソースをプロビジョニングして設定するには、AWS CloudFormation テンプレートについて理解しておく必要があります。テンプレートは、JSON またはYAMLでフォーマットされたテキストファイルです。これらのテンプレートには、AWS CloudFormation スタックにプロビジョニングしたいリソースを記述します。JSON や YAML に不慣れな方は、AWS CloudFormation デザイナー を使えば、AWS CloudFormation テンプレートを使いこなすことができます。詳細については、「AWS CloudFormation ユーザーガイド」の「AWS CloudFormation デザイナー とは」を参照してください。

AWS Resilience Hub はAWS CloudFormation での AWS:: レジリエンスハブ:: レジリエンスポリシーと AWS:: レジリエンスハブ::: アプリケーションの作成をサポートします。AWS::ResilienceHub:::ResiliencyPolicyとAWS::ResilienceHub:::AppのJSONとYAMLテンプレー

トの例を含む詳細については、AWS CloudFormation ユーザーガイドのAWS Resilience Hub リソースタイプのリファレンスを参照してください。

AWS CloudFormationスタックを使用してAWS Resilience Hub アプリケーションを定義できます。関連リソースは単一のユニットとして管理できます。ウェブサーバーやネットワークルールなど、ウェブアプリケーションの実行に必要なすべてのリソースをスタックに格納できます。

AWS CloudFormation の詳細情報

AWS CloudFormation の詳細については、次のリソースを参照してください。

- AWS CloudFormation
- AWS CloudFormation ユーザーガイド
- AWS CloudFormation API リファレンス
- AWS CloudFormation コマンドラインインターフェイスユーザーガイド

AWS CloudTrail

AWS Resilience Hub ユーザー AWS CloudTrail、ロール、 AWS またはサービスが実行したアクションの記録を提供するサービスと統合されています AWS Resilience Hub。 CloudTrail すべての API AWS Resilience Hub 呼び出しをイベントとしてキャプチャします。キャプチャされる呼び出しには、 AWS Resilience Hub コンソールからの呼び出しと AWS Resilience Hub API オペレーションへのコード呼び出しが含まれます。証跡を作成すると、Amazon S3 CloudTrail バケットへのイベント (のイベントを含む) の継続的な配信を有効にできます AWS Resilience Hub。証跡を設定しなくても、 CloudTrail コンソールの [イベント履歴] で最新のイベントを確認できます。によって収集された情報を使用して CloudTrail、要求の送信元 IP アドレス AWS Resilience Hub、要求の実行者、実行日時、その他の詳細情報を確認できます。

詳細については CloudTrail、『AWS CloudTrail ユーザーガイド』を参照してください。

AWS Systems Manager

AWS Resilience Hub は Systems Manager と連携して、SOP の基礎として使用できる多数の SSM ドキュメントを提供することで、SOP の手順を自動化します。

AWS Resilience Hub には、さまざまな Systems Manager ドキュメントを実行するために必要な IAM AWS CloudFormation ロールを含むテンプレートが用意されています。ドキュメントごとに 1 つのロールと、特定のドキュメントに必要な権限が付与されます。 AWS CloudFormation テンプ

レートを使用してスタックを作成すると、IAM ロールを設定し、Systems Manager 自動化ドキュメント用のメタデータを Systems Manager パラメータに保存して、さまざまな復旧手順で実行します。

SOP の使い方については、標準操作手順を参照してください。

AWS Trusted Advisor

AWS Trusted Advisor は、導入の特定、優先順位付け、 AWS 最適化に役立つベストプラクティスの推奨事項をまとめたものです。 AWS AWS Trusted Advisor AWS お客様の環境を検査し、コストの節約、システムの可用性とパフォーマンスの向上、またはセキュリティギャップの解消に役立つ機会があれば、チェックを通じて推奨事項を提示します。これらのチェックは、目的に応じて複数のカテゴリに分類されます。チェックインのさまざまなカテゴリについて詳しくは AWS Trusted Advisor、『AWS Supportユーザーガイド』を参照してください。

AWS Trusted Advisor AWS Resilience Hub 耐障害性カテゴリに属する各アプリケーションの耐障害性チェックを通じて、複数の高レベルの耐障害性推奨事項を提供します。耐障害性カテゴリには、アプリケーションをテストして耐障害性と信頼性を判断するすべてのチェックが一覧表示されます。これらのチェックは、 AppComponent 耐障害性リスクを引き起こし、事業継続のためのアプリケーションの可用性に影響を与える可能性のある障害やポリシー違反が発生した場合に警告します。また、「推奨処置」セクションには、これらのリスクを軽減できる可能性を高めるための耐障害性に関する推奨事項も記載されています。これについては、で説明します。 AWS Resilience Hubに記載されている各アプリケーションの推奨事項について詳しくは AWS Trusted Advisor、に記載されている詳細な推奨事項を参照することをお勧めします。 AWS Resilience Hub

AWS Trusted Advisor 内の各アプリケーションについて次のチェックを行います AWS Resilience Hub。

- AWS Resilience Hub アプリケーションレジリエンススコア — AWS Resilience Hub アプリケーションのレジリエンススコアを最新の評価からチェックし、レジリエンススコアが特定の値を下回っている場合は警告します。

  アラート基準

  - 緑 — アプリケーションの耐障害性スコアが 70 以上であることを示します。
  - 黄色 — アプリケーションの耐障害性スコアが 40 ~ 69 であることを示します。
  - 赤 — アプリケーションの耐障害性スコアが 40 未満であることを示します。

  推奨処置

耐障害性を改善し、アプリケーションの耐障害性スコアを可能な限り高めるには、アプリケーションリソースの最新バージョンを使用して評価を実施し、該当する場合は、推奨運用上の推奨事項を実施してください。評価の実行、見直し、実装、運用上の推奨事項の見直しと追加/除外、および実施の詳細については、以下のトピックを参照してください。

- the section called “障害耐性評価の実行”
- the section called “評価レポートのレビュー”
- the section called “障害耐性に関する推奨事項の確認”
- the section called “運用上の推奨事項を含めるまたは除外する”

- AWS Resilience Hub アプリケーションポリシー違反 — AWS Resilience Hub アプリケーションがアプリケーションに設定した RTO と RPO の目標を達成しているかどうかを確認し、アプリケーションが RTO と RPO の目標を達成していない場合は警告します。

  アラート基準

  - 緑 — アプリケーションにポリシーがあり、推定ワークロード RTO と推定ワークロード RPO が RTO と RPO の目標を達成していることを示します。
  - 黄色 — アプリケーションにポリシーがあり、評価されていないことを示します。
  - 赤 — アプリケーションにポリシーがあり、推定作業負荷 RTO と推定作業負荷 RPO が RTO と RPO の目標を達成していないことを示します。

  推奨処置

  アプリケーションの推定ワークロード RTO と推定ワークロード RPO が、定義されている RTO と RPO の目標を引き続き満たすようにするには、アプリケーションリソースの最新バージョンを使用して定期的に評価を実施してください。さらに、アプリケーションの耐障害性ポリシーに違反していないことを確認したい場合は、評価レポートを確認して、推奨されている耐障害性に関する推奨事項を実施することをお勧めします。 AWS Resilience Hub ユーザーに代わって日常的に評価を実施できるようにすること、評価を実施すること、耐障害性に関する推奨事項を検討すること、およびそれらを実施することについて詳しくは、以下のトピックを参照してください。

  - the section called “アプリケーションリソースの表示”(AWS Resilience Hub ユーザーに代わって毎日評価を実行できるようにするには、「アプリケーションの耐障害性ドリフト検出を更新するには」の手順を実行して、「このアプリケーションを毎日自動的に評価する」チェックボックスをオンにしてください)。
  - the section called “障害耐性評価の実行”
  - the section called “評価レポートのレビュー”

  - the section called “障害耐性に関する推奨事項の確認”
  - the section called “運用上の推奨事項を含めるまたは除外する”
- AWS Resilience Hub アプリケーション評価期間 — 内の各アプリケーションについて、最後に評価を実行してからの経過時間をチェックします。 AWS Resilience Hubこのチェックでは、指定した日数の間評価を実行していない場合に警告を表示します。

  アラート基準

  - 緑 — 過去 30 日間にアプリケーションの評価を実行したことを示します。
  - 黄色 — 過去 30 日間にアプリケーションの評価を実施していないことを示します。

  推奨処置

  定期的に評価を実施して、アプリケーションの耐障害性を管理および改善してください。 AWS ユーザーに代わってアプリケーションを日常的に評価したい場合は AWS Resilience Hub 、 AWS Resilience Hub レジリエンシードリフト検出の [このアプリケーションを毎日自動的に評価する] チェックボックスをオンにすることで有効にできます。「このアプリケーションを毎日自動的に評価する」チェックボックスをオンにするには、の「アプリケーションの耐障害性ドリフト検出を更新するには」の手順を実行します。???

  > **Note**
  >
  > このチェックでは、少なくとも 1 回評価されたアプリケーションのみの評価期間を決定します。 AWS Resilience Hub

- AWS Resilience Hub アプリケーションコンポーネントチェック — アプリケーション内のアプリケーションコンポーネント (AppComponent) が回復不能かどうかをチェックします。つまり、AppComponent 障害発生時に回復しないと、未知のデータ損失やシステムダウンタイムが発生する可能性があります。アラート基準が赤に設定されている場合は、 AppComponent が回復不能であることを示しています。

  推奨処置

  回復可能であることを確認するには、耐障害性に関する推奨事項を確認して実装し、新しい評価を実施してください AppComponent 。耐障害性に関する推奨事項の見直しについて詳しくは、を参照してください。the section called “障害耐性に関する推奨事項の確認”

の使用について詳しくは AWS Trusted Advisor、『AWS Supportユーザーガイド』を参照してください。

AWS Resilience Hub ユーザーガイドのドキュメント履歴

次の表は、本リリースのドキュメントをまとめたものです。 AWS Resilience Hub

- API バージョン: 最新
- ドキュメントの最新更新日:2024 年 3 月 28 日

変更	説明	日付
AWS Trusted Advisor 機能強化	AWS Resilience Hub は、回復不可能なアプリケーションコンポーネントを識別するチェック () AWS Trusted Advisor を追加することでサポートを拡張しました。AppComponents 詳細については、「the section called “AWS Trusted Advisor”」を参照してください。	2024 年 3 月 28 日
AWS Resilience Hub 推奨アラームのサポートを拡張します。	AWS Resilience Hub `README.md` テンプレートファイルが更新され、 AWS Resilience Hub 内部 AWS （ Amazonなど CloudWatch ） AWSまたは外部が推奨するアラームを作成できる値が追加されました。 詳細については、「the section called “アラームの管理”」を参照してください。	2024 年 3 月 26 日

AWS Resilience Hub Windows ファイルサーバー用 Amazon FSx のサポートを拡張	AWS Resilience Hub アプリケーションの耐障害性を評価しながら、Amazon FSx for Windows File Server リソースの評価サポートを拡張します。Windows File Server 用 Amazon FSx を使用するアプリケーション向けに、アベイラビリティーゾーン (AZ) とマルチ AZ のデプロイ、バックアッププラン、 AWS Resilience Hub データレプリケーションを対象とする新しい耐障害性推奨事項を提供します。 AWS Resilience Hub Microsoft Active Directory へのファイルシステム依存関係を含め、Windows ファイルサーバー用 Amazon FSx をサポートし、リージョン内デプロイとクロスリージョンデプロイの両方に対応しています。 詳細については、次のトピックを参照してください。 • the section called “ AWS Resilience Hub サポート対象リソース” • the section called “AWSResilienceHubAsssessmentExecutionPolicy” • the section called “リソースをグループ化する AppComponent”	2024 年 3 月 26 日

AWS Resilience Hub 耐障害性スコアに関する追加情報を提供します。	AWS Resilience Hub レジリエンススコアのユーザーエクスペリエンスを更新しました。これにより、アプリケーションのレジリエンス態勢を改善するために必要なアクションを簡単にナビゲートして理解できるようになりました。 詳細については、「the section called “障害耐性スコアの理解”」を参照してください。	2023 年 11 月 9 日
AWS Resilience Hub Amazon Elastic Kubernetes サービス (Amazon EKS) リソースを含むアプリケーションのサポートを拡張します	AWS Resilience Hub Amazon EKS リソースを含むアプリケーションのサポートを拡張し、新しい運用上の推奨事項を含めます。Amazon EKS クラスターのリソースを含む評価を実施する際、アプリケーションの耐障害性の態勢を向上させるためにテストとアラームを実行することを推奨するようになりました。 詳細については、「the section called “Amazon Fault Injection Service の実験”」を参照してください。	2023 年 11 月 9 日

AWS Resilience Hub アプリケーションレベルで追加情報を提供します。	AWS Resilience Hub 推定ワークロード RTO と推定ワークロード RPO に関するアプリケーションレベルの追加情報を提供します。この追加情報には、直近の成功した評価で得られたアプリケーションの最大推定ワークロード RTO と推定ワークロード RPO が示されます。この値は、すべての中断タイプにおける最大推定ワークロード RTO と推定ワークロード RPO です。 詳細については、「the section called “アプリケーション”」を参照してください。	2023 年 10 月 30 日

AWS Resilience Hub リソースの評価サポートを拡張します。 AWS Step Functions	AWS Resilience Hub アプリケーションの耐障害性を評価しながら、 AWS Step Functions リソースの評価サポートを拡張します。 AWS Resilience Hub ステートマシンタイプ (標準ワークフローまたはエクスプレスワークフロー) AWS Step Functions を含む構成を分析します。さらに、 AWS Resilience Hub 予測されるワークロードの回復時間目標 (RTO) と予測されるワークロードの回復ポイント目標 (RPO) を満たすのに役立つ推奨事項も提供します。 AWS Step Functions リソースを含むアプリケーションを評価するには、 AWS 管理ポリシーを使用するか、 AWS Resilience Hub AWS Step Functions 構成の読み取りを許可する特定の権限を手動で追加して、必要な権限を設定する必要があります。 関連する権限の詳細については、「the section called “AWSResilienceHubAsssessmentExecutionPolicy”」を参照してください。	2023 年 10 月 30 日

AWS Resilience Hub 運用上の推奨事項を除外できます。	AWS Resilience Hub アラーム、標準運用手順 (SOP)、Amazon 障害注入サービス (AWS FIS) テストなどの運用上の推奨事項を除外する機能が追加されています。評価を実行すると AWS Resilience Hub、推定復旧時間と、評価対象アプリケーションの耐障害性を高める方法に関する推奨事項が表示されます。推奨項目の除外ワークフローを使用すると、推奨アラーム、SOP、 AWS FIS およびそれらに関係のないテストを除外できるようになりました。除外ワークフローは、推奨されているプラットフォーム以外のプラットフォームを使用している場合や、推奨を既に別の方法で実装している場合に役立ちます。 詳細については、次のトピックを参照してください。 • the section called “運用上の推奨事項を含めるまたは除外する” • the section called “ AWS Resilience Hub 推奨事項を含めたり除外したりする権限の制限”	2023 年 8 月 9 日

の権限設計の改善 AWS Resilience Hub	AWS Resilience Hub の AWS Identity and Access Management (IAM) ロールを柔軟に設定できるようにする新しい権限設計を導入しました。 AWS Resilience Hubまた、権限を 1 つのロールに統合し、自分やチームにとって意味のあるカスタムロール名を作成できるようになりました。 AWS Resilience Hub の新しい管理ポリシーにより、サポートされているサービスに対して適切な権限を付与できます。現在の権限設定方法に慣れている方のために、引き続き手動設定をサポートします。 AWS 管理ポリシーの詳細については、を参照してくださいthe section called “AWSResilienceHubAsssessmentExecutionPolicy”。	2023 年 8 月 2 日

によるアプリケーションレジリエンスドリフト検出 AWS Resilience Hub	AWS Resilience Hub アプリケーションの耐障害性を解決するために必要なアクションを事前に検出して把握できます。Amazon Simple Notification Service (Amazon SNS) を有効にして、推定ワークロード目標復旧時間 (RTO) または推定ワークロード目標復旧時点 (RPO) が目標の達成から組織のビジネス目標に達しなくなったときに通知を受信できるようにします。評価を手動で実行する際に耐障害性の問題を事後的に発見することから、Amazon SNS トピックを通じて事前に通知を受けることへと移行することで、潜在的な障害を早期に予測できるようになり、復旧目標が達成されるという確信がさらに高まります。 詳細については、次のトピックを参照してください。 • the section called “ステップ 5: 障害耐性ドリフト検出の設定” • the section called “アプリケーションリソースの表示”	2023 年 8 月 2 日

AWS Resilience Hub Amazon Relational Database Service と Amazon Aurora のサポートを改善します	AWS Resilience Hub Amazon Relational Database Service プロキシ、ヘッドレスおよび Amazon Aurora DB データベース構成の評価サポートを拡張します。さらに、Amazon RDS を含むアプリケーションを評価する際には、さまざまなデータベースエンジンを区別して、ワークロードの推定目標復旧時間 (RTO) をより正確に算出します。 AWS Resilience Hub また、お客様の環境内に耐障害性のベストプラクティスを実装するための追加アクションも提供します。 AWS ベストプラクティスには、 DevOps Guru for Amazon RDS によるパフォーマンスの洞察、強化されたモニタリング、サポートされているデータベースエンジンでのブルー/グリーンデプロイの自動化などがあります。 AWS Resilience Hub サポートされているすべてのサービスのリソースを評価に含めるために必要な権限の詳細については、「」を参照してください。the section called “AWSResilienceHubAsssessmentExecutionPolicy”	2023 年 8 月 2 日

AWS Resilience Hub Amazon エラスティックブロックストアスナップショットのサポートを拡張	AWS Resilience Hub Amazon Elastic Block Store (Amazon EBS) の評価サポートを拡張し、同じ Amazon EBS リージョン内で直接 API を使用して取得された Amazon EBS スナップショットを認識できるようにします。延長サポートは、Amazon Data Lifecycle Manager (Amazon Data Lifecycle Manager) または AWS Backup を使用しているお客様向けの現在のサポートに追加されます。 詳細については、Amazon Elastic Block Store (Amazon EBS) を参照してください。	2023 年 8 月 2 日

Amazon Elastic Compute Cloud の強化	AWS Resilience Hub Amazon Elastic Compute Cloud (Amazon EC2) のサポートを拡大しました。さまざまなサイズのアプリケーションについて、Amazon EC2 AWS を使用する顧客がそのユースケースに適した設定を選択できるようにします。AWS Resilience Hub 以下の Amazon EC2 設定の評価をサポートします。 • オンデマンドインスタンス。 • AWS Backup およびによるインスタンスのバックアップ AWS Elastic Disaster Recovery。 • Amazon Route 53 Application Recovery Controller (Route 53 ARC) によるAuto Scaling グループのサポート 今後、評価サポートはスポットインスタンス、専有ホスト、専有インスタンス、プレイスメントグループ、フリートにも及ぶ予定です。 詳細については、「the section called “AWS Resilience Hub アクセス権限リファレンス”」を参照してください。	2023 年 6 月 27 日

AWS 管理ポリシーの更新	AWS 評価を実施するための他のサービスへのアクセスを提供する新しいポリシーを追加しました。 詳細については、「the section called “AWSResilienceHubAsssessmentExecutionPolicy”」を参照してください。	2023 年 6 月 26 日
新しい Amazon DynamoDB のオペレーションに関するレコメンデーションのアラーム	Amazon DynamoDB を使用するアプリケーション向けに、オンデマンドとプロビジョニングされたキャパシティモード、 AWS Resilience Hub およびグローバルテーブルの回復リスクを警告する新しいアラームセットが提供されるようになりました。新しいアラームにアクセスするには、使用しているロールの AWS Identity and Access Management (IAM) ポリシーを更新する必要がある場合があります。 詳細については、「the section called “AWS Resilience Hub アクセス権限リファレンス”」を参照してください。	2023 年 5 月 2 日

AWS Trusted Advisor 機能強化	AWS Resilience Hub Amazon DynamoDB AWS Trusted Advisor を使用するアプリケーションのサポートが拡張されました。 AWS Trusted Advisor とを使用すると AWS Resilience Hub、過去 30 日間にアプリケーションが評価されなかった場合に通知を受け取ることができるようになりました。この通知により、アプリケーションを再評価して、障害耐性に影響する変更がないかを確認するよう求められます。 AWS Resilience Hub 評価からの経過時間の詳細については、「the section called “AWS Trusted Advisor”」を参照してください。	2023 年 5 月 2 日

Amazon Simple Storage Service の追加サポート	現在サポートされている Amazon Simple Storage Service (Amazon S3) クロスリージョンレプリケーション (Amazon S3 CRR) /Amazon S3 同一リージョンレプリケーション (SRR)、バージョニング、 AWS Backup に加え、マルチリージョンアクセスポイント、Amazon S3 レプリケーションタイムコントロール (Amazon S3 RTC)、およびBackup リカバリ (PITR) 設定について Amazon S3 AWS Resilience Hub を評価する予定です。 AWS point-in-time 詳細については、次のトピックを参照してください。 • the section called “AWS Resilience Hub アクセス権限リファレンス” • Amazon S3 ストレージの管理	2023 年 3 月 21 日

Amazon Elastic Kubernetes Service の追加サポート	AWS Resilience Hub は、アプリケーションの耐障害性を定義、検証、追跡するためのサポート対象リソースとして Amazon EKS クラスターを追加しました。お客様は Amazon EKS クラスターを新規または既存のアプリケーションに追加して、障害耐性を向上させるための評価や推奨事項を受け取ることができます。お客様は、Terraform AWS CloudFormation、、を使用してアプリケーションリソースを追加できます。 AWS Resource Groups AppRegistryさらに、お客様は 1 つ以上のリージョンに 1 つ以上の Amazon EKS クラスターを直接追加できます。各クラスターには 1 つ以上の名前空間があります。これにより、 AWS Resilience Hub 単一地域または地域をまたがる評価と推奨事項を提供できます。デプロイメント、レプリカ、ポッドの調査に加えて、ReplicationControllersクラスター全体の耐障害性を分析します。 AWS Resilience Hub AWS Resilience Hub ステートレスな Amazon EKS クラスターワークロードをサポートします。新機能は、 AWS AWS Resilience Hub サポート	2023 年 3 月 21 日

	されているすべてのリージョンで利用できます。 詳細については、次のトピックを参照してください。 • the section called “ステップ 2: アプリケーションリソースを管理する” • the section called “EKS クラスターを追加します” • the section called “AWS Resilience Hub アクセス権限リファレンス” • AWS 地域サービス	
Amazon Elastic File System の追加サポート	現在サポートされている Amazon Elastic File System (Amazon EFS) バックアップに加え、 AWS Resilience Hub 今後は Amazon EFS レプリケーションと AZ 設定について Amazon EFS を評価する予定です。 詳細については、次のトピックを参照してください。 • the section called “ AWS Resilience Hub サポート対象リソース” • Amazon Elastic File System とは	2023 年 3 月 21 日

アプリケーション入力ソースのサポート	AWS Resilience Hub これで、アプリケーションソースに関する透明性が確保されます。アプリケーションの入力ソースを追加、削除、再インポートしたり、新しいアプリケーションバージョンを公開したりするのに役立ちます。 詳細については、「the section called “アプリケーションリソースの表示”」を参照してください。	2023 年 2 月 21 日
アプリケーション構成パラメータのサポート	AWS Resilience Hub アプリケーションに関連するリソースに関する追加情報を収集するための入力メカニズムが提供されるようになりました。AWS Resilience Hub この情報により、お客様のリソースをより深く理解し、より優れた耐障害性に関する推奨事項を提示できるようになります。 詳細については、次のトピックを参照してください。 • the section called “アプリケーションの設定パラメータ” • the section called “ステップ 7: アプリケーションの設定パラメータを設定する” • the section called “アプリケーション設定パラメータの更新”	2023 年 2 月 21 日

Amazon Elastic Block Store の追加サポート	Amazon Elastic Block Store (Amazon EBS) ボリュームの現在のサポートに加えて、Amazon Amazon Data Lifecycle Manager と Amazon EBS 高速スナップショット復元 (FSR) による Amazon EBS AWS Resilience Hub スナップショットを評価するようになります。 詳細については、次のトピックを参照してください。 • the section called “AWS Resilience Hub アクセス権限リファレンス” • Amazon Elastic Block Store (Amazon EBS)	2023 年 2 月 21 日

との統合 AWS Trusted Advisor	AWS Trusted Advisor ユーザーは、自分のアカウントに関連付けられているアプリケーションのうち、 AWS Resilience Hubによって評価されたものを表示できます。 AWS Trusted Advisor 最新のレジリエンススコアを表示し、目標とするレジリエンスポリシー (RTO と RPO) が満たされているかどうかを示すステータスを表示します。評価が実行されるたびに、 AWS Resilience Hub AWS Trusted Advisor 最新の結果で更新されます。 AWS Trusted Advisor は、 AWS アカウントを継続的に分析し、 AWS ベストプラクティスと AWS Well-Architected ガイドラインに従うのに役立つ推奨事項を提供するサービスです。 詳細については、「the section called “AWS Trusted Advisor”」を参照してください。	2022 年 11 月 18 日

Amazon Simple Notification Service (Amazon SNS)のサポート	AWS Resilience Hub サブスクライバーを含む Amazon SNS 設定を分析して Amazon SNS を使用するアプリケーションを評価し、そのアプリケーションについて組織の推定ワークロード復旧目標 (推定ワークロード RTO と推定ワークロード RPO) を満たすための推奨事項を提示しています。Amazon SNS は、パブリッシャー (プロデューサー) からサブスクライバー (コンシューマー) にメッセージを配信するマネージド型サービスです。 詳細については、次のトピックを参照してください。 • the section called “ AWS Resilience Hub サポート対象リソース” • the section called “Identity and Access Management” • the section called “リソースをグループ化する AppComponent”	2022 年 11 月 16 日

Amazon Route 53 Application Recovery Controller (Amazon Route 53 ARC) の追加サポート	AWS Resilience Hub 現在、Amazon Route 53 ARC のElastic Load Balancing と Amazon Relational Database Service (Amazon RDS) の評価を行っています。これには、Amazon Route 53 ARC がどのような場合にメリットがあるかをアドバイスすることも含まれます。Amazon Route 53 ARC AWS 評価サポートを Auto Scaling グループ (AWS ASG) や Amazon DynamoDB AWS Resilience Hub以外にも拡張しています。Amazon Route 53 ARC はアプリケーションの可用性を高め、アプリケーション全体をフェイルオーバーリージョンにすばやくフェイルオーバーできます。 詳細については、次のトピックを参照してください。 • the section called “ AWS Resilience Hub サポート対象リソース” • the section called “Identity and Access Management”	2022 年 11 月 16 日

AWS Backup の追加Support	AWS Resilience Hub 現在、Amazon Route 53 ARC のElastic Load Balancing と Amazon Relational Database Service (Amazon RDS) の評価を行っています。これには、Amazon Route 53 ARC がどのような場合にメリットがあるかをアドバイスすることも含まれます。Amazon Route 53 ARC AWS 評価サポートを Auto Scaling グループ (AWS ASG) や Amazon DynamoDB AWS Resilience Hub以外にも拡張しています。Amazon Route 53 ARC はアプリケーションの可用性を高め、アプリケーション全体をフェイルオーバーリージョンにすばやくフェイルオーバーできます。 詳細については、次のトピックを参照してください。 • the section called “ AWS Resilience Hub サポート対象リソース” • the section called “Identity and Access Management”	2022 年 11 月 16 日
内容の更新: 新しいアプリケーションコンポーネントリソースの追加	AppComponent グループ化セクションのサポート対象アプリケーションコンポーネントリソースのリストに Route53 と AWS Backup を追加しました。	2022 年 7 月 1 日

新しい内容: アプリケーションコンプライアンスステータスの概念	変更が検出されましたステータスタイプが追加されました。	2022 年 6 月 2 日
はじめに AWS Resilience Hub	AWS Resilience Hub が利用可能になりました。このガイドでは、インフラストラクチャの分析、 AWS Resilience Hub AWS アプリの復元力を向上させるための推奨事項の取得、回復力スコアの確認などを行う方法について説明します。	2021 年 11 月 10 日

AWS 用語集

AWS の最新の用語については、「AWS の用語集リファレンス」の「AWS 用語集」を参照してください。

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。