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 AWS Resilience Hub

AWS Resilience Hub は、 でアプリケーションのレジリエンス体制を管理および改善するための中心的な場所です AWS。 AWS Resilience Hub を使用すると、レジリエンス目標を定義し、それらの目標に対するレジリエンス体制を評価し、 AWS Well-Architected フレームワークに基づいて改善のための推奨事項を実装できます。内では AWS Resilience Hub、Amazon Fault Injection Service の実験を作成して実行することもできます。これは、アプリケーションの実際の中断を模倣して、依存関係をよりよく理解し、潜在的な弱点を発見するのに役立ちます。 AWS Resilience Hub は、回復力体制を継続的に強化するために必要なすべての AWS サービスとツールを一元的に提供します。 AWS Resilience Hub は、他の のサービスと連携してレコメンデーションを提供し、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。

関連する障害 AWS 耐性サービスとリファレンス

AWS 障害耐性サービス	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 53ARC)	Amazon Route 53 Application Recovery Controller とは

トピック

- AWS Resilience Hub – 耐障害性管理
- AWS Resilience Hub – 耐障害性テスト
- AWS Resilience Hub の概念
- AWS Resilience Hub ペルソナ
- AWS Resilience Hub サポートされているリソース

AWS Resilience Hub – 耐障害性管理

AWS Resilience Hub は、 AWS アプリケーションの耐障害性を定義、検証、追跡するための一元的な場所を提供します。 AWS Resilience Hub は、アプリケーションの中断からの保護と復旧コストの

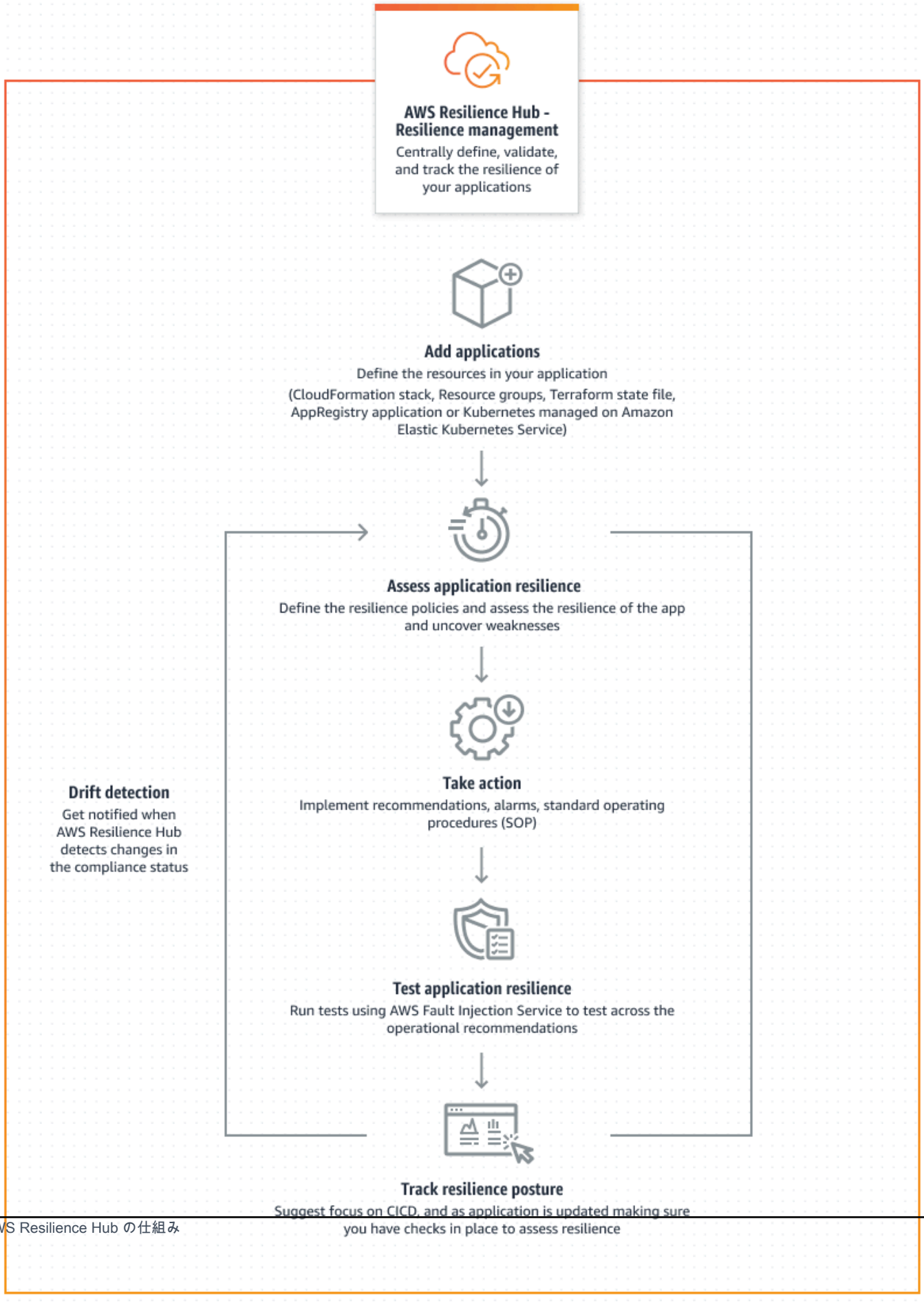
削減を支援し、ビジネス継続性を最適化してコンプライアンスと規制の要件を満たすのに役立ちます。を使用して AWS Resilience Hub 、次の操作を実行できます。

- 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。レコメンデーションには、アプリケーションの耐障害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が記載されています。このコードでは、統合および配信 (CI/CDSOPs) パイプラインでアプリケーションを使用してデプロイおよび実行できるテスト、アラーム、標準運用手順 () を実装します。
- さまざまな条件下で、目標復旧時間 (RTO) と目標復旧時点 (RPO) の目標を評価します。
- 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 パイプライン AWS Resilience Hub に を追加して、すべてのビルドを本番環境にリリースする前に検証できます。

AWS Resilience Hub の仕組み

次の図は、 AWS Resilience Hub の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説明するか、 で既に定義されているアプリケーションから選択できます 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RTO、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、およびリージョンの中断の およびRPO ターゲットが含まれます。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。この AWS Resilience Hub 評価では、 AWS Well-Architected フレームワーク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、潜在的な回復力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 の設定が含まれますSOPs。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が と のRPOターゲットRPOを満たすまでRTO、このプロセスを繰り返します。

検証

テストを実行して、 AWS リソースの障害耐性と、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 AWS リージョン からの復旧にかかる時間を測定します。障害耐性を測定するために、これらのテストでは AWS リソースの停止をシミュレートします。停止の例としては、ネットワーク使用不可エラー、フェイルオーバー、停止したプロセス、Amazon RDS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

AWS アプリケーションを本番環境にデプロイした後、 AWS Resilience Hub を使用してアプリケーションの障害耐性体制の追跡を継続できます。停止が発生した場合、オペレーターは で停止を表示 AWS Resilience Hub し、関連する復旧プロセスを起動できます。

AWS Resilience Hub – 耐障害性テスト

AWS Resilience Hub では、ワークロードに対して Amazon Fault Injection Service (AWS FIS) のテストと実験を実行し、最適な耐障害性を維持できます AWS 。これらのテストでは、破壊的なイベントを作成してアプリケーションにストレスを与え、アプリケーションの応答を観察できるようにします。 AWS FIS は、複数の事前構築済みのシナリオと、中断を発生させる多数のアクションを提供します。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。を使用してコンソール から実験 AWS FIS を実行するには、 the section called “前提条件”セクションで定義されている前提条件を完了します。 AWS Resilience Hub

次の表に、ナビゲーションペインで使用可能なすべての AWS FIS オプションと、 AWS Resilience Hub コンソールからテストの使用 AWS FIS を開始する手順を含む関連 AWS FIS ドキュメントへのリンクを示します。

AWS FIS ナビゲーションメニューのオプションとリファレンス

AWS FIS ナビゲーションメニューオプション	AWS FIS ドキュメント
[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 ライブラリ
[実験テンプレート]	の実験テンプレート AWS FIS

次の表に、障害耐性テストセクションのドロップダウンメニューから使用可能なすべての AWS FIS オプションと、コンソールから AWS FIS AWS Resilience Hub テストの使用を開始する手順を含む関連 AWS FIS ドキュメントへのリンクを示します。

AWS FIS ドロップダウンメニューのオプションとリファレンス

AWS FIS ドロップダウンメニューオプション	AWS FIS ドキュメント
[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 の概念

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、アプリケーションの停止を防ぐための AWS Resilience Hub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)

最後のデータリカバリポイントからの最大許容時間です。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損失の程度が決まります。

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、インポートされたアプリケーション定義に基づいてアプリケーションRTOが満たすと推定され、評価を実行する です。

ワークロード目標復旧時点

推定ワークロード復旧ポイント目標 (推定ワークロード RPO) は、インポートされたアプリケーション定義に基づいてアプリケーションRPOが満たすと推定され、評価を実行する です。

アプリケーション

AWS Resilience Hub アプリケーションは、 AWS サポートされているリソースのコレクションであり、障害耐性体制を管理するために継続的にモニタリングおよび評価されます。

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および失敗する関連 AWS リソースのグループ。例えば、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が同じアプリケーションコンポーネント () に属しますAppComponent。

AWS Resilience Hub は、どの AWS リソースをどのタイプの 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 は、アプリケーションの次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および RPOターゲットを満たすと推定されます。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。例えば、 AWS リージョン間の中断に対して RTOと のRPOターゲットを 24 時間選択したとします。 AWS Resilience Hub は、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。バックアップの標準運用手順 (SOP) からの復旧を維持し、テストして時間をかけることが期待されます。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

アプリケーションは、ポリシーで定義されている RTOおよび RPOターゲットを満たすと推定できませんでした。1 つ以上の がポリシーの目標を達成 AppComponents していません。例えば、 AWS リージョン間の中断に対して RTOと のRPOターゲットを 24 時間選択したが、データベース設定に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のクロスリージョンリカバリ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。

ドリフト検出

AWS Resilience Hub は、アプリケーションの評価の実行中にドリフト通知を実行して、AppComponent 設定の変更がアプリケーションのコンプライアンスステータスに影響を与えたかどうかを確認します。さらに、アプリケーションの入力ソース内のリソースの追加や削除などの変更もチェックおよび検出し、そのことを通知します。比較のために、 は、アプリケーションコンポーネ

ントがポリシーを満たした以前の評価 AWS Resilience Hub を使用します。 は、次のタイプのドリフト AWS Resilience Hub を検出します。

- アプリケーションポリシードリフト – このドリフトタイプは AppComponents 、前の評価でポリシーに準拠していたが、現在の評価で準拠に失敗したすべての を識別します。
- アプリケーションリソースドリフト — このドリフトタイプは、現在のアプリケーションバージョンのドリフトされたリソースをすべて識別します。

障害耐性評価

AWS Resilience Hub は、ギャップと潜在的な対策のリストを使用して、災害から回復して継続するために、選択したポリシーの有効性を測定します。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 は、アプリケーションの障害耐性ポリシー、アラーム、標準運用手順 (SOPs) 、および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示すスコアを生成します。

中断タイプ

AWS Resilience Hub は、次のタイプの停止に対する障害耐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 では、さまざまなタイプ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ています。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操作手順 (SOPs) が正しく動作して、停止からアプリケーションを復旧することを確認します。

SOPs 推定ワークロードRTOと推定ワークロードの測定テストRPO。さまざまなアプリケーション設定をテストし、 RTOと がポリシーで定義された目的RPOを満たしているかどうかを測定できます。

SOP

標準運用手順 (SOP) は、機能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ように設計された一連の規範的な手順です。アプリケーション評価に基づいて、 は のセット AWS Resilience Hub を推奨SOPsします。また、タイムリーな復旧を確保するために、中断SOPsの前に準備、テスト、測定することをお勧めします。

AWS Resilience Hub ペルソナ

エンタープライズアプリケーションを構築するには、インフラストラクチャ、ビジネス継続性、アプリケーション所有者、アプリケーションのモニタリングを担当するその他の利害関係者など、さまざまな部門横断的なチームからの協力が必要です。さまざまなチームのさまざまなペルソナは、 での

アプリケーションの構築と管理に貢献し AWS Resilience Hub、それぞれに異なる役割と責任があります。さまざまなペルソナへのアクセス許可のグレートの詳細については、「」を参照してくださいthe section called “AWS Resilience Hub ペルソナとIAMアクセス許可のリファレンス”。

でアプリケーションの作成と評価の実行を開始するには AWS Resilience Hub、次のペルソナを作成することをお勧めします。

- インフラストラクチャアプリケーションマネージャー – このペルソナを持つユーザーは、インフラストラクチャとアプリケーションリソースをセットアップ、設定、保守し、アプリケーションの信頼性とセキュリティを確保する責任があります。その責任には以下が含まれます。
  - アプリケーションが定期的にデプロイおよび更新されていることを確認する
  - システムパフォーマンスのモニタリング
  - 問題のトラブルシューティング
  - バックアップとディザスタリカバリプランの実装
- ビジネス継続性マネージャー – このペルソナを持つユーザーは、アプリケーションポリシーを指示し、アプリケーションのビジネス重要度を判断する責任があります。その責任には以下が含まれます。
  - ポリシーの設定における重要な意思決定
  - ビジネスの重要性の評価
  - 重要なアプリケーションにリソースを割り当てる
  - リスクの評価と管理
- アプリケーション所有者 – このペルソナを持つユーザーは、可用性と信頼性の高いアプリケーションを確保する責任があります。その責任には以下が含まれます。
  - アプリケーションのパフォーマンスを測定およびモニタリングし、ボトルネックを特定するための主要なパフォーマンス識別子の定義
  - 複数の利害関係者向けのトレーニングの整理
  - 次のドキュメントが であることを確認します up-to-date。
    - アプリケーションのアーキテクチャ
    - デプロイプロセス
    - 設定のモニタリング
    - パフォーマンス最適化手法
- 読み取り専用アクセス – このペルソナを持つユーザーは、読み取り専用アクセス許可に制限されます。その責任には、レジリエンススコア、運用上の推奨事項、および障害耐性の推奨事項をモニタリングすることで、アプリケーションのパフォーマンスと健全性を可視化および監視すること

が含まれます。さらに、アプリケーションが組織の目標を達成していることを確認するために、問題、傾向、改善すべき分野を特定する責任もあります。

AWS Resilience Hub サポートされているリソース

中断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::RDS::DBInstance`や などの AWS Resilience Hub 最上位リソースによって完全にサポートされます`AWS::RDS::DBCluster`。

が、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 AWS Resilience Hub ために必要なアクセス許可の詳細については、「」を参照してくださいthe section called "AWSResilienceHubAsssessmentExecutionPolicy"。

AWS Resilience Hub は、以下の AWS 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)

    > **Note**
    >
    > AWS Resilience Hub は、Amazon リソースにアクセスするための古い Amazon EC2リソースネーム (ARN) 形式をサポートしていません。新しいARN形式では、 AWS アカウント ID が使用され、クラスター内のリソースにタグを付ける機能が強化されます。また、クラスターで実行されているサービスとタスクのコストも追跡されます。
    >
    > - 古い形式 (廃止) – `arn:aws:ec2:<region>::instance/<instance-id>`
    > - 新しい形式 – `arn:aws:ec2:<region>:<account-id>:instance/<instance-id>`
    >
    > 新しいARN形式の詳細については、「Amazon ECSデプロイを新しい ARNおよびリソース ID 形式 に移行する」を参照してください。

  - 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 Elastic Disaster Recovery

> **Note**
>
> - AWS Resilience Hub は、各リソースでサポートされている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、 は、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、各リソースの一意のインスタンスを識別することで、より正確な障害耐性に関する推奨事項 AWS Resilience Hub を提供します。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 アプリケーションリソースの編集 を参照してください。
> - AWS Resilience Hub は、 ECSで Amazon EKSと Amazon をサポートします AWS Fargate。
> - AWS Resilience Hub は、以下のサービスの一環として AWS Backup 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
  - ARC の Amazon Route 53 は、Amazon DynamoDB Global、Elastic Load Balancing、RDS および AWS Auto Scaling グループのみ AWS Resilience Hub を評価します。
  - がクロスリージョンリソースを評価する AWS Resilience Hub 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、アプリケーションコンポーネントのリソースのグループ化 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、 は Amazon EKSクラスターのクロス AWS リージョン評価をサポート AWS Resilience Hub していません。
  - 現在、 は次の Kubernetes リソースタイプのみ AWS Resilience Hub を評価します。
    - デプロイ
    - ReplicaSets
    - ポッド

AWS Resilience Hub は、次のタイプのリソースを無視します。

- 推定ワークロードRTOまたは推定ワークロードに影響を与えないリソース RPO – 推定ワークロードRTOまたは推定ワークロードに影響を与えAWS::RDS::DBParameterGroupない などのリソースはRPO、 では無視されます AWS Resilience Hub。
- 最上位以外のリソース – 最上位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、最上位リソース AWS Resilience Hub 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 でサポートされているリソースです。ただし、AWS::ApiGatewayV2::Stage は最上位のリソースではありません。したがって、 によってインポートされません 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 および API-GW HTTP) と Amazon Aurora Global 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で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 “のアプリケーションリソースの編集”」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を与える可能性がありますが、 AWS Resilience Hub 現時点では によって完全にはサポートされていません。 は、アプリケーションが AWS CloudFormation スタック、Terraform 状態ファイル AWS Resource Groups、または AppRegistry アプリケーションによってバックアップされている場合に、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作業 AWS Resilience Hub を行います。

開始

このセクションでは、 の使用を開始する方法について説明します AWS Resilience Hub。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。

トピック

前提条件

を使用する前に AWS Resilience Hub、次の前提条件を満たす必要があります。

- AWS accounts – 内で使用する AWS 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 つ以上のアカウントを作成します AWS Resilience Hub。 AWS アカウントの作成と管理の詳細については、以下を参照してください。
  - 初回 AWS ユーザー – 開始方法: 初回 AWS ユーザーですか？
  - AWS アカウントの管理 – https://docs.aws.amazon.com/accounts/latest/reference/managing-accounts.html
- AWS Identity and Access Management (IAM) アクセス許可 – AWS 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 アクセス許可を設定する必要があります。例えば、アプリケーションリソースにアクセスするための AWS アカウントを作成した場合は、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 AWS Resilience Hub にアクセスするために必要な IAM アクセス許可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 Resilience Hub と の連携方法 IAM” 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、ロールに IAM アクセス許可を追加する方法をすばやく開始するには、 AWS マネージドポリシー () を使用できますthe section called “AWS マネージドポリシー”。 AWS マネージドポリシーを使用すると、 で利用可能な一般的なユースケースを自分で記述する AWS アカウント よりも簡単にカバーできます。 は、 AWS マネージドポリシーに追加のアクセス許可 AWS Resilience Hub を追加して、サポートを他の AWS サービスに拡張し、新機能を含めます。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 管理ポリシーを使用してユーザー、グループ、ロールに適切な IAM アクセス許可を割り当てる場合は、これらのアクセス許可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、「」を参照してくださいthe section called “AWSResilienceHubAsssessmentExecutionPolicy”。

へのアプリケーションの追加 AWS Resilience Hub

AWS Resilience Hub は、ソフトウェア開発ライフサイクルに統合される障害耐性評価と検証を提供します。 AWS Resilience Hub は、以下によって AWS アプリケーションを事前に準備し、中断から保護します。

- 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推定します。
- 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。既存のアプリケーション、 AWS CloudFormation スタック、または からリソースを収集 AppRegistry し AWS Resource Groups、適切な障害耐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、 で公開し 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。別の評価を実行し、結果を比較して、推定ワークロードRTOと推定ワークロードが RTOと のRPOターゲットRPOを達成するまで反復できます。

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
- 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 3: AWS Resilience Hub アプリケーションにリソースを追加する
- ステップ 4: RTOと を設定する RPO
- ステップ 5: スケジュールされた評価とドリフト通知を設定する

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

AWS アプリケーションの詳細 AWS Resilience Hub を説明し、障害耐性を評価するレポートを実行して、 の使用を開始します。

開始するには、「開始方法」の AWS Resilience Hub ホームページで、「アプリケーションの追加」を選択します。

に関連するコストと請求の詳細については AWS Resilience Hub、「 のAWS Resilience Hub 料金」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、 で既存の AWS アプリケーションの詳細を記述する方法について説明します 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、 AWS Resource Groups AppRegistry アプリケーション、Terraform 状態ファイルに加えて、Amazon Elastic Kubernetes Service (Amazon EKS) クラスターにあるリソースを追加できます。つまり、AWSResilience Hub では、Amazon EKSクラスターにあるリソースをオプションの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 AWS Resource Groups、 AppRegistry アプリケーション、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 only – 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 クラスターの追加” 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 & EKS — リソースコレクションと Amazon EKSクラスターのいずれか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 “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 クラスターの追加” 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: AWS Resilience Hub アプリケーションにリソースを追加する

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

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 クラスターの追加”

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
- の使用 AWS Resource Groups
- AppRegistry アプリケーションの使用
- Terraform 状態ファイルの使用
- 既存の AWS Resilience Hub アプリケーションの使用

AWS CloudFormation スタックの使用

記述するアプリケーションで使用するリソースを含む AWS CloudFormation スタックを選択します。スタックは、アプリケーションの記述に AWS アカウント 使用している から取得することも、異なるアカウントまたは異なるリージョンから取得することもできます。

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. CloudFormation スタックを選択して、スタックベースのリソースを検出します。
2. スタックの選択ドロップダウンリストから、 AWS アカウント とリージョンに関連付けられているスタックを選択します。

   別の 、別のリージョン AWS アカウント、また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 AWS 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、スタックを追加 ARNを選択します。の詳細についてはARNs、「 AWS 全般のリファレンス」の「Amazon リソースネーム (ARNs) 」を参照してください。

の使用 AWS Resource Groups

記述 AWS Resource Groups するアプリケーションで使用するリソースを含む を選択します。

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. リソースグループを選択して、リソース AWS Resource Groups を含む を見つけます。
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。

   別の 、別のリージョン AWS アカウント、またはその両方 AWS Resource Groups にある を使用するには、リソースグループ ボックスにスタックの Amazon リソースARNネーム (ARN) を入力し、リソースグループの追加 ARNを選択します。の詳細についてはARNs、「 AWS 全般のリファレンス」の「Amazon リソースネーム (ARNs) 」を参照してください。

AppRegistry アプリケーションの使用

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

記述する AppRegistry アプリケーションで使用するリソースを含むアプリケーションを選択します。

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. AppRegistry で作成されたアプリケーションのリストから選択します 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 は、Terraform ステートファイルバージョン `0.12` 以降をサポートしています。

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 URLフィールドで Terraform 状態ファイルの場所へのリンクを指定し、S3 の追加 URL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 AWS Resilience Hub アプリケーションの使用

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 クラスターの追加

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 アクセスEKS許可と追加のIAMロールが必要です。クラスターに接続するための単一アカウント、クロスアカウント Amazon アクセスEKS許可、および追加のIAMロールの追加の詳細については、以下のトピックを参照してください。
>
> - AWS Resilience Hub アクセス許可リファレンス
> - the section called “Amazon EKSクラスター AWS Resilience Hub へのアクセスの有効化”

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

> **Note**
>
> AWS Resilience Hub が Amazon EKSクラスターを評価するには、関連する名前空間をEKSクラスターEKSと名前空間の各 Amazon クラスターに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正確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. AWS アカウント とリージョンに関連付けられているEKSクラスターの選択ドロップダウンリストから Amazon EKSクラスターを選択します。
2. 別の 、別のリージョン AWS アカウント、またはその両方にある Amazon EKSクラスターを使用するには、クロスアカウントまたはリージョンボックスにスタックの Amazon リソースネーム (ARN) EKS を入力し、 の追加ARNを選択します。の詳細についてはARNs、「 AWS 全般のリファレンス」の「Amazon リソースネーム (ARNs) 」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クラスター AWS Resilience Hub へのアクセスの有効化”」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EKS」セクションのクラスターと名前空間テーブルから、Amazon 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。 EKS

   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 – AWS Resilience Hub がアプリケーション内の選択した Amazon EKSクラスターの名前空間を含めた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が含まれていないことを示します。
     - 名前空間の追加 – 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、名前空間をすべてのEKSクラスターに適用する 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は、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 を設定する RPO

ステップ 4: RTOと を設定する RPO

独自の RTO/RPO ターゲットを使用して新しい障害耐性ポリシーを定義することも、定義済みの RTO/RPO ターゲットを使用して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 RTOターゲットセクションで /RPO を定義します。

> **Note**
>
> - アプリケーションのデフォルト RTOと が入力されRPOました。RTO と をRPO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 では、障害耐性ポリシーの RTOおよび 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 および RPOフィールドに値 0 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 0 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、ボックスに数値を入力し、その値が RTOと の両方を表す時間単位を選択しますRPO。

   Infrastructure and RTOセクションの Infrastructure RPO and Availability Zone に対してこれらの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があり、リージョンRTOと を定義する場合はRPO、リージョン - オプション をオンにします。

   RTO と でRPO、ボックスに数値を入力し、その値が RTOと の両方を表す時間単位を選択しますRPO。

次へ

the section called “ステップ 5: スケジュールされた評価とドリフト通知を設定する”

ステップ 5: スケジュールされた評価とドリフト通知を設定する

AWS Resilience Hub では、スケジュールされた評価とドリフト通知を設定して、アプリケーションを毎日評価し、ドリフトが検出されたときに通知を受け取ることができます。

ドリフト通知を設定するには

1. アプリケーションを毎日評価するには、毎日の を自動的に評価をオンにします。

   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は適切なIAMロールが設定されています。
   - アプリケーションが現在のIAMユーザーアクセス許可で設定されている場合は、`AWSResilienceHubAsssessmentExecutionPolicy`

     the section called “AWS Resilience Hub と の連携方法 IAM” でロールが適切な手順を使用している。

2. が障害耐性ポリシーからドリフト AWS Resilience Hub を検出したとき、またはそのリソースがドリフトしたときに通知を受け取るには、アプリケーションが をドリフトしたときに通知を受け取るをオンにします。

   このオプションがオンになっている場合、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「トピックの選択」オプションを選択し、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許可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 “ AWS Resilience Hub を有効にして Amazon SNSトピックに発行する”」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。

   異なる AWS アカウント リージョンまたは異なるリージョン、またはその両方にある Amazon SNSトピックを使用するには、SNSトピックを入力 ARN を選択し、Amazon SNSトピックの Amazon リソースネーム (ARN) を SNS トピックの提供 ボックスに入力します。の詳細についてはARNs、「 AWS 全般のリファレンス」の「Amazon リソースネーム (ARNs) 」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 では、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アクセス許可を設定して、リソースを検出して評価できます。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、IAM ロールの選択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では、IAMロールの入力 ボックスにロールの Amazon リソースネーム (ARNs) を指定しない場合、 AWS Resilience Hub はすべてのアカウントのIAMロールを選択 ドロップダウンリストから選択したIAMロールを使用します。 IAM ARN

   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、次のいずれかのオプションを使用して 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した場合は、IAM「コンソールでAWSレジリエンス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した場合は、 のすべてのステップを完了する必要がありますAWS CLI。
   - CloudFormation テンプレート – このオプションを選択した場合、どのアカウントタイプ (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、適切な AWS CloudFormation 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. 右矢印を選択して、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ロールの入力ボックスにロールARNsのを入力します。 IAM ARN入力するIAMロールARNsの が現在のアカウントに属していないことを確認します。
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出する場合は、右矢印を選択して展開します。現在のIAMユーザーアクセス許可を使用するセクションを選択し、 内で必要な機能を有効にするにはアクセス許可を手動で設定する必要があることを理解しました AWS Resilience Hub。

   このオプションを選択すると、一部の AWS Resilience Hub 機能 (ドリフト通知など) が期待どおりに機能せず、ステップ 1 とステップ 3 で指定した入力は無視されます。

次へ

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

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、 を使用してクロスリージョンフェイルオーバーサポートの詳細を提供できます AWS Elastic Disaster Recovery。 AWS Resilience Hub はこの情報を使用して障害耐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 に使用されるアカウント ID があらかじめ入力されており AWS Resilience Hub、これを変更できます。
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

AWS リソースを検索およびフィルタリングしたり、 AWS コストを追跡したりするために、タグまたはラベルを リソースに割り当てます。

(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 “のアプリケーションリソースの編集”

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、アプリケーション概要ページにリダイレクトされ、障害耐性評価を実行できます。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。

の使用 AWS Resilience Hub

AWS Resilience Hub は、 でのアプリケーションの耐障害性を向上させ AWS 、アプリケーションの停止時の復旧時間を短縮するのに役立ちます。

トピック:

AWS Resilience Hub ダッシュボード

ダッシュボードには、アプリケーションポートフォリオの耐障害性ステータスが包括的に表示されます。ダッシュボードは、 や Amazon Fault Injection Service () などの のサービスからの回復力イベント (データベースが使用できない、回復力の検証に失敗したなど) 、アラート、インサイトを集約して整理 CloudWatch しますAWS FIS。

ダッシュボードでは、評価される各アプリケーションの耐障害性スコアも生成されます。このスコアは、推奨される耐障害性ポリシー、アラーム、復旧標準運用手順 (SOPs)、およびテストに対して評価された場合にアプリケーションがどの程度うまく機能するかを示します。このスコアを使用して、時間の経過に伴う回復力の向上を測定できます。

AWS Resilience Hub ダッシュボードを表示するには、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。ダッシュボードページには、次のセクションが表示されます。

アプリケーションのステータス

アプリケーションのステータスは、アプリケーションがアタッチされた障害耐性ポリシーに準拠しているかどうかを示します。さらに、評価が完了すると、ステータスはアプリケーションの入力ソース

が変更されたかどうかも示します。次の各ステータスの数値を選択すると、アプリケーションページで同じステータスを共有するすべてのアプリケーションが表示されます。

- ポリシー内のアプリケーション — アタッチされた障害耐性ポリシーに準拠するすべてのアプリケーションを示します。
- ポリシーに違反するアプリケーション — アタッチされた障害耐性ポリシーに準拠していないすべてのアプリケーションを示します。
- 評価されていないアプリケーション — コンプライアンスがまだ評価または追跡されていないすべてのアプリケーションを示します。
- アプリケーションのドリフト — 障害耐性ポリシーからドリフトしたすべてのアプリケーション、またはリソースがドリフトしたかどうかを示します。

時間の経過に伴うアプリケーションの障害耐性スコア

時間の経過に伴うアプリケーションの障害耐性スコアを使用すると、過去 30 日間のアプリケーションの障害耐性の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が 10 個一覧表示できますが、 には一度に最大 4 つのアプリケーションのグラフ AWS Resilience Hub のみが表示されます。障害耐性スコアの詳細については、「」を参照してください障害耐性スコアの理解。

> **Note**
>
> AWS Resilience Hub は、スケジュールされた評価を同時に実行しません。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、時間の経過に伴う障害耐性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、Amazon CloudWatch を使用してこれらのグラフも生成します。でメトリクスを表示 CloudWatch を選択して、 CloudWatch ダッシュボードでアプリケーションの障害耐性に関するより詳細な情報を作成および表示します。の詳細については CloudWatch、「Amazon CloudWatch ユーザーガイド」の「ダッシュボードの使用」を参照してください。

実装されたアラーム

このセクションでは、すべてのアプリケーションをモニタリング CloudWatch するために Amazon で設定したすべてのアラームを一覧表示します。詳細については、アラームを表示する を参照してください。

実施した実験

このセクションでは、すべてのアプリケーションに実装したすべてのフォールトインジェクション実験を一覧表示します。詳細については、「故障注入実験を表示する」を参照してください。

AWS Resilience Hub アプリケーションの説明と管理

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、回復するように構造化された AWS リソースのコレクションです。

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 つ以上の AWS CloudFormation スタックのリソース、および適切な障害耐性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。

AWS Resilience Hub アプリケーションを記述したら、障害耐性評価を実行できるように公開する必要があります。その後、評価からの推奨事項を使用して、別の評価を実行し、結果を比較し、推定ワークロードRTOと推定ワークロードが RTOおよび RPOのターゲットRPOを満たすまでプロセスを繰り返すことで、回復性を向上させることができます。

アプリケーションページを表示するには、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 – アプリケーションステータスを評価済み、未評価、ポリシー違反、または変更検出済み AWS Resilience Hub に設定します。
  - 評価済み - アプリケーションを評価し AWS Resilience Hub ました。
  - 未評価 - AWS Resilience Hub アプリケーションは評価されていません。
  - ポリシー違反 - アプリケーションが目標復旧時間 (RTO) と目標復旧時点 () の障害耐性ポリシーの目的を満たさなかった AWS Resilience Hub と判断しましたRPO。アプリケーションの耐障害性を評価する AWS Resilience Hub 前に、 が提供する推奨事項を確認して使用します。推奨事項の詳細については、「へのアプリケーションの追加 AWS Resilience Hub」を参照してください。
  - 検出された変更 - アプリケーションに関連付けられた障害耐性ポリシーに加えられた変更 AWS Resilience Hub が検出されました。アプリケーションが障害耐性ポリシーの目的を満たしている

かどうかを判断する AWS Resilience Hub には、 のアプリケーションを再評価する必要があります。

- [スケジュールされた評価] – 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。スケジュールされた評価についての詳細は、「アプリケーションの障害耐性」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 によって毎日自動的に評価されない AWS Resilience Hub ため、アプリケーションを手動で評価する必要があることを示します。
- 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ドリフトしたかどうかを示し、次のいずれかのステータスを設定します。
  - ドリフト - 前回の評価で障害耐性ポリシーに準拠していたアプリケーションが、現在は障害耐性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。さらに、現在のアプリケーションバージョンに含まれている入力ソース内のリソースが追加または削除されたかどうかも示します。
  - ドリフトなし - アプリケーションがポリシーで定義されている RTOおよび RPOターゲットを満たすと推定されていることを示します。さらに、現在のアプリケーションバージョンに含まれている入力ソース内のリソースが追加または削除されなかったことも示します。
- 推定ワークロード RTO — アプリケーションの推定ワークロードRTOの最大数を示します。この値は、前回の評価RTOで成功したすべての中断タイプの最大推定ワークロードです。
- 推定ワークロード RPO — アプリケーションの推定ワークロードRPOの最大数を示します。この値は、前回の評価RTOで成功したすべての中断タイプの最大推定ワークロードです。
- [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) 。の詳細についてはARNs、「 AWS 全般のリファレンス」の「Amazon リソースネーム (ARNs) 」を参照してください。

> **Note**
>
> AWS Resilience Hub は、イメージリポジトリECRに Amazon を使用している場合にのみ、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。

- [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 アプリケーションを記述するためのさまざまなアプローチと、それらの管理方法について説明します。

トピック

AWS Resilience Hub アプリケーションの概要の表示

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障害耐性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から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、表示するアプリケーションの名前を選択します。

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

評価の概要

このセクションでは、最後に成功した評価の概要を示し、重要な推奨事項を実用的なインサイトとして強調表示します。 AWS Resilience Hub は Amazon Bedrock の生成 AI 機能を使用して、 が提供する最も重要なレジリエンスに関する推奨事項にユーザーを集中させます AWS Resilience Hub。重要な項目に焦点を当てることで、アプリケーションのレジリエンス体制を改善する最も重要な推奨事項に集中できます。レコメンデーションを選択して概要を表示し、詳細を表示を選択して、評価レポートの関連セクションのレコメンデーションに関する詳細を表示します。評価レポートのレビューの詳細については、「」を参照してくださいthe section called “評価レポートのレビュー”。

> **Note**
>
> - この評価の概要は、米国東部 (バージニア北部) リージョンでのみ利用できます。
> - Amazon Bedrock の大規模言語モデル (LLMs) によって生成された評価の概要は、提案にすぎません。生成 AI テクノロジーの現在のレベルは完全ではなくLLMs、不可逆性もありません。バイアスと誤った回答はまれですが、予想する必要があります。からの出力を使用する前に、評価の概要の各推奨事項を確認してくださいLLM。

[概要]

このセクションでは、以下のセクションで選択したアプリケーションの概要を示します。

- アプリケーション情報 – このセクションでは、選択したアプリケーションに関する以下の情報を提供します。

- アプリケーションステータス — アプリケーションのステータスを示します。
- 説明 – アプリケーションの説明。
- Version – 現在評価されているアプリケーションのバージョンを示します。
- 障害耐性ポリシー — アプリケーションにアタッチされている障害耐性ポリシーを示します。障害耐性ポリシーの詳細については、「障害耐性ポリシーの管理」を参照してください。

- アプリケーションのドリフト – このセクションでは、選択したアプリケーションの評価の実行中に検出されたドリフトが強調表示され、障害耐性ポリシーに準拠しているかどうかが確認されます。さらに、アプリケーションバージョンが最後に公開されてから、いずれかのリソースが追加または削除されたかどうかも確認します。このセクションでは、次の情報が表示されます。
  - ポリシードリフト — 以下の番号を選択すると、前の評価でポリシーに準拠していたが、現在の評価では準拠に失敗したすべてのアプリケーションコンポーネントが表示されます。
  - リソースドリフト – 以下の数値を選択すると、最新の評価でドリフトされたすべてのリソースが表示されます。

アプリケーションの障害耐性

障害耐性スコアセクションに表示されるメトリクスは、アプリケーションの最新の障害耐性評価からのものです。

[障害耐性スコア]

障害耐性スコアは、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、AWS Resilience Hub アプリケーションの障害耐性ポリシー、アラーム、標準運用手順 (SOPs) 、テストを満たすための推奨事項をアプリケーションがどの程度順守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障害耐性スコアは 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。これは、テストが正しいアラームを開始していること、およびアラームが正しい を開始していることを示しますSOP。

例えば、 が 1 つのアラームと 1 つの を含む 1 つのテスト AWS Resilience Hub を推奨するとしますSOP。テストが実行されると、アラームは関連付けられた を開始しSOP、正常に実行されます。障害耐性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。

実装されたアラーム

アプリケーション概要の「アラームの実装」セクションには、アプリケーションをモニタリング CloudWatch するために Amazon 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、「アラームの管理」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。故障注入実験の詳細については、「Amazon Fault Injection Service 実験の管理」を参照してください。

AWS Resilience Hub アプリケーションリソースの編集

正確で有用な障害耐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 アプリケーションとリソースと一致す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。 AWS アプリケーションからリソースを追加または削除する場合は、それらの変更を に反映する必要があります AWS Resilience Hub。

AWS Resilience Hub は、アプリケーションソースに関する透明性を提供します。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 リファレンス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。リソースは論理アプリケーションコンポーネント () にグループ化されます AppComponents。を編集 AppComponents して、アプリケーションの構造をよりよく反映できます。

アプリケーションのドラフトバージョンを編集し、新しい (リリース) バージョンに変更を公開することで、アプリケーションリソースに追加または更新します。 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) AWS Resilience Hub を使用して障害耐性評価を実行します。

アプリケーションの障害耐性を評価するには

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 [障害耐性の評価] を選択します。
4. [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。

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. [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。

スケジュールされた評価を有効にするには

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、スケジュールされた評価を有効にするアプリケーションを選択します。
3. をオンにすると、毎日 が自動的に評価されます。

スケジュールされた評価を無効にするには

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、スケジュールされた評価を有効にするアプリケーションを選択します。
3. オフ 日次 を自動的に評価します。

> **Note**
>
> スケジュールされた評価を無効にすると、ドリフト通知が無効になります。

4. をオフにする を選択します。

アプリケーションのドリフト通知を有効にするには

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、ドリフト通知を有効にするアプリケーションを選択するか、ドリフト通知設定を編集します。
3. ドリフト通知は、次のいずれかのオプションを選択して編集できます。
   - アクション から、ドリフト通知を有効にする を選択します。
   - 「アプリケーションドリフト」セクションで「通知を有効にする」を選択します。

4. のステップを完了しステップ 5: スケジュールされた評価とドリフト通知を設定する、この手順に戻ります。
5. [Enable (有効化)] を選択します。

   ドリフト通知を有効にすると、スケジュールされた評価も有効になります。

アプリケーションのドリフト通知を編集するには

> **Note**
>
> この手順は、スケジュールされた評価 (毎日自動的に評価がオンになっている) とドリフト通知を有効にしている場合に適用されます。

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、ドリフト通知を有効にするアプリケーションを選択するか、ドリフト通知設定を編集します。
3. ドリフト通知は、次のいずれかのオプションを選択して編集できます。
   - アクション から、ドリフト通知の編集 を選択します。
   - 「アプリケーションドリフト」セクションで「通知の編集」を選択します。
4. のステップを完了しステップ 5: スケジュールされた評価とドリフト通知を設定する、この手順に戻ります。
5. [保存] 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。

障害耐性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 [障害耐性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、[障害耐性ポリシーの選択] ドロップダウンリストから障害耐性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、および 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. AppComponents アプリケーションの入力ソース、リソース、および を編集するには、以下の手順を実行します。

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。例えば、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、コンソールのスタックの詳細ページ AWS CloudFormation 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。例えば、 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 状態ファイル、および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。入力ソース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リ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。検索エクスペリエンスを向上させるために、 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ました。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 スタック、Terraform 状態ファイル、手動で追加されたアプリケーション、 AppRegistry アプリケーション、または 内のリソースを識別するために使用される名前です AWS Resource Groups。

  > **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 “サポートされている AWS Resilience Hub 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。例えば、`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、「」を参照してくださいアプリケーションコンポーネントのリソースのグループ化。
- [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。例えば、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、 のスタックの詳細ページにリダイレクトされます AWS CloudFormation。
- [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 状態ファイル、および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 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。
- [評価可能] – AWS Resilience Hub がリソースの障害耐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 コンポーネント。
- [名前] – アプリケーションリソースの名前。
- アカウント – 物理リソースを所有する AWS 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: AWS Resilience Hub アプリケーションにリソースを追加する 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. リソース識別子を編集するには、リソースを選択し、[アクション] から [リソース識別子を編集] 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. を変更するには AppComponent、リソースを選択し、アクション から変更 AppComponentを選択し、次のステップを実行します。

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

   b. [追加] 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. リソースを含めるには、リソースを選択し、[アクション] から [リソースを含める] 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 を編集する AppComponents 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、「」を参照してくださいアプリケーションコンポーネントのリソースのグループ化。

AppComponents セクションには、リソースがグループ化されているすべての論理コンポーネントが一覧表示されます。は、次の AppComponents 方法で識別できます。

- AppComponent name – 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コンポーネントの名前 AWS Resilience Hub 。
- AppComponent type – コンポーネントのタイプ AWS Resilience Hub 。
- [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。例えば、 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. を作成するには AppComponent、アクションメニューから新規作成 AppComponentを選択し、次のステップを実行します。

   a. 名前ボックスに AppComponent 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. タイプドロップダウンリストから AppComponent AppComponentのタイプを選択します。
   c. [保存] を選択します。

3. を編集するには AppComponent、 を選択し AppComponent、アクション から編集 AppComponent を選択します。
4. を削除するには AppComponent、 を選択し AppComponent、アクション AppComponentから削除を選択します。

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。正確な障害耐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 AWS Resilience Hub アプリケーションバージョンの公開」を参照してください。

アプリケーションコンポーネントの管理

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動作および失敗する関連 AWS リソースのグループです。例えば、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 AppComponent. AWS Resilience Hub has ルールに属し、どの AWS リソースがどの AppComponent タイプに属するかを管理します。例えば、`DBInstance`は に属`AWS::ResilienceHub::DatabaseAppComponent`し、 に属さないことができます`AWS::ResilienceHub::ComputeAppComponent`。

は、以下のリソース AWS Resilience Hub AppComponents をサポートしています。

- `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、 は Amazon FSx for Windows File Server のみ AWS Resilience Hub をサポートしています。

  - AWS::S3::Bucket

トピック

- アプリケーションコンポーネントのリソースのグループ化

アプリケーションコンポーネントのリソースのグループ化

アプリケーションが リソース AWS Resilience Hub とともに にインポートされると、 AWS Resilience Hub は関連するリソースを同じ にグループ化するために最善を尽くしますが AppComponent、必ずしも 100% 正確であるとは限りません。さらに、アプリケーションとそのリソースが正常にインポートされた後、 は次のアクティビティ AWS Resilience Hub を実行します。

- リソースをスキャンして、評価の精度を向上させるために新しい AppComponents に再グループ化できるかどうかを確認します。
- が新しい に再グループ化できるリソース AWS Resilience Hub を識別すると AppComponents、レコメンデーションと同じ が表示され、同じ を承認、変更 (追加または削除) 、または拒否することができます。では AWS Resilience Hub、グループ化に関する推奨事項に割り当てられた信頼度は、属性とメタデータに基づいてリソースをグループ化する確実性の程度を示します。高い信頼レベル AWS Resilience Hub は、 の信頼レベルが 90% 以上の場合に、そのグループ内のリソースが関連しており、グループ化する必要があることを示します。中程度の信頼レベルは、 が 70% から 90% の間の信頼レベル AWS Resilience Hub を持ち、そのグループ内のリソースが関連しており、グループ化する必要があることを示します。

> **Note**
>
> AWS Resilience Hub では、推定ワークロードRTOと推定ワークロードを計算してレコメンデーションを生成できるようにRPO、正しいグループ化が必要です。

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 にグループ化します AppComponent。
- Amazon S3 バケットとそのターゲットレプリケーションを 1 つの 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 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 つの にグループ化します AppComponent。

- Amazon ECSサービスを 1 つのリージョンにグループ化し、1 つの で別のリージョンの Amazon ECSサービスをフェイルオーバーします AppComponent。

によるリソースグループ化のレコメンデーションの確認と含めの詳細については AWS Resilience Hub、以下のトピックを参照してください。

- AWS Resilience Hub リソースのグループ化に関する推奨事項
- リソースの への手動グループ化 AppComponent

AWS Resilience Hub リソースのグループ化に関する推奨事項

このセクションでは、 でリソースグループのレコメンデーションを生成して確認する方法について説明します AWS Resilience Hub。

> **Note**
>
> `AWSResilienceHubAsssessmentExecutionPolicy` AWS 管理ポリシー AWS Resilience Hub を使用して、 の操作に必要なIAMアクセス許可を付与できます。 AWS 管理ポリシーの詳細については、「」を参照してくださいAWSResilienceHubAsssessmentExecutionPolicy。

リソースグループ化の推奨事項を表示するには

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. 「アプリケーションの追加」ページを選択し、リソースグループ化の推奨事項を確認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. に情報アラート AWS Resilience Hub が表示される場合は、レコメンデーションの確認 を選択して、すべてのリソースグループのレコメンデーションを表示します。それ以外の場合は、次の手順を実行して、リソースグループ化の推奨事項を手動で生成します。

   a. [リソース] をクリックします。

   b. アクションメニューから「レコメンデーションのグループ化の取得」を選択します。

      AWS Resilience Hub は、リソースをスキャンして、評価の精度を向上させる AppComponents ために、可能な限り適切な方法でリソースをグループ化する方法を確認し

ます。がリソースをグループ化できることを AWS Resilience Hub 学習すると、同じ の情報アラートが表示されます。

c. 情報アラートが表示されたら、「レコメンデーションの確認」を選択して、すべてのリソースグループのレコメンデーションを表示します。

以下を使用して、「リソースグループ化のレコメンデーションの確認」セクション AppComponents で を識別できます。

- AppComponent name – リソース AppComponent がグループ化される の名前。
- 信頼度 – グループ化レコメンデーションの AWS Resilience Hub の信頼度を示します。
- リソース数 — でグループ化されるリソースの数を示します AppComponent。
- AppComponent type – のタイプを示します AppComponent。

でグループ化されるリソースを表示するには AppComponents

1. リソースグループ化の推奨事項を表示するには 手順のステップを完了し、この手順に戻ります。
2. 「リソースグループ化のレコメンデーションの確認」セクションで、チェックボックス (AppComponent 名前 に隣接) を選択して、選択した 内でグループ化されるすべてのリソースを表示します AppComponent。複数のチェックボックスを選択すると、 は、動的に生成されたレコメンデーションの選択したセクション AWS Resilience Hub を表示し、選択した をそれぞれの AppComponentタイプ AppComponents でグループ化します。各 AppComponent タイプの下にある番号を選択すると、選択した 内でグループ化されるすべてのリソースが表示されます AppComponent。

   以下を使用して、リソースセクション AppComponent で選択した にグループ化されるリソースを特定できます。

   - 論理 ID – リソースの論理 ID を示します。論理 ID は、AWS CloudFormation スタック、Terraform 状態ファイル、手動で追加されたアプリケーション、 AppRegistry アプリケーション、または 内のリソースを識別するために使用される名前です AWS Resource Groups。
   - 物理 ID – Amazon EC2インスタンス ID や Amazon S3 バケット名など、リソースに実際に割り当てられた識別子。
   - Type – リソースのタイプを示します。
   - リージョン — リソースが配置されている AWS リージョン。

リソースグループ化の推奨事項を受け入れるには

1. リソースグループ化の推奨事項を表示するには 手順のステップを完了し、この手順に戻ります。
2. 「リソースグループ化のレコメンデーションの確認」セクションで、AppComponent名前 の横にあるすべてのチェックボックスをオンにします。特定の を検索するには AppComponent、検索 AppComponentsボックスに名前を入力します AppComponent。

   > **Note**
   >
   > デフォルトでは、 はすべてのリソースグループのレコメンデーション AWS Resilience Hub を表示します。以前に拒否されたリソースグループのレコメンデーションでテーブルをフィルタリングするには、検索 AppComponentsボックスの横にあるドロップダウンメニューから「以前に拒否済み」を選択します。

3. [Accept (承諾)] を選択します。
4. リソースグループ化のレコメンデーションを受け入れるダイアログで Accept を選択します。

   AWS Resilience Hub は、リソースのグループ化が成功すると、情報アラートを表示します。リソースグループレコメンデーションのサブセットのみを受け入れた場合、リソースグループレコメンデーションの確認セクションには、受け入れていないすべてのリソースグループレコメンデーションが表示されます。

リソースグループ化の推奨事項を拒否するには

1. リソースグループ化の推奨事項を表示するには 手順のステップを完了し、この手順に戻ります。
2. 「リソースグループ化のレコメンデーションの確認」セクションで、AppComponent名前 の横にあるすべてのチェックボックスをオンにします。特定の を検索するには AppComponent、検索 AppComponentsボックスに名前を入力します AppComponent。

   > **Note**
   >
   > デフォルトでは、 はすべてのリソースグループのレコメンデーション AWS Resilience Hub を表示します。以前に拒否されたリソースグループのレコメンデーションでテーブルをフィルタリングするには、検索 AppComponentsボックスの横にあるドロップダウンメニューから「以前に拒否済み」を選択します。

3. [拒否] を選択します。
4. リソースグループレコメンデーションを拒否する理由のいずれかを選択し、リソースグループレコメンデーションを拒否ダイアログで拒否を選択します。

   AWS Resilience Hub は、同じことを確認する情報アラートを表示します。リソースグループレコメンデーションのサブセットのみを拒否した場合、リソースグループレコメンデーションの確認セクションには、承認されていないすべてのリソースグループレコメンデーションが表示されます。

リソースの への手動グループ化 AppComponent

このセクションでは、リソースを に手動でグループ化 AppComponent し、 のリソース AppComponent に異なる を割り当てる方法について説明します AWS Resilience Hub。

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. 論理 ID の横にあるチェックボックスをオンにして、グループ化するすべてのリソースを選択します。

   > **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。
8. リソース AppComponent をグループ化する を選択 AppComponent ドロップダウンリストから を選択します。
9. [Save] 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。

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. 論理 ID の横にあるチェックボックスをオンにして、リソースを選択します。
7. アクションから変更 AppComponentメニューを選択します。
8. AppComponent セクション AppComponent から現在の を削除するには、現在の AppComponent 名前を表示す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 にグループ化するには AppComponent、ドロップダウンリストから別の AppComponent AppComponentを選択します。
10. [追加] を選択します。
11. AppComponents タブ AppComponents から空の を削除します。
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。

新しい AWS Resilience Hub アプリケーションバージョンの公開

「」の説明に従って AWS Resilience Hub アプリケーションリソースを変更したらAWS Resilience Hub アプリケーションリソースの編集、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

障害耐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、、SOPsおよびテストをアプリケーションに追加した場合、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、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. [新しいバージョンを発行] を選択します。
5. バージョン発行ダイアログの「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、 で提案されているデフォルト名を使用できます AWS Resilience Hub。
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、そのバージョンが障害耐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、新しい障害耐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、「障害 AWS Resilience Hub 耐性評価の実行と管理」を参照してください。

すべての AWS Resilience Hub アプリケーションバージョンの表示

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

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する前にプラス記号 (+) を選択します。 は、ドラフトリリースステータスと現行リリースステータスをそれぞれ使用して、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 AWS Resilience Hub を示します。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、入力ソース AppComponent、およびその他の関連情報を表示できます。

さらに、次のオプションのいずれかを使用して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。
  - [相対範囲] – 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。

AWS Resilience Hub アプリケーションのリソースの表示

アプリケーションのリソースを表示するには

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

     > **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 “サポートされている AWS Resilience Hub リソース”を参照してください。

- [ステータス] – AWS Resilience Hub がリソースの障害耐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。例えば、 は Amazon EC2インスタンスを`AWS::EC2::Instance`宣言します。AppComponent リソースのグループ化の詳細については、「」を参照してくださいアプリケーションコンポーネントのリソースのグループ化。
- [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。例えば、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、 のスタックの詳細ページにリダイレクトされます AWS CloudFormation。
- [ソースタイプ] – 入力ソースのタイプ。
- AppComponent type – 入力ソースのタイプ。入力ソースには、 AWS CloudFormation AppRegistryスタック、アプリケーション AWS Resource Groups、Terraform 状態ファイル、および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、「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」の手順 AWS Resilience Hub 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 コンポーネント。
- [名前] – アプリケーションリソースの名前。
- アカウント – 物理リソースを所有する AWS アカウント。

4. [保存とテスト] を選択します。

AWS Resilience Hub 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付けられたリソースに関する追加情報を収集する入力メカニズムを提供します。この情報 AWS Resilience Hub により、 は リソースをより深く理解し、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] 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。例えば、フェイルオーバー構成などです。
- 目的 — が情報を AWS Resilience Hub リクエストした理由を示します。
- パラメータ – アプリケーションの領域に固有の詳細を示します。この詳細 AWS Resilience Hub を使用して、アプリケーションにレコメンデーションを提供します。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 つの関連付けられたアカウントのキー値のみを使用します。

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、 の設定パラメータを更新 AWS Elastic Disaster Recovery し、アプリケーションを発行して、障害耐性評価用に更新されたパラメータを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。

障害耐性ポリシーの管理

このセクションでは、アプリケーションの障害耐性ポリシーを作成する方法について説明します。障害耐性ポリシーを正しく設定することで、アプリケーションの障害耐性状態を把握できます。障害耐性ポリシーには、アプリケーションがソフトウェア、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回復すると推定されるかどうかを評価するために使用する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障害耐性ポリシーを適用することができます。

障害耐性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障害耐性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、障害耐性評価を実行します。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。例えば、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障害耐性ポリシーが適用されます。

> **Note**
>
> AWS Resilience Hub では、障害耐性ポリシーの RTO および RPO フィールドに値 0 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。

評価では、添付されている障害耐性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、 は、アプリケーションの障害耐性ポリシーの復旧ターゲットに対する測定方法の評価 AWS Resilience Hub を提供します。

障害耐性ポリシーは、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 のターゲットを使用して、これらの潜在的なタイプの中断に対する回復性を測定します。

- 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 では、カスタマイズされた障害耐性ポリシーを作成したり、推奨されるオープンスタンダードの障害耐性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、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。例えば、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障害耐性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。

障害耐性ポリシーは、障害耐性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。

障害耐性ポリシーの作成

では AWS Resilience Hub、障害耐性ポリシーを作成できます。障害耐性ポリシーには、アプリケーションがソフトウェア、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回復できるかどうかを評価するために使用する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障害耐性ポリシーを適用することができます。

障害耐性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、 は、アプリケーションが障害耐性ポリシーで定義されている目的を達成すると推定されるかどうか AWS Resilience Hub を決定します。

評価では、添付されている障害耐性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、 は、アプリケーションが障害耐性ポリシーの目的に対してどのように測定するかの評価 AWS Resilience Hub を提供します。

> **Note**
>
> AWS Resilience Hub では、障害耐性ポリシーの RTO および RPO フィールドに値 0 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。

障害耐性ポリシーは、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障害耐性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. [障害耐性ポリシー] セクションで、[障害耐性ポリシーの作成] を選択します。

   [障害耐性ポリシーの作成] ページが表示されます。
4. [作成方法の選択] セクションで、[ポリシーの作成] を選択します。
5. ポリシーの名前を入力します。
6. (オプション) 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 [アベイラビリティーゾーン] 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. (オプション) 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. (オプション) 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。

障害耐性ポリシーで障害耐性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. [障害耐性ポリシー] セクションで、[障害耐性ポリシーの作成] を選択します。

   [障害耐性ポリシーの作成] 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. (オプション) ポリシーの説明を入力します。
5. [ティア] 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. [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 [アベイラビリティーゾーン] 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. (オプション) 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。[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. (オプション) 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障害耐性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. [障害耐性ポリシー] セクションで、[障害耐性ポリシーの作成] を選択します。

   [障害耐性ポリシーの作成] 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. (オプション) ポリシーの説明を入力します。
6. [推奨障害耐性ポリシー] セクションで、以下の定義済みの障害耐性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. 障害耐性ポリシーを作成するには、[ポリシーの作成] を選択します。

障害耐性ポリシーの詳細へのアクセス

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

障害耐性ポリシーの詳細は、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]

障害耐性ポリシーについて、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

この障害耐性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。

障害耐性ポリシーの詳細で障害耐性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. 障害耐性ポリシーで、障害耐性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。

障害耐性ポリシーで障害耐性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. 障害耐性ポリシーで、障害耐性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。

障害耐性ポリシー詳細で障害耐性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. 障害耐性ポリシーで、障害耐性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。

障害耐性ポリシー内の障害耐性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. 障害耐性ポリシーで、障害耐性ポリシーを選択します。
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。

障害 AWS Resilience Hub 耐性評価の実行と管理

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。この評価では、各アプリケーションコンポーネント設定をポリシーと比較し、アラーム、SOP、テストのレコメンデーションを作成します。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 レコメンデーションは、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を提供します。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、また、指定した条件下での正常なSOPs動作をテストすることもできます。

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 “アプリケーションの管理”」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、、SOPsおよびテストを設定するための推奨事項
- AWS リソースを検索および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

確認

このセクションでは、評価 report. AWS Resilience Hub lists の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の概要を示します。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決定します。

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。

検出されたリソースドリフト

このセクションでは、公開されたアプリケーションの最新バージョンに含まれた後に追加または削除されたすべてのリソースを一覧表示します。入力ソースの再インポート を選択して、入力ソースタブのすべての入力ソース (ドリフトしたリソースを含む) を再インポートします。公開と評価を選択して、更新されたリソースをアプリケーションに含め、正確な障害耐性評価を受け取ります。

ドリフトした入力ソースは、以下を使用して識別できます。

- 論理 ID – リソースの論理 ID を示します。論理 ID は、 AWS CloudFormation スタック、Terraform 状態ファイル、手動で追加されたアプリケーション、 AppRegistry アプリケーション、または 内のリソースを識別するために使用される名前です AWS Resource Groups。
- 変更 — 入力リソースが を追加または削除されたかどうかを示します。
- ソース名 — リソース名を示します。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。例えば、 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、 のスタックの詳細ページにリダイレクトされます AWS CloudFormation。
- リソースタイプ — リソースタイプを示します。
- Account – 物理リソースを所有する AWS アカウントを示します。
- リージョン — リソースが配置されているリージョンを示します AWS 。

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。評価では、推定ワークロード が提供されますRTO。

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。評価では、推定ワークロード が提供されますRPO。

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 とターゲット RTOの 2 つの値を提供します。 RTO例えば、ターゲットの RTO に 2 番目の値が表示され、推定ワークロード に 40m と表示される場合は、アプリケーションの現在のワークロードが 2 時間であるのに対し、推定ワークロードは RTO 40 分RTOであることを示します。 RTO推定ワークロードRTO計算は、ポリシーではなく設定に基づいています。その結果、選択したポリシーに関係なく、マルチアベイラビリティーゾーンデータベースのアベイラビリティーゾーン障害RTOの推定ワークロードは同じになります。

- RTO ドリフト

  前回成功した評価RTOの推定ワークロードからアプリケーションがドリフトした時間を示します。推定RTOとRTOドリフトの 2 つの値を提供します。例えば、推定 に 2h RTO値、RTOドリフト に 40m と表示される場合は、アプリケーションが前回の成功した評価RTOの推定ワークロードから 40 分ドリフトすることを示します。

- 推定 RPO

  各アプリケーションコンポーネントに設定したターゲットRPOポリシーに基づいて AWS Resilience Hub 推定される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ターゲットを 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。

  指定しないことを選択できる唯一の RTOとRPOターゲットはリージョンです。一部のアプリケーションでは、 AWSサービスに重要な依存関係があり、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、復旧を計画すると便利です。

  リージョンの RTOまたは RPOターゲットの設定など、このオプションを選択すると、こ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

  前回成功した評価RPOの推定ワークロードからアプリケーションがドリフトした時間を示します。推定RPOとRPOドリフトの 2 つの値を提供します。例えば、推定 に 2h RPO値、RPOドリフト に 40m と表示される場合は、アプリケーションが前回の成功した評価RPOの推定ワークロードから 40 分ドリフトしていることを示します。

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RTOと推定ワークロード、コストRPO、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る必要がある理由」の以下の推奨オプションのいずれかを使用して、障害耐性を最適化できます。

> **Note**
>
> - AWS Resilience Hub には、最大 3 つの AWS Resilience Hub 推奨オプションがあります。
> - リージョンとRPOターゲットを設定するRTOと、推奨オプションにリージョン RTO/ の最適化RPO AWS Resilience Hub が表示されます。リージョンRTOとRPOターゲット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) の最適化RTO/RPO が表示されます。障害耐性ポリシーの作成中にリージョンRTO/RPOターゲットを設定する方法の詳細については、「」を参照してください障害耐性ポリシーの作成 。

- アプリケーションRTOとその設定の推定ワークロードと推定ワークロードRPO値は、データ量と個々の 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の最適化RTO/RPO

アベイラビリティーゾーン (AZRPO) の中断中の推定ワークロード復旧時間 (RTO/) の最小値。RTO および RPOの目標を達成するために設定を十分に変更できない場合は、推定される最小ワークロード AZ 復旧時間について通知され、設定がポリシーを満たす可能性に近づきます。

リージョン RTO/ に最適化するRPO

リージョンの中断時の推定ワークロード復旧時間 (RTO/RPO) が最も低くなります。RTO および RPOの目標を達成するために設定を十分に変更できない場合は、推定される最小ワークロードリージョン復旧時間について通知され、設定がポリシーを満たす可能性に近づきます。

コストに合わせた最適化

障害耐性ポリシーを満たしながら発生する可能性のある最低コスト。最適化目標を達成するために設定を十分に変更できない場合は、設定がポリシーを満たす可能性に近づく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必要な最小限の変更。最適化目標を達成するために設定を十分に変更できない場合は、ポリシーを満たす可能性に近い設定に推奨される変更について通知されます。

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

  によって提案される設定について説明します AWS Resilience Hub。
- 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

  推奨される変更に関連する推定コスト。

> **Note**
>
> 基本料金は使用量によって異なり、Enterprise Discount Program () の割引やオファーは含まれませんEDP。

- 推定ワークロードRTOと RPO

  変更RPO後の推定ワークロードRTOと推定ワークロード。

AWS Resilience Hub は、アプリケーションコンポーネント (AppComponent) が障害耐性ポリシーに準拠できるかどうかを評価します。 AppComponent が障害耐性ポリシーに準拠しておらず、AWSResilience Hub がコンプライアンスを容易にするためにレコメンデーションを作成できない場合、選択した の復旧時間を の制約内で満たす AppComponent ことができ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。

の障害耐性ポリシー AppComponent への準拠を容易にするには、 のリソースタイプを変更する AppComponent か、リソースが提供できる内容に合わせて障害耐性ポリシーを更新します。

運用上の推奨事項のレビュー

運用上の推奨事項には、 AWS CloudFormation テンプレートを使用してアラーム、SOPs、および AWS FIS 実験を設定するための推奨事項が含まれています。

AWS Resilience Hub は、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および管理するための AWS CloudFormation テンプレートファイルを提供します。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 以上で、500 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 のリソースを含む複数の AWS CloudFormation テンプレートファイル AWS Resilience Hub を生成します。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 、 AWS CloudFormation テンプレートファイル名には が付加されます。ここで`partXofY`、 `X`はシーケンス内のファイル番号を示し、はテンプレートファイルが分割された AWS CloudFormation ファイルの合計数`Y`を示します。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、大きな AWS CloudFormation テンプレートの場合は、/ を入力としてCLIローカルファイルで使用するURI代わりに、Amazon Simple Storage Service APIを提供するように求められます。

では AWS Resilience Hub、次のアクションを実行できます。

- 選択したアラーム、、SOPs AWS FIS および実験をプロビジョニングできます。アラーム、SOPs、および AWS FIS 実験をプロビジョニングするには、適切なレコメンデーションを選択し、一意の名前を入力します。 AWS Resilience Hub は、選択したレコメンデーション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) を使用して作成したテンプレートにアクセスできますURL。
- アプリケーションに推奨された選択したアラーム、SOPs、および AWS FIS 実験を任意の時点で含めたり除外したりできます。詳細については、「」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”。
- 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 には、アプリケーションの障害耐性スコアを向上させるために推奨されたアラームSOPs、、および AWS FIS 実験 (テスト) を任意の時点で含めたり除外したりするためのオプションが用意されています。運用上のレコメンデーションの包含と除外は、新しい評価を実行した後にのみ、アプリケーションの障害耐性スコアに影響します。したがって、評価を実行して、更新された障害耐性スコアを取得し、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。
      - 既に実装済み — Amazon などの AWS サービス、またはその他のサードパーティーサービスプロバイダーでこれらのアラームを既に実装している場合は CloudWatch、このオプションを選択します。
      - [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。

推奨される標準操作手順 (SOPs) 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 を除外するにはSOPs、次のステップを実行します。

a. 標準操作手順タブのSOPs表で、除外するすべての SOPs (実装済みまたは実装されていない状態) を選択します。の現在の実装状態は、State 列SOPから識別できます。

b. アクション から、選択した をアプリケーションSOPsから除外するには、選択した を除外を選択します。

c. 「レコメンデーションを除外する」ダイアログで、次のいずれかの理由 (オプション) を選択し、「選択した除外」を選択して、選択した をアプリケーションSOPsから除外します。

- 既に実装済み – AWS サービスや他のサードパーティーサービスプロバイダーSOPsにこれらを既に実装している場合は、このオプションを選択します。
- 関連なし — がビジネス要件に合SOPsわない場合は、このオプションを選択します。
- 実装が複雑すぎる – 実装が複雑すぎると思われる場合はSOPs、このオプションを選択します。
- [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. を含めるにはSOPs、次のステップを実行します。

a. 「標準操作手順」タブのSOPs表から、含めるすべてのアラーム (除外状態) を選択します。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 を含める」を選択して、選択したすべての をアプリケーションSOPsに含めます。

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。

- 既に実装済み — これらのテストを AWS サービスや他のサードパーティーサービスプロバイダーで既に実装している場合は、このオプションを選択します。

- [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

運用上の推奨事項 AWS Resilience Hub の一環として、障害耐性評価を実行する場合、 はアプリケーションの障害耐性をモニタリングするために Amazon CloudWatch アラームを設定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 の内部 (Amazon などREADME.md) または外部 で推奨され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 AWS。アラームで提供されるデフォルト値は、これらのアラームの作成に使用されるベストプラクティスに基づいています。

トピック

運用上の推奨事項からのアラームの作成

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

AWS Resilience Hub レコメンデーションに基づいてアラームを作成するには、レコメンデーションアラームのテンプレートを作成し AWS CloudFormation 、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 — が推奨するアラーム AWS Resilience Hub 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。
     - Not implemented – によって推奨されるアラーム AWS Resilience Hub は含まれているが、アプリケーションには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 — が推奨するアラーム AWS Resilience Hub 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 — アラームが Amazon にデプロイされているが CloudWatch、Amazon でステータスが 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。

- リファレンス ID – の AWS CloudFormation 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 — 内の AWS CloudFormation 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する推奨アラームを選択し、 CloudFormation テンプレートの作成 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、 AWS CloudFormation テンプレート名ボックスにCloudFormation テンプレートの名前を入力できます。
10. [Create] (作成) を選択します。これには、 AWS CloudFormation テンプレートの作成に数分かかる場合があります。

    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。

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

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。
   - 形式 – テンプレートが作成される形式 (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ARNの 。
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 コンソールの Objects テーブルからフォルダSOPリンクを選択します。
4. Amazon S3 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オンにし、コピーを選択しますURL。

5. AWS CloudFormation コンソールから AWS CloudFormation スタックを作成します。
   AWS CloudFormation スタックの作成の詳細については、「」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、前のステップからコピーした 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障害耐性を監視するために設定したすべてのアクティブなアラームを表示できます。 は AWS CloudFormation 、テンプレート AWS Resilience Hub を使用して、アラームの作成に使用されたアラームの詳細を Amazon に保存します CloudWatch。Amazon S3 を使用して AWS CloudFormation テンプレートにアクセスしURL、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。実装済みアラームテーブルでは、次の情報を使用して実装済み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 進行中 – アプリケーションに対して現在実行されている AWS FIS 実験を示します。

アプリケーションに実装されているアラームを表示するには

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 — が推奨するアラーム AWS Resilience Hub 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。
  - Not implemented – によって推奨されるアラーム AWS Resilience Hub は含まれているが、アプリケーションには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 — が推奨するアラーム AWS Resilience Hub 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 – アラームが Amazon にデプロイされているが CloudWatch、Amazon でステータスが 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 – アラームの詳細を含む AWS CloudFormation 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。
- メトリクス — 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 CloudWatch メトリクスの詳細については、「Amazon CloudWatch Metrics」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 — アラームが Amazon にデプロイされているが CloudWatch、Amazon でステータスが 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。
- リファレンス ID – の AWS CloudFormation 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 – 内の AWS CloudFormation スタックリソースの論理識別子を示します AWS CloudFormation。

標準運用手順の管理

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、 は準備すべき SOPs AWS Resilience Hub を推奨します。 AWS Resilience Hub は Systems Manager と連携して、SOPs 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、SOPs。

例えば、既存の SSM Automation 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 AWS Resilience Hub できます。この SSM ドキュメントを実行するには、正しいアクセス許可を持つ特定の IAM ロールが必要です。 は、ディスクが不足した場合に実行する SSM オートメーションドキュメントと、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 AWS Resilience Hub 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。したがって、 は SSM 自動化ドキュメントを呼び出す AWS FIS 実験 AWS Resilience Hub も提供します。このようにして、アプリケーションを事前にテストして、作成した SOP が意図したジョブを実行していることを確認することができます。

AWS Resilience Hub は、アプリケーションコードベースに追加できる AWS CloudFormation テンプレートの形式でレコメンデーションを提供します。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 のテストに使用できる AWS FIS 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。アプリケーションに対して障害耐性評価を実行し、 AWS Resilience Hub レコメンデーションから AWS CloudFormation テンプレートを生成するのが良いスタートです。 AWS CloudFormation テンプレートを使用して AWS CloudFormation スタックを生成し、SOP で SSM パラメータとそのデフォルト値を使用します。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。これにより、アプリケーションをデプロイするたびに、SOP も最も多くデプロイされます up-to-date 。

トピック

- AWS Resilience Hub 推奨事項に基づく SOP の構築
- カスタム SSM ドキュメントの作成
- 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 のテスト
- 標準操作手順を表示する

AWS Resilience Hub 推奨事項に基づく SOP の構築

AWS Resilience Hub 推奨事項に基づいて SOP を構築するには、障害耐性ポリシーがアタッチされた AWS Resilience Hub アプリケーションが必要であり、そのアプリケーションに対して障害耐性評価を実行している必要があります。障害耐性評価により、SOP の推奨事項が生成されます。

AWS Resilience Hub レコメンデーションに基づいて SOP を構築するには、レコメンデーション SOPs 用の AWS CloudFormation 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 レコメンデーションの AWS CloudFormation テンプレートを作成する

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. [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、[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。これには、 AWS CloudFormation 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。

レ AWS Resilience Hub 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、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 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 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. AWS CloudFormation コンソールから AWS CloudFormation スタックを作成します。AWS CloudFormation スタック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 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。

カスタム SSM ドキュメントの作成

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。

SSM ドキュメントアクションの自動化については、「Systems Manager Automation アク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 に AWS Resilience Hub 提案されている SSM ドキュメント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ます。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 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、 で推奨されるデフォルト値を操作し AWS Resilience Hub 、必要に応じてカスタマイズするのが最も効率的です。例えば、IAM ロールに必要なアクセス許可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 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できます。

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 実験を追加して SOPs を定期的にテストすることです。これにより、停止が発生した場合にすぐに実行できるようになります。

が提供する SOP AWS Resilience Hubとカスタム SOPs。

標準操作手順を表示する

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。

   [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. [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。サポートされている の詳細については AppComponents、「 でのリソースのグループ化 AppComponent」を参照してください。

- リファレンス ID — の AWS CloudFormation 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 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 実験の管理

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復旧にかかる時間を測定します。

障害耐性を測定するために、これらの AWS FIS 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、ネットワーク使用不可エラー、フェイルオーバー、Amazon EC2 または ASG AWS 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 実験が終了したら、障害耐性ポリシーの 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回復できるかどうかを推定できます。

のすべての実験 AWS Resilience Hub は を使用して構築 AWS FIS され、 AWS FIS アクションを実行します。 AWS FIS 実験の大部分は Systems Manager のオートメーションアクションを呼び出して中断を実行し、アラームをモニタリングします。他の AWS FIS 実験では、特定の AWS サービス (Amazon EKS アクションなど) にカスタマイズされた AWS FIS オートメーションアクションのみを使用します。 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 実験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 実験には AWS Resilience Hub （ the section called “故障注入実験を表示する”) または AWS FIS コンソール (AWS FIS) からアクセスできます。

トピック

- 運用上の推奨事項からの AWS FIS 実験の作成
- から AWS FIS 実験を実行する 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

運用上の推奨事項からの AWS FIS 実験の作成

AWS Resilience Hub では、評価レポートを実行した後にアプリケーションをテストすることをお勧めします。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 は、テストパラメータを含む Systems Manager ドキュメントである AWS FIS 実験のリストを提供します。リストから AWS FIS 実験を選択すると、 は Systems Manager ドキュメントで定義したパラメータを使用して AWS CloudFormation テンプレート AWS Resilience Hub を作成します。 AWS CloudFormation スタックの作成後、アプリケーションのプロビジョニングされた AWS FIS 実験を確認できます。

AWS CloudFormation テンプレートは、各 Systems Manager ドキュメントの IAM ロールと、実行に必要な最小限のアクセス許可で構成されます。

AWS Resilience Hub レコメンデーションに基づいて AWS FIS 実験を作成するには、レコメンデーションテスト用の AWS CloudFormation 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 FIS 実験用の AWS CloudFormation 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 テンプレートの作成 を選択します。これには、 AWS CloudFormation テンプレートの作成に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。

   新しく作成された AWS CloudFormation テンプレートは、テンプレートテーブルで表示できます。

   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。

レ AWS Resilience Hub 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、先ほど作成した AWS FIS 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 — テストが に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 – 実験の詳細を含む AWS CloudFormation 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 コンソールから AWS CloudFormation スタックを作成します。AWS CloudFormation スタックの作成の詳細については、「」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。

から AWS FIS 実験を実行する AWS Resilience Hub

アプリケーションでは、 が AWS FIS 実験 AWS Resilience Hub を実行する前に、運用上の推奨事項から AWS FIS 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 実験を停止するには

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 リソースの障害耐性と、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 リージョン インシデントからの復旧にかかる時間を測定するために設定した AWS FIS 実験を表示します。

ダッシュボードから AWS FIS 実験を表示するには、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。Experiments テーブルでは、次の情報を使用して実装された AWS FIS 実験を特定できます。

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

実装された AWS FIS 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 タブには、 AWS FIS Experiment テーブルにアクティブな実験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 実験の目的について説明します。
   - [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 FIS 実験の詳細を含む AWS CloudFormation 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。
     - 非アクティブ — テストが に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。サポートされている の詳細については AppComponents、「 でのリソースのグループ化 AppComponent」を参照してください。
   - [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。

- リファレンス ID — の AWS CloudFormation 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 — の AWS CloudFormation 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 では、開始した実験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

- Systems Manager を使用した AWS FISAWS 実験実行の分析
- AWS FIS Amazon Elastic Kubernetes Service 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

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

AWS FIS 実験を実行した後、Systems Manager で AWS 実行の詳細を表示できます。

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は、実行詳細の「入力パラメータ」セクションに表示され、 AWS FIS 実験に表示されないオプションパラメータが含まれます。

   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。
  - 修復： 個々のステップで予想される入出力を調べる前に、 AWS FIS 「実験実行の分析」で説明されているように、入力パラメータを確認し、実行されたステップを確認します。

AWS FIS Amazon Elastic Kubernetes Service 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 実験または Kubernetes サービスアカウントの IAM ロールの設定が正しくありません。
  - 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 FISaws: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 (テストの AWS CloudFormation スタックの出力を参照) を Kubernetes ユーザーにマッピングしていることを確認します。
- AWS FIS ポッドを起動できません: 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、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 AWS FIS 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障害耐性体制を表す障害耐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、標準運用手順 (SOPs) 、および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ています。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、および各中断タイプの一連のテスト 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。可能な限り最高のスコアまたはトップスコアを得るには、アプリケーションにすべての推奨アラーム、SOPs、およびテストを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 を含む 1 つのテスト AWS Resilience Hub を推奨しますSOP。テストが実行され、アラームが発せられ、関連する が開始されますSOP。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、、およびテストレコメンデーションの包含と除外の詳細についてはSOP、「」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”。

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。

   障害耐性スコアグラフには、アプリケーションの障害耐性スコアの傾向が最大 1 年間表示されます。 には、以下を使用して、可能な限り最大の障害耐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、障害耐性ポリシー違反、運用上の推奨事項 AWS Resilience Hub 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/RPOs) 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、修正が必要な 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。
  - SOPs – アプリケーションに実装SOPsする必要がある推奨 の数を示します。値を選択すると、修正が必要な SOPs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が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、推定ワークロード復旧時間と、アプリケーションの障害耐性ポリシーで定義されている目標復旧時間とどの程度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 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障害耐性スコアに対する最大の寄与度を比較します。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。
  - SOPs implemented – 実装された の実際の寄与度と、アプリケーションの障害耐性スコアに対する最大の寄与度SOPs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SOPsに実装されている が表示されます。
  - FIS 実装された実験 – 実装されたテストの実際の寄与度と、アプリケーションの障害耐性スコアに対する最大の寄与度を示します。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。
  - SOPs – 実装SOPsする必要がある推奨 の数を示します。
  - FIS – 実装する必要が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る推奨 Amazon CloudWatch アラームの数を示します。
  - SOPs – アプリケーションから除外SOPsされる推奨 の数を示します。
  - FIS – アプリケーションから除外され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障害耐性スコアを決定する AWS Resilience Hub ために が使用す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障害耐性スコア AWS Resilience Hub について によって決定される結果値はすべて、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` を介してのみ取得できますAPI。この の詳細については、API「」を参照してくださいScoringComponentResiliencyScore。

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 中断タイプの障害耐性スコアを計算する式

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 が使用する式を示しています。

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** 障害耐性スコアを計算するには、 が実装済みと見なす AWS Resilience Hub ために、推奨されるテストが過去 30 日間に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 AWS CloudFormation コンソールで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。 • 推奨されるテストの総数 — アプリケーションリソース AWS Resilience Hub に基づいて が推奨するテストを示します。	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`

スコアリングコンポーネント	説明	計算式	例
		• [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。	

スコアリングコンポーネント	説明	計算式	例
アラームカバレッジ (A)	AWS Resilience Hub 推奨される Amazon CloudWatch アラームの総数のうち、正常に実装および除外された 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。	`A = ((Total number of alarms implemented) + (Total number 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総数 – AWS CloudFormation テンプレートが AWS CloudFormation コンソールで作成およびアップロードされたときに設定された Amazon CloudWatch アラームの総数を示します。 • 推奨されるアラームの総数 — 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 Amazon CloudWatch アラームを示します。 • 除外されたアラームの総数 — 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。	20 個の AWS Resilience Hub 推奨 Amazon CloudWatch アラームのうち 10 個を実装し、5 個の Amazon CloudWatch アラームを除外した場合、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 推奨される の総数のうち、正常に実装および除外SOPsされた の数に基づく正規化されたスコア (0 ~ 100 ポイント) SOPs。	`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。 • SOPs 設定された の総数 — AWS CloudFormation テンプレートが AWS CloudFormation コンソールで作成およびアップロードされたときにSOPs設定された の総数を示します。 • SOPs 推奨される の総数 — アプリケーションリソース AWS Resilience Hub に基づいて が SOPs推奨する を示します。 • SOPs 除外された の総数 — アプリケーションから除外SOPsした推奨の数を示します。	20 個の推奨 SOPs のうち 10 AWS Resilience Hub 個を実装し、5 個を除外した場合SOPs、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。 • リージョン RTO と RPOターゲット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` • リージョン別ターゲットRTO と RPOターゲットを設定していない場合、 Pは次のように計算されます。

スコアリングコンポーネント	説明	計算式	例
			P = (22.22 + 33.33)/ 99.9 つまり、P = .55 or 55 points

次の表は、アプリケーション全体の障害耐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

スコアリングコンポーネント	説明	計算式	例
			アプリケーションごとの障害耐性ス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) と中断タイプの障害耐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。ただし、 AppComponents および 中断タイプの障害耐性スコアは、次の AWS Resilience Hub からのみ取得できますAPIs。

- DescribeAppAssessment 取得する RSo
- ListAppComponentCompliances RSaoと を取得するには RSA

AppComponents および 中断タイプの障害耐性スコアを計算する式

スコアリングコンポーネント	説明	計算式	例
AppComponent 中断タイプごとの障	中断タイプごとの障害耐性ポリシー AppCompon	中断タイプごとの障害耐性スコアは AppComponent 、次の式を使用して計算されます。	すべての推奨タイプの RSao の前提条件は次のとおりです。

スコアリングコンポーネント	説明	計算式	例
害耐性スコア (RSao)	ent を満たすことに基づく正規化されたスコア (0～100 ポイント)。中断タイプ AppComponent ごとの障害耐性スコアは、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 中断タイプのすべての推奨テスト、アラーム、SOPs、および対応障害耐性ポリシーに対してT, A, S, P計算されます。	RSao = (T * Weight(T) + A * Weight(A) + S * Weight(S) + P * Weight(P)) / (Weight(T) + Weight(A) + Weight(S) + Weight(P))	• Test coverage (T) = .75 • Alarms (A) = .75 • SOPs (S) = .75 • Meeting resiliency policy (P) = .5 AppComponent および の中断タイプあたりの障害耐性スコアは、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

AppComponent (RSa) あたりの障害耐性スコア	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)。あたりの障害耐性スコア 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T, A, S, P、すべての推奨テスト、アラーム、、SOPs および の障害耐性ポリシーを満たすために計算されます AppComponent。
		あたりの障害耐性スコア 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`
			
			あたりの障害耐性スコア 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) の値はT, A, S, P、すべての推奨テスト、アラーム、、SOPs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ます。	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、総障害耐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、、テストSOPs、障害耐性ポリシーへの対応、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**
>
> ポリシーにリージョンRTOまたはRPOターゲットを定義しない場合、リージョンが定義されていない場合の重み列に示すように、他の中断タイプの重みがそれに応じて増加します。

アラーム、、テストSOPs、ポリシーターゲットの重み

推奨事項の種類	(重量)
アラーム	20 ポイント
SOPs	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

と運用上の推奨事項をアプリケーションに統合する AWS CloudFormation

「運用上の推奨事項」ページで CloudFormation 「テンプレートの作成 AWS Resilience Hub 」を選択すると、 はアプリケーションの特定のアラーム、標準操作手順 (SOP) 、または AWS FIS 実験を記述する AWS CloudFormation テンプレートを作成します。 AWS CloudFormation 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。

例えば、以下のリストは、 によってレンダリングされたアラームレコメンデーションを記述する JSON形式の AWS CloudFormation テンプレートを示しています AWS Resilience Hub。これは、Employees という 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、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することなく AWS Resilience Hub 、 がインストール済み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 Amazon SNS topic to which alarm status changes
 are to be sent. This must be in the same Region being deployed.",
      "AllowedPattern" : "^arn:(aws|aws-cn|aws-iso|aws-iso-[a-z]{1}|aws-us-gov):sns:
([a-z]{2}-((iso[a-z]{0,1}-)|(gov-)){0,1}[a-z]+-[0-9]):[0-9]{12}:[A-Za-z0-9/][A-Za-
z0-9:_/+=,@.-]{1,256}$"
    }
  },
  "Resources" : {

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

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

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

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

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

AWS CloudFormation テンプレートの変更

アラーム、、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 SOP、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。以下の JSON形式のファイルは、DynamoDB テーブルが AWS CloudFormation 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提供します。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"
```

次のように変更します。

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

AWS::SSM::Parameter のリソース定義で以下を変更します。

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

次のように変更します。

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

SOPs および AWS FIS 実験の AWS CloudFormation テンプレートを変更する場合も、ハードコードされた参照IDsを、ハードウェアが変更された後も引き続き機能する動的な参照に置き換え、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と、 AWS CloudFormation で次の操作を実行できます。

- 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 をアラームで常に使用し、 AWS CloudFormation がリソースを置き換える必要がある場合はアラームを動的に更新します。

> **Note**
>
> スタックのネストや別のスタックのリソース出力の参照など、 で AWS CloudFormation アプリケーションリソースを管理するためのより高度な方法を選択できます。 AWS CloudFormation(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、 による Terraform などのサードパーティーツールを使用して HashiCorp、Infrastructure as Code (IaC) をプロビジョニングすることもできます。

を使用した AWS Resilience Hub APIs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ための代替方法として、 AWS Resilience Hub を使用すると、 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 AWS Resilience Hub APIs。この章では、 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 AWS Resilience Hub APIs。また、 を実行する必要があるシーケンスAPIsと、適切な例を指定する必要があるパラメータ値も定義します。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 “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、障害耐性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 の詳細については AWS Resilience Hub APIs、以下のトピックを参照してください。

- the section called “アプリケーションの作成”
- the section called “障害耐性ポリシーの作成”
- 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障害耐性ポリシーの割り当て”

アプリケーションを作成する

で新しいアプリケーションを作成するには AWS Resilience Hub、 を呼び出し`CreateApp`API、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 の詳細については、API「」を参照してくださいhttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_CreateApp.html。

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

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"
    }
}
```

障害耐性ポリシーの作成

アプリケーションを作成したら、 を使用してアプリケーションの障害耐性体制を理解できるようにする障害耐性ポリシーを作成する必要がありますCreateResiliencyPolicyAPI。この の詳細については、API「」を参照してくださいhttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_CreateResiliencyPolicy.html。

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

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 では、 リソースAPIsをアプリケーションにインポートするために、以下が用意されています。

- `ImportResourcesToDraftAppVersion` – API これにより、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 の詳細については、API「」を参照してくださいhttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_ImportResourcesToDraftAppVersion.html。
- `PublishAppVersion` – これにより、更新された API とともにアプリケーションの新しいバージョンが公開されます AppComponents。この の詳細については、API「」を参照してくださいhttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_PublishAppVersion.html。
- `DescribeDraftAppVersionResourcesImportStatus` – API これにより、アプリケーションバージョンへのリソースのインポートステータスをモニタリングできます。この の詳細については、API「」を参照してくださいhttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_DescribeDraftAppVersionResourcesImportStatus.html。

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

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、 AWS Resilience Hub を使用して CreateAppVersionResource で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API。

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"
            }
        ]
    }
}
```

次の例は、 AWS Resilience Hub を使用して でリソースのインポートステータスをモニタリングする方法を示していますDescribeDraftAppVersionResourcesImportStatusAPI。

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障害耐性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障害耐性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、障害耐性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公開するには、 PublishAppVersion を使用しますAPI。この の詳細については、API「」を参照してくださいhttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_PublishAppVersion.html。

   次の例は、 AWS Resilience Hub を使用して で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PublishAppVersionAPI。

   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. を使用して、アプリケーションのリリース済みバージョンに障害耐性ポリシーを適用しますUpdateAppAPI。この の詳細については、API「」を参照してくださいhttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_UpdateApp.html。

   次の例は、 AWS Resilience Hub を使用して のアプリケーションのリリース済みバージョンに障害耐性ポリシーを適用する方法を示していますUpdateAppAPI。

   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 障害耐性評価の実行と管理

アプリケーションの新しいバージョンを公開したら、新しい障害耐性評価を実行し、結果を分析して、アプリケーションが推定ワークロードRTOを満たしRPO、障害耐性ポリシーで定義されている推定ワークロードを満たしていることを確認する必要があります。この評価では、各アプリケーションコンポーネント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 “障害耐性評価の実行と監視”
- the section called “障害耐性ポリシーの作成”

AWS Resilience Hub 障害耐性評価の実行と監視

で障害耐性評価を実行し AWS Resilience Hub 、そのステータスをモニタリングするには、次の を使用する必要がありますAPIs。

- `StartAppAssessment` – これにより、アプリケーションの新しい評価APIが作成されます。この の詳細については、API「」を参照してくださいhttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_StartAppAssessment.html。
- `DescribeAppAssessment` — アプリケーションの評価APIについて説明し、評価の完了ステータスを示します。この の詳細については、API「」を参照してくださいhttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_DescribeAppAssessment.html。

次の例は、 を使用して で AWS Resilience Hub 新しい評価の実行を開始する方法を示していますStartAppAssessmentAPI。

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": {}
    }
}
```

次の例は、 AWS Resilience Hub を使用して DescribeAppAssessment で評価のステータスをモニタリングする方法を示していますAPI。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 を使用して評価結果を確認できますAPIs。

- `DescribeAppAssessment` – API これにより、障害耐性ポリシーに照らしてアプリケーションの現在のステータスを追跡できます。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障害耐性スコアを抽出したりすることもできます。この の詳細については、API「」を参照してくださいhttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_DescribeAppAssessment.html。
- `ListAlarmRecommendations` – API これにより、評価の Amazon リソースネーム (ARN) を使用してアラームのレコメンデーションを取得できます。この の詳細についてはAPI、「」を参照してくださいhttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_ListAlarmRecommendations.html。

> **Note**
>
> SOP および FISテストの推奨事項を取得するには、 `ListSopRecommendations`および `ListTestRecommendations` を使用しますAPIs。

次の例は、 を使用して評価の Amazon リソースネーム (ARN) `ListAlarmRecommendations` を使用してアラームレコメンデーションを取得する方法を示していますAPI。

> **Note**
>
> SOP および FISテストの推奨事項を取得するには、 を `ListSopRecommendations`または に置き換えます`ListTestRecommendations`。

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 Amazon CloudWatch Synthetics is setup to monitor
 the application (see the <a href=\"https://docs.aws.amazon.com/AmazonCloudWatch/
latest/monitoring/CloudWatch_Synthetics_Canaries.html\" target=\"_blank\">docs</a>).
 \nMake sure that the Synthetics Name passed in the alarm dimension matches the name of
 the Synthetic Canary. It Defaults to the name of the application.\n"
        },
        {
            "recommendationId": "d9c72c58-8c00-43f0-ad5d-0c6e5332b84b",
            "referenceId": "efs:alarm:percent_io_limit:2020-04-01",
            "name": "AWSResilienceHub-EFSHighIoAlarm_2020-04-01",
            "description": "An alarm by AWS Resilience Hub that reports when Amazon EFS
 I/O load is more than 90% for too much time",
            "type": "Metric",
            "appComponentName": "storageappcomponent-rlb",
            "items": [
                {
                    "resourceId": "fs-0487f945c02f17b3e",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ]
        },
```

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

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

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

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

次の例は、 を使用して設定の推奨事項 (現在の障害耐性を向上させる方法に関する推奨事項) を取得する方法を示していますListAppComponentRecommendationsAPI。

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
Amazon EFS file system. No data loss is expected as objects are be stored in multiple
AZs."
                        },
                        "Hardware": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 0,
                            "expectedRtoDescription": "No expected downtime. You're
launching using EC2, with DesiredCount > 1 and CapacityProviders with MinSize > 1",
                            "expectedRpoInSecs": 0,
                            "expectedRpoDescription": "ECS Service state is saved on
Amazon EFS file system. No data loss is expected as objects are be stored in multiple
AZs."
                        },
                        "Software": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": " Estimated time to restore
cluster with volumes. (Estimate is based on averages, real time restore may vary).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Based on the frequency of the
backups"
                        }
                    },
```

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

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

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

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

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

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


ステップ 3: アプリケーションを変更する

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、新しい (公開された) バージョンに変更を公開することで、アプリケーションリソースを変更できます。 AWS Resilience Hub は、更新されたリソースを含むアプリケーションの公開バージョンを使用して、障害耐性評価を実行します。

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 “からのリソースの除外 AppComponent”

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 を使用して手動でリソースをアプリケーションに追加できますCreateAppVersionResourceAPI。この の詳細についてはAPI、「」を参照してくださいhttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_CreateAppVersionResource.html。

この には、次のパラメータを指定する必要がありますAPI。

- 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 タイプ

次の例は、 AWS Resilience Hub を使用して CreateAppVersionResource で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API。

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動作および失敗する関連 AWS リソースのグループです。例えば、スタンバイデプロイとして使用されるクロスリージョンワークロードがある場合、 には、どの AWS リソースがどのタイプの に属できるかを規定するルール AWS Resilience Hub があります AppComponent。 AWS Resilience Hub では、次のリソース管理 AppComponent を使用して、リソースを 1 つの にグループ化できますAPIs。

- `UpdateAppVersionResource` – これにより、アプリケーションのリソースの詳細がAPI更新されます。この の詳細については、API「」を参照してくださいUpdateAppVersionResource。
- `DeleteAppVersionAppComponent` – これにより、アプリケーション AppComponent から がAPI削除されます。この の詳細についてはAPI、「」を参照してくださいDeleteAppVersionAppComponent。

次の例は、 AWS Resilience Hub を使用して でアプリケーションのリソースの詳細を更新する方法を示していますDeleteAppVersionAppComponentAPI。

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"
    }
}
```

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

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"
    }
}
```

からのリソースの除外 AppComponent

AWS Resilience Hub では、 UpdateAppVersionResource を使用して評価からリソースを除外できますAPI。これらのリソースは、アプリケーションの障害耐性を計算する際には考慮されません。

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

> **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、 AWS Resilience Hub を使用して で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UpdateAppVersionResourceAPI。

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

のクラウドセキュリティが最優先事項 AWS です。お客様は AWS 、セキュリティを最も重視する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からメリットを得られます。

セキュリティは、 AWS とユーザー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 — クラウドで AWS 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 AWS は AWS にあります。 AWS また、 では、安全に使用できるサービスも提供しています。コンプライアンスAWS プログラムコンプライアンスプログラム の一環として、サードパーティーの監査者は定期的にセキュリティの有効性をテストおよび検証。に適用されるコンプライアンスプログラムの詳細については AWS Resilience Hub、「コンプライアンスプログラムAWS による対象範囲内のサービスコンプライアンスプログラム」を参照してください。
- クラウドのセキュリティ — お客様の責任は、使用する AWS 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、 を使用する際の責任共有モデルの適用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、セキュリティおよびコンプライアンスの目的 AWS Resilience Hub を達成するために を設定する方法を示します。また、 AWS Resilience Hub リソースのモニタリングや保護に役立つ他の AWS のサービスの使用方法についても説明します。

内容

- でのデータ保護 AWS Resilience Hub
- AWS Resilience Hub の Identity and Access Management
- のインフラストラクチャセキュリティ AWS Resilience Hub

でのデータ保護 AWS Resilience Hub

責任 AWS 共有モデル、 でのデータ保護に適用されます AWS Resilience Hub。このモデルで説明されているように、 AWS はすべての を実行す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 AWS クラウド。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 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 FAQ」を参照してください。欧州におけるデータ保護の詳細については、AWS 「 セキュリティブログ」のAWS 「責任共有モデル」とGDPRブログ記事を参照してください。

データ保護の目的で、認証情報を保護し AWS アカウント 、 AWS IAM Identity Center または AWS Identity and Access Management () 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IAM。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 AWS リソースと通信します。1TLS.2 が必要で、1.3 TLS をお勧めします。
- を使用して APIおよびユーザーアクティビティのログ記録を設定します AWS CloudTrail。
- AWS 暗号化ソリューションと、 内のすべてのデフォルトのセキュリティコントロールを使用します AWS サービス。
- 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 AWS を介して にアクセスするときに FIPS 140-3 検証済みの暗号化モジュールが必要な場合はAPI、FIPSエンドポイントを使用します。利用可能なFIPS エンドポイントの詳細については、「連邦情報処理標準 (FIPS) 140-3」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。これは、コンソール、、またはを使用して Resilience Hub または他の AWS サービス を使用する場合API AWS CLIも同様です AWS SDKs。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。URL を外部サーバーに提供する場合は、そのサーバーへのリクエストを検証URLするために認証情報を に含めないことを強くお勧めします。

保管中の暗号化

AWS Resilience Hub は保管中のデータを暗号化します。のデータは AWS Resilience Hub 、保管時に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 は、 サービスと他の統合 AWS サービスの間で転送中のデータを暗号化します。 AWS Resilience Hub と統合サービス間を通過するすべてのデータは、Transport Layer Security () を使用して暗号化されますTLS。 は、 AWS サービス全体で特定のタイプのターゲットに対して事前設定されたアクション AWS Resilience Hub を提供し、ターゲットリソースのアクションをサポートします。

AWS Resilience Hub の Identity and Access Management

AWS Identity and Access Management （ IAM) は、管理者が AWS リソースへのアクセスを安全に制御 AWS サービス するのに役立つ です。IAM 管理者は、誰を認証 (サインイン) し、誰に AWS Resilience Hub リソースの使用を承認する (アクセス許可を付与する) かを制御します。IAM は、追加料金なしで AWS サービス 使用できる です。

トピック

- 対象者
- アイデンティティを使用した認証
- ポリシーを使用したアクセスの管理
- AWS Resilience Hub と の連携方法 IAM
- IAM ロールとアクセス許可の設定
- AWS Resilience Hub のアイデンティティとアクセスのトラブルシューティング
- AWS Resilience Hub アクセス許可リファレンス
- AWS の マネージドポリシー AWS Resilience Hub
- AWS Resilience Hub ペルソナとIAMアクセス許可のリファレンス
- Terraform 状態ファイルの へのインポート AWS Resilience Hub
- Amazon Elastic Kubernetes Service クラスター AWS Resilience Hub へのアクセスの有効化
- AWS Resilience Hub を有効にして Amazon Simple Notification Service トピックに発行する
- AWS Resilience Hub レコメンデーションを含めるまたは除外するためのアクセス許可の制限

対象者

AWS Identity and Access Management （ IAM) の使用方法は、 AWS Resilience Hub で行う作業によって異なります。

サービスユーザー – ジョブを実行するために AWS Resilience Hub サービスを使用する場合、管理者から必要な認証情報とアクセス許可が与えられます。さらに多くの AWS Resilience Hub 機能を使用して作業を行う場合は、追加のアクセス許可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 のアイデンティティとアクセスのトラブルシューティング。

サービス管理者 – 社内の AWS Resilience Hub リソースを担当している場合は、通常、Resilience AWS Hub へのフルアクセスがあります。サービスユーザーがどの AWS Resilience Hub 機能やリソースにアクセスするかを決めるのは管理者の仕事です。次に、サービスユーザーのアクセス許可を変更するリクエストをIAM管理者に送信する必要があります。このページの情報を確認して、 の基本概念を理解してくださいIAM。会社で AWS Resilience Hub IAMを使用する方法の詳細については、「」を参照してくださいAWS Resilience Hub と の連携方法 IAM。

IAM 管理者 – IAM管理者は、 AWS Resilience Hub へのアクセスを管理するポリシーの作成方法の詳細について確認する場合があります。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表示するにはIAM、「」を参照してくださいAWS Resilience Hub のアイデンティティベースのポリシーの例。

アイデンティティを使用した認証

認証とは、ID 認証情報 AWS を使用して にサインインする方法です。として、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ロールを引き受けることによって認証 （ にサインイン AWS) される必要があります。

ID ソースを介して提供された認証情報を使用して、フェデレーティッド ID AWS として にサインインできます。 AWS IAM Identity Center （ IAM Identity Center) ユーザー、会社のシングルサインオン認証、Google または Facebook の認証情報は、フェデレーティッド ID の例です。フェデレーティッド ID としてサインインすると、管理者は以前に IAMロールを使用して ID フェデレーションをセットアップしていました。フェデレーション AWS を使用して にアクセスすると、間接的にロールを引き受けることになります。

ユーザーのタイプに応じて、 AWS Management Console または AWS アクセスポータルにサインインできます。へのサインインの詳細については AWS、「 ユーザーガイド」の「 にサインインする方法 AWS アカウントAWS サインイン 」を参照してください。

AWS プログラムで にアクセスする場合、 は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、認証情報を使用してリクエストに暗号で署名します。 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。推奨される方法を使用してリクエストを自分で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。例えば、 AWS では、アカウントのセキュリティを高めるために多要素認証 (MFA) を使用することをお勧めします。詳細については、「 AWS IAM Identity Center ユーザーガイド」の「多要素認証」および「 ユーザーガイド」の「 での多要素認証 (MFA) AWS IAM の使用」を参照してください。

AWS アカウント ルートユーザー

を作成するときは AWS アカウント、アカウント内のすべての およびリソースへの AWS サービス 完全なアクセス権を持つ 1 つのサインインアイデンティティから始めます。この ID は AWS アカウント ルートユーザーと呼ばれ、アカウントの作成に使用した E 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できます。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「ルートユーザーの認証情報を必要とするタスク」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、一時的な認証情報を使用して にアクセスするための ID プロバイダーとのフェデレーションの使用を要求 AWS サービス します。

フェデレーティッド ID 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、AWS Directory Service、アイデンティティセンターディレクトリのユーザー、または ID ソースを通じて提供された認証情報 AWS サービス を使用して にアクセスするユーザーです。フェデレーティッド ID が にアクセスすると AWS アカウント、ロールを引き受け、ロールは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することも、独自の ID ソース内のユーザーとグループのセットに接続して同期して、すべての AWS アカウント とアプリケーションで使用できるようにすることもできます。IAM Identity Center の詳細については、「 ユーザーガイド」のIAM「Identity Center とはAWS IAM Identity Center 」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、単一のユーザーまたはアプリケーションに対して特定のアクセス許可 AWS アカウント を持つ 内のアイデンティティです。可能な場合は、パスワードやアクセスキーなどの長期的な認証情報を持つIAMユーザーを作成するのではなく、一時的な認証情報を使用することをお勧めします。ただし、IAMユーザーとの長期的な認証情報を必要とする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、「 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でアクセスキーを定期的にローテーションするIAM」を参照してください。

IAM グループは、IAMユーザーのコレクション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、 という名前のグループを作成しIAMAdmins、そのグループにIAMリソースを管理するアクセス許可を付与できます。

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、ロールでは一時認証情報が提供されます。詳細については、「 ユーザーガイド」のIAM「 (ロールではなく) ユーザーを作成する場合IAM」を参照してください。

IAM ロール

IAM ロールは、特定のアクセス許可 AWS アカウント を持つ 内のアイデンティティです。これは IAM ユーザーと似ていますが、特定のユーザーに関連付けられていません。IAM ロール を切り替える AWS Management Console ことで、 で ロールを一時的に引き受けることができます。ロールを引き受けるには、 または AWS API オペレーションを AWS CLI 呼び出すか、カスタム を使用しますURL。ロールの使用方法の詳細については、「 ユーザーガイド」のIAM「ロールの使用IAM」を参照してください。

IAM 一時的な認証情報を持つ ロールは、以下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 ID に許可を割り当てるには、ロールを作成してそのロールの許可を定義します。フェデレーティッド ID が認証されると、その ID はロールに関連付けられ、ロールで定義されている許可が付与されます。フェデレーションのロールの詳細については、「 ユーザーガイド」の「サードパーティー ID プロバイダーのロールの作成IAM」を参照してください。IAM Identity Center を使用する場合は、アクセス許可セットを設定します。ID が認証後にアクセスできる内容を制御するために、IAMIdentity Center はアクセス

許可セットを のロールに関連付けますIAM。アクセス許可セットの詳細については、「AWS IAM Identity Center ユーザーガイド」の「アクセス許可セット」を参照してください。

- 一時的なIAMユーザーアクセス許可 – IAM ユーザーまたはロールは、 IAMロールを引き受けて、特定のタスクに対して異なるアクセス許可を一時的に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、別のアカウントのユーザー (信頼されたプリンシパル) がアカウントのリソースにアクセスすることを許可できます。クロスアカウントアクセスを許可する主な方法は、ロールを使用することです。ただし、一部の では AWS サービス、(ロールをプロキシとして使用する代わりに) ポリシーをリソースに直接アタッチできます。クロスアカウントアクセスのロールとリソースベースのポリシーの違いについては、「 ユーザーガイド」の「 でのクロスアカウントリソースアクセスIAMIAM」を参照してください。
- クロスサービスアクセス — 一部の は、他の の機能 AWS サービス を使用します AWS サービス。例えば、サービスで呼び出しを行うと、そのサービスが Amazon でアプリケーションを実行EC2したり、Amazon S3 にオブジェクトを保存したりするのが一般的です。サービスでは、呼び出し元プリンシパルの許可、サービスロール、またはサービスリンク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 でアクションを実行すると AWS、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、 を呼び出すプリンシパルのアクセス許可を AWS サービス、ダウンストリームサービス AWS サービス へのリクエストのリクエストと組み合わせて使用します。FAS リクエストは、サービスが他の AWS サービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するための権限が必要です。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 – サービスロールは、ユーザーに代わってアクションを実行するためにサービスが引き受ける IAMロールです。IAM 管理者は、 内からサービスロールを作成、変更、削除できますIAM。詳細については、「 ユーザーガイド」の「 にアクセス許可を委任するロールの作成 AWS サービスIAM」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、 にリンクされたサービスロールの一種です AWS 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。サービスにリンクされたロールは に表示され AWS アカウント 、サービスによって所有されます。IAM 管理者は、サービスにリンクされたロールのアクセス許可を表示できますが、編集することはできません。
- Amazon で実行されているアプリケーション EC2 – IAMロールを使用して、EC2インスタンスで実行され、 AWS CLI または AWS API 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インスタンス内にアクセスキーを保存するよりも望ましいです。 AWS ロールをEC2インスタンスに割り当て、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た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 ロールが含まれており、EC2インスタンスで実行されているプログラムが一時的な認証情報を取得できるようにします。詳細については、「 ユーザーガイド」の「 IAMロールを使用して Amazon EC2インスタンスで実行されているアプリケーションにアクセス許可を付与するIAM」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、「 ユーザーガイド」の「 (ユーザーではなく) IAMロールを作成する場合IAM」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

でアクセスを制御する AWS には、ポリシーを作成し、 AWS ID またはリソースにアタッチします。ポリシーは AWS 、アイデンティティまたはリソースに関連付けられているときにアクセス許可を定義する のオブジェクトです。 は、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きに、これらのポリシー AWS 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ドキュメント AWS として に保存されます。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、「 ユーザーガイド」のJSON「ポリシーの概要IAM」を参照してください。

管理者はポリシーを使用して AWS JSON、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のリソースに対してどのような条件下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。必要なリソースに対してアクションを実行するアクセス許可をユーザーに付与するために、IAM管理者はIAMポリシーを作成できます。その後、管理者はIAMポリシーをロールに追加し、ユーザーはロールを引き受けることができます。

IAM ポリシーは、オペレーションの実行に使用するメソッドに関係なく、アクションのアクセス許可を定義します。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ーは、 AWS Management Console、、 AWS CLIまたは AWS からロール情報を取得できますAPI。

アイデンティティベースのポリシー

ID ベースのポリシーは、IAMユーザー、ユーザーのグループ、ロールなどの ID にアタッチできるJSONアクセス許可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、「 ユーザーガイド」のIAM「ポリシーの作成IAM」を参照してください。

アイデンティティベースのポリシーは、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、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 管理ポリシーとカスタマー管理ポリシーが含まれます。管理ポリシーとインラインポリシーのどちらかを選択する方法については、IAM ユーザーガイドの「管理ポリシーとインラインポリシーの選択」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、リソースにアタッチする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の例としては、IAMロールの信頼ポリシー や Amazon S3 バケットポリシー などがあります。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コントロールできます。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、ユーザー、ロール、フェデレーティッドユーザー、または を含めることができます AWS 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。リソースベースのポリシーIAMでは、 の AWS 管理ポリシーを使用できません。

アクセスコントロールリスト (ACLs)

アクセスコントロールリスト (ACLs) は、リソースへのアクセス許可を持つプリンシパル (アカウントメンバー、ユーザー、またはロール) を制御します。ACLs 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を使用しません。

Amazon S3、 AWS WAF、および Amazon VPCは、 をサポートするサービスの例ですACLs。の詳細についてはACLs、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 は、一般的ではない追加のポリシータイプをサポートします。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がIAMエンティティ (IAMユーザーまたはロール) に付与できるアクセス許可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 (SCPs) – SCPsは、 の組織または組織単位 (OU) に対する最大アクセス許可を指定するJSONポリシーです AWS Organizations。 AWS Organizations は、 AWS アカウント ビジネスが所有する複数の 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 (SCPs) をアカウントの一部またはすべてに適用できます。は、各 を含むメンバーアカウントのエンティティのアクセス許可SCP を制限します AWS アカウントのルートユーザー。Organizations と の詳細についてはSCPs、「 AWS Organizations ユーザーガイド」の「サービスコントロールポリシー」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、「 ユーザーガイド」の「セッションポリシーIAM」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。複数のポリシータイプが関与する場合にリクエストを許可するかどうか AWS を決定する方法については、「 ユーザーガイド」の「ポリシー評価ロジックIAM」を参照してください。

AWS Resilience Hub と の連携方法 IAM

IAM を使用して AWS Resilience Hub へのアクセスを管理する前に、Resilience AWS Hub で使用できるIAM機能を確認してください。

IAM AWS Resilience Hub で使用できる機能

IAM 機能	AWS Resilience Hub のサポート
アイデンティティベースのポリシー	あり
リソースベースのポリシー	なし
ポリシーアクション	あり
ポリシーリソース	はい
ポリシー条件キー (サービス固有)	あり
ACLs	なし
ABAC (ポリシー内のタグ)	部分的
一時的な認証情報	あり
転送アクセスセッション (FAS)	あり
サービスロール	あり

AWS Resilience Hub およびその他の AWS のサービスがほとんどの IAM 機能と連携する方法の概要を把握するには、IAM「 ユーザーガイド」のAWS 「 と連携する のサービスIAM」を参照してください。

AWS Resilience Hub の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のポリシーのサポート: あり

ID ベースのポリシーは、IAMユーザー、ユーザーのグループ、ロールなどの ID にアタッチできるJSONアクセス許可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、「 ユーザーガイド」のIAM「ポリシーの作成IAM」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、許可または拒否されたアクションとリソース、およびアクションが許可または拒否され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、「 ユーザーガイド」の「 IAMJSONポリシー要素のリファレンスIAM」を参照してください。

AWS Resilience Hub のアイデンティティベースのポリシーの例

AWS Resilience Hub のアイデンティティ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AWS Resilience Hub のアイデンティティベースのポリシーの例。

AWS Resilience Hub 内のリソースベースのポリシー

リソースベースのポリシーのサポート: なし

リソースベースのポリシーは、リソースにアタッチする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の例としては、IAMロールの信頼ポリシー や Amazon S3 バケットポリシー などがあります。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コントロールできます。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、ユーザー、ロール、フェデレーティッドユーザー、または を含めることができます AWS サービス。

クロスアカウントアクセスを有効にするには、リソースベースのポリシーのプリンシパルとして、アカウント全体または別のアカウントのIAMエンティティを指定できます。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 にある場合 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許可も付与する必要があります。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さらに付与する必要はありません。詳細については、「 ユーザーガイド」の「 でのクロスアカウントリソースアクセスIAMIAM」を参照してください。

AWS Resilience Hub のポリシーアクション

ポリシーアクションのサポート: あり

管理者はポリシーを使用して AWS JSON、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のリソースに対してどのような条件下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要素は、ポリシーで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を記述します。ポリシーアクションの名前は通常、関連する AWS APIオペレーションと同じです。一致するAPIオペレーションがないアクセス許可のみのアクションなど、いくつかの例外があります。また、ポリシーに複数の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を確認するには、「サービス認証リファレンス」の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 のアイデンティティ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AWS Resilience Hub のアイデンティティベースのポリシーの例。

AWS Resilience Hub のポリシーリソース

ポリシーリソースのサポート: あり

管理者はポリシーを使用して AWS JSON、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のリソースに対してどのような条件下でアクションを実行できるかということです。

Policy ResourceJSON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、リソースレベルの許可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 リソースタイプとその のリストを確認するにはARNs、「サービス認証リファレンス」のAWS 「Resilience Hub で定義されるリソース」を参照してください。各リソースARNのを指定できるアクションについては、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 のアイデンティティ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AWS Resilience Hub のアイデンティティベースのポリシーの例。

AWS Resilience Hub のポリシー条件キー

サービス固有のポリシー条件キーのサポート: あり

管理者はポリシーを使用して AWS JSON、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、どのリソースに対してどのような条件下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 要素を指定する場合、または 1 つの Condition 要素に複数のキーを指定する場合、 AWS では 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、 は論理ORオペレーションを使用して条件 AWS 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ユーザー名でタグ付けされている場合にのみ、リソースにアクセスするアクセス許可をIAMユーザーに付与できます。詳細については、「 ユーザーガイド」のIAM「ポリシー要素: 変数とタグIAM」を参照してください。

AWS は、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。すべての AWS グローバル条件キーを確認するには、「 ユーザーガイド」のAWS 「 グローバル条件コンテキストキーIAM」を参照してください。

AWS Resilience Hub の条件キーのリストを確認するには、「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 のアイデンティティ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AWS Resilience Hub のアイデンティティベースのポリシーの例。

ACLs AWS Resilience Hub の

をサポートACLs： いいえ

アクセスコントロールリスト (ACLs) は、リソースへのアクセス許可を持つプリンシパル (アカウントメンバー、ユーザー、またはロール) を制御します。ACLs 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を使用しません。

ABAC AWS Resilience Hub を使用する

サポート ABAC (ポリシー内のタグ): 部分的

属性ベースのアクセスコントロール (ABAC) は、属性に基づいてアクセス許可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。タグは、IAMエンティティ (ユーザーまたはロール) および多くの AWS リソースにアタッチできます。エンティティとリソースのタグ付けは、の最初のステップですABAC。次に、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する場合に、オペレーションを許可するABACポリシーを設計します。

ABAC は、急速に成長している環境や、ポリシー管理が煩雑になる状況に役立ちます。

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ありです。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。

の詳細についてはABAC、「 IAMユーザーガイド」の「 とはABAC」を参照してください。のセットアップ手順を含むチュートリアルを表示するにはABAC、「 ユーザーガイド」の「属性ベースのアクセスコントロール (ABAC) 」を使用するIAM」を参照してください。

AWS Resilience Hub での一時的な認証情報の使用

一時的な認証情報のサポート: あり

一部の は、一時的な認証情報を使用してサインインすると機能 AWS サービス しません。一時的な認証情報 AWS サービス を使用する などの詳細については、 ユーザーガイドのAWS サービス「 と連携する IAM IAM 」を参照してください。

ユーザー名とパスワード以外の AWS Management Console 方法で にサインインする場合、一時的な認証情報を使用します。例えば、会社のシングルサインオン (SSO) リンク AWS を使用して にアクセスすると、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。ロールの切り替えの詳細については、「 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。

一時的な認証情報は、 AWS CLI または を使用して手動で作成できます AWS API。その後、これらの一時的な認証情報を使用して . AWS recommends にアクセスできます AWS。これは、長期的な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推奨しています。詳細については、「」の「一時的なセキュリティ認証情報IAM」を参照してください。

AWS Resilience Hub の転送アクセスセッション

転送アクセスセッションをサポート (FAS): はい

IAM ユーザーまたはロールを使用して でアクションを実行すると AWS、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、 を呼び出すプリンシパルのアクセス許可を AWS サービス、ダウンストリームサービス AWS サービス へのリクエストのリクエストと組み合わせて使用します。FAS リクエストは、サービスが他の AWS サービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するための権限が必要です。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 Resilience Hub のサービスロール

サービスロールのサポート: あり

サービスロールは、ユーザーに代わってアクションを実行するためにサービスが引き受ける IAM ロールです。IAM 管理者は、 内からサービスロールを作成、変更、削除できますIAM。詳細につい

ては、「 ユーザーガイド」の「 にアクセス許可を委任するロールの作成 AWS サービスIAM」を参照してください。

> **Warning**
>
> サービスロールのアクセス許可を変更すると、 AWS Resilience Hub の機能が破損する可能性があります。 AWS Resilience Hub が指示する場合以外は、サービスロールを編集しないでください。

AWS Resilience Hub のアイデンティティベースのポリシーの例

デフォルトでは、ユーザーとロールには Resilience Hub AWS リソースを作成または変更するアクセス許可はありません。また、、 AWS Command Line Interface （ AWS CLI ） AWS Management Console、または を使用してタスクを実行することはできません AWS API。必要なリソースに対してアクションを実行するアクセス許可をユーザーに付与するために、IAM管理者はIAMポリシーを作成できます。その後、管理者はIAMポリシーをロールに追加し、ユーザーはロールを引き受けることができます。

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

ARNs 各リソースタイプの の形式など、 AWS Resilience Hub で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
- AWS Resilience Hub コンソールの使用
- 自分の権限の表示をユーザーに許可する
- 利用可能な AWS Resilience Hub アプリケーションの一覧表示
- アプリケーション評価の開始
- アプリケーション評価の削除
- 特定のアプリケーション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レコメンデーションテンプレートの削除
- 特定の障害耐性ポリシーを使用したアプリケーションの更新

ポリシーのベストプラクティス

ID ベースのポリシーは、ユーザーのアカウントで誰かが AWS Resilience Hub リソースを作成、アクセス、または削除できる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 管理ポリシーを開始し、最小特権のアクセス許可に移行する – ユーザーとワークロードにアクセス許可を付与するには、多くの一般的なユースケースにアクセス許可を付与する AWS 管理ポリシーを使用します。これらは で使用できます AWS アカウント。ユースケースに固有の AWS カスタマー管理ポリシーを定義して、アクセス許可をさらに減らすことをお勧めします。詳細については、「 ユーザーガイド」の「 AWS 管理ポリシー」または「 ジョブ機能の 管理ポリシーIAM」を参照してください。 AWS
- 最小特権のアクセス許可を適用する – IAMポリシーでアクセス許可を設定する場合は、タスクの実行に必要なアクセス許可のみを付与します。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、最小特権アクセス許可とも呼ばれています。IAM を使用してアクセス許可を適用する方法の詳細については、「 ユーザーガイド」の「 のポリシーとアクセス許可IAMIAM」を参照してください。
- IAM ポリシーの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、アクションと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 を使用して送信する必要があることを指定できますSSL。条件を使用して、 などの特定の を介してサービスアクションが使用される場合に AWS サービス、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、「 ユーザーガイド」のIAMJSON「ポリシー要素: 条件IAM」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、安全で機能的なアクセス許可を確保する – IAM Access Analyzer は、ポリシーがポリシー言語 (JSON) とIAMベストプラクティスに準拠するように、新規および既存のIAMポリシーを検証します。IAM Access Analyzer には、安全で機能的なポリシーの作成に役立つ 100 を超えるポリシーチェックと実用的な推奨事項が用意されています。詳細については、「 ユーザーガイド」のIAM「Access Analyzer ポリシーの検証IAM」を参照してください。
- 多要素認証を要求する (MFA) – でIAMユーザーまたはルート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MFAするために をオンにします。API オペレーションが呼び出されるMFAタイミングを要求するには、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「 で保護されたAPIアクセスの設定」を参照してください。

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「 のセキュリティのベストプラクティスIAMIAM」を参照してください。

AWS Resilience Hub コンソールの使用

AWS Resilience Hub コンソールにアクセスするには、最小限のアクセス許可が必要です。これらのアクセス許可により、 の AWS Resilience Hub リソースの詳細をリストおよび表示できます 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 のみを呼び出すユーザーには、最小限のコンソールアクセス許可を付与する必要はありません AWS API。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を許可します。

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、エンティティに AWS Resilience Hub *ConsoleAccess*または *ReadOnly* AWS 管理ポリシーもアタッチします。詳細については、「 ユーザーガイド」の「ユーザーへのアクセス許可の追加IAM」を参照してください。

次のポリシーは、 AWS Resilience Hub コンソールですべてのリソースを一覧表示および表示するアクセス許可をユーザーに付与しますが、作成、更新、削除することはできません。

```
{
     "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、IAMユーザーがユーザー ID にアタッチされているインラインポリシーと管理ポリシーを表示できるようにするポリシーを作成する方法を示します。このポリシーには、コンソールで、ま

たは AWS CLI または を使用してプログラムでこのアクションを実行するアクセス許可が含まれています AWS API。

```
{
    "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 AWS Resilience Hub アプリケーションの一覧表示

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": [
        "*"
      ]
    }
  ]
}
```

アプリケーション評価の開始

次のポリシーは、特定の AWS Resilience Hub アプリケーションの評価を開始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:StartAppAssessment"
      ],
      "Resource": [
        "arn:aws:resiliencehub:*:*:app/appId"
      ]
    }
  ]
}
```

アプリケーション評価の削除

次のポリシーは、特定の AWS Resilience Hub アプリケーションの評価を削除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:DeleteAppAssessment"
      ],
      "Resource": [
        "arn:aws:resiliencehub:*:*:app/appId"
      ]
    }
  ]
}
```

特定のアプリケーション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、特定の AWS Resilience Hub アプリケーションのレコメンデーションテンプレートを作成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:CreateRecommendationTemplate"
      ],
      "Resource": [
        "arn:aws:resiliencehub:*:*:app/appId"
      ]
    }
  ]
}
```

特定のアプリケーションのレコメンデーションテンプレートの削除

次のポリシーは、特定の AWS Resilience Hub アプリケーションのレコメンデーションテンプレートを削除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:DeleteRecommendationTemplate"
      ],
      "Resource": [
        "arn:aws:resiliencehub:*:*:app/appId"
      ]
    }
  ]
}
```

特定の障害耐性ポリシーを使用したアプリケーションの更新

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 ロールとアクセス許可の設定

AWS Resilience Hub では、アプリケーションの評価の実行時に使用する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 は、アプリケーションのリソースにアクセスするためにこのロールを引き受けます。

  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ための読み取り専用アクセス許可 (AWS Resilience Hub `AWSResilienceHubAsssessmentExecutionPolicy`マネージドポリシーの使用を推奨) 。
  - このロールを引き受けるための信頼ポリシー。これにより、 AWS Resilience Hub サービスプリンシパルはこのロールを引き受けることができます。アカウントにこのようなロールが設定されていない場合、 AWS Resilience Hub はそのロールを作成する手順を表示します。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、 AWS Resilience Hub は他のアカウントの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ARNs他のアカウントのロールを設定できます。

- 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、 AWS Resilience Hub はリソースにアクセスするために次のIAMロールを引き受けます。

  - 現在のアカウントでの `AwsResilienceHubAdminAccountRole`
  - 他のアカウントでの `AwsResilienceHubExecutorAccountRole`

  さらに、スケジュールされた評価を設定すると、 AWS Resilience Hub が`AwsResilienceHubPeriodicAssessmentRole`ロールを引き受けます。ただし、ロールとアクセス許可を手動で設定する必要があり、一部の機能 (ドリフト通知 など) `AwsResilienceHubPeriodicAssessmentRole`が期待どおりに動作しない可能性があるため、の使用はお勧めしません。

AWS Resilience Hub のアイデンティティとアクセスのトラブルシューティング

以下の情報は、 AWS Resilience Hub と の使用時に発生する可能性がある一般的な問題の診断と修正に役立ちますIAM。

トピック

- AWS Resilience Hub でアクションを実行する権限がない
- iam を実行する権限がありません。PassRole
- 自分の 以外のユーザーに AWS Resilience Hub リソース AWS アカウント へのアクセスを許可したい

AWS Resilience Hub でアクションを実行する権限がない

「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。

次の例のエラーは、mateojacksonIAMユーザーが コンソールを使用して架空の*my-example-widget*リソースの詳細を表示しようとしているが、架空のresiliencehub:*GetWidget*アクセス許可がない場合に発生します。

```
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 管理者にお問い合わせください。サインイン認証情報を提供した担当者が管理者です。

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、ポリシーを更新して Resilience Hub AWS にロールを渡すことができるようにする必要があります。

一部の AWS サービス では、新しい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作成する代わりに、そのサービスに既存のロールを渡すことができます。そのためには、サービスにロールを渡す権限が必要です。

次の例のエラーは、 というIAMユーザーがコンソールを使用して AWS Resilience marymajor Hub でアクションを実行しようする場合に発生します。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。メアリーには、ロールをサービスに渡す許可がありません。

```
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、 AWS 管理者にお問い合わせください。サインイン認証情報を提供した担当者が管理者です。

自分の 以外のユーザーに AWS Resilience Hub リソース AWS アカウント 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コントロールリスト (ACLs) をサポートするサービスでは、これらのポリシーを使用して、ユーザーにリソースへのアクセスを許可できます。

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を確認するには、「」を参照してくださいAWS Resilience Hub と の連携方法 IAM。
- 所有している のリソースへのアクセスを提供する方法については、 AWS アカウント 「 ユーザーガイド」の「所有 AWS アカウント している別の のIAMユーザーへのアクセスを提供するIAM」を参照してください。
- リソースへのアクセスをサードパーティー 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「サードパーティー AWS アカウント が所有する へのアクセスを提供する」を参照してください。
- ID フェデレーションを通じ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「外部認証されたユーザーへのアクセスの提供 (ID フェデレーション)」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については、「 ユーザーガイド」の「 でのクロスアカウントリソースアクセスIAMIAM」を参照してください。

AWS Resilience Hub アクセス許可リファレンス

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。

すべての AWS Resilience Hub 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ユーザーアクセス許可 (クロスアカウントおよびスケジュールされた評価用の事前定義されたロールのセット) を使用するように設定できます。このロールでは、 が他のリソースまたはアプリケーション AWS リソースにアクセス AWS Resilience Hub するために必要なアクセス許可を定義するポリシーをアタッチできます。呼び出しロールには、 AWS Resilience Hub サービスプリンシパル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 マネージドポリシー”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 ロールの使用”
- the section called “現在のIAMユーザーアクセス許可の使用”

IAM ロールの使用

AWS Resilience Hub は、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/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 “クロス AWS アカウントアクセスのための異なるアカウントのロール”

呼び出しロール

AWS Resilience Hub 呼び出しロールは、 が AWS サービスとリソースにアクセスするために引き受ける AWS Identity and Access Management AWS Resilience Hub (IAM) ロールです。例えば、CFN テンプレートとそのテンプレートが作成するリソースにアクセスするためのアクセス許可を持つ呼び出しロールを作成できます。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。が呼び出しロールを適切に引き受け AWS Resilience Hub るには、ロールの信頼ポリシーで AWS Resilience Hub サービスプリンシパル (resiliencehub.amazonaws.com) を信頼された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 コンソールでの呼び出しロールの作成”
- the section called “を使用したロールの管理 IAM API”
- the section called “JSON ファイルを使用した信頼ポリシーの定義”

IAM コンソールでの呼び出しロールの作成

AWS Resilience Hub が 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に呼び出し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たロールの作成の詳細については、「 AWS サービスのロールの作成 (コンソール) 」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で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 アクセスiam:passRole許可が必要です。ただし、評価を実行するのにこの権限は必要ありません。

を使用したロールの管理 IAM API

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、ロールを引き受けるプリンシパル許可を AWS Resilience Hub サービスに付与する方法を示しています。

> **Note**
>
> JSON 文字列内の引用符 (' ') をエスケープする要件は、シェルのバージョンによっ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

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。ロールにアクセス許可を追加するには、 attach-policy-to-role コマンドを使用します。まず、 `AWSResilienceHubAsssessmentExecutionPolicy`マネージドポリシーを追加します。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
```

クロス AWS 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/リソースアカウントにある場合は、これらの各アカウントにロールを作成して、 AWS Resilience Hub がアプリケーションを正常に評価できるように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 “を使用したロールの管理 IAM API”
- 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 が他の AWS アカウントの 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、これらの各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コンソールで作成するには

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"
      ]
}
```

を使用したロールの管理 IAM API

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、ロールを引き受けるアクセス許可を AWS Resilience Hub 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 文字列内の引用符 (' ') をエスケープする要件は、シェルのバージョンによっ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"}]}'
```

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

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。ロールにアクセス許可を追加するには、 attach-policy-to-role コマンドを使用します。まず、 AWSResilienceHubAsssessmentExecutionPolicyマネージドポリシーを追加します。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ユーザーアクセス許可の使用

現在のIAMユーザーアクセス許可を使用して評価を作成および実行する場合は、この方法を使用します。AWSResilienceHubAsssessmentExecutionPolicy 管理ポリシーは、IAMユーザーまたはユーザーに関連付けられたロールにアタッチできます。

単一アカウントの設定

上記の管理ポリシーを使用すると、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のに十分です。

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 がスケジュールされた評価関連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ている AWS アカウントであり、評価を実行します。さらに、スケジュールされた評価のロールに関連付けられた信頼ポリシー (AwsResilienceHubPeriodicAssessmentRole) を追加する必要があります。これにより、 AWS Resilience Hub サービスがスケジュールされた評価のロールを引き受けるアクセス許可が付与されます。

```
{
  "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アクセス許可ポリシーが必要です。アカウントごとに、ユースケースに応じて異なるアクセス許可が必要になる AWS 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。
- セカンダリ/リソースアカウント (複数可) – リソースが配置されている AWS アカウント (複数可) 。

> **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クラスター AWS Resilience Hub へのアクセスの有効化”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AwsResilienceHubAdminAccountRoleで新しいロールを作成し、そのロールを引き受ける AWS Resilience Hub アクセスを有効にする必要があります。このロールは、リソースを含む AWS アカウント内の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アクセスiam:assumeRole許可が必要です。
- 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。

次のポリシーは、アカウントの別のロールのリソースにアクセスするための エグゼキュターアクセス許可をロールに提供します AWS 。

```
{
  {
  "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 によってアプリケーションリソースの AWS Resilience Hub スキャンと評価に使用されるため、適切なアクセス許可も必要です。

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 マネージドポリシー 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ポリシーです AWS。 AWS 管理ポリシーは、多くの一般的なユースケースに対するアクセス許可を付与するように設計されているため、ユーザー、グループ、ロールへのアクセス許可の割り当てを開始できます。

AWS 管理ポリシーは、すべての AWS お客様が使用できるため、特定のユースケースに対して最小特権のアクセス許可を付与し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アクセス許可は変更できません。が AWS 管理ポリシーで定義されたアクセス許可 AWS を更新すると、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) が更新されます。 AWS サービス は、新しい AWS が起動されたとき、または既存のサービスで新しいAPIオペレーションが使用可能になったときに、 AWS 管理ポリシーを更新する可能性が最も高くなります。

詳細については、「 ユーザーガイド」の「 AWS 管理ポリシーIAM」を参照してください。

AWSResilienceHubAsssessmentExecutionPolicy

ID `AWSResilienceHubAsssessmentExecutionPolicy`に IAM をアタッチできます。このポリシーは、評価の実行中に、評価を実行するためのアクセス許可を他の AWS サービスに付与します。

アクセス許可の詳細

このポリシーは、Amazon Simple Storage Service (Amazon S3) バケットにアラーム AWS FIS と SOPテンプレートを発行するための適切なアクセス許可を提供します。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 バケットに発行する場合は、 CreateRecommendationTemplate を呼び出すときに発行できますAPI。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) – アプリケーションをモニタリング CloudWatch するために Amazon で設定したすべての実装済みアラームを取得します。さらに、cloudwatch:PutMetricDataを使用して、 ResilienceHub名前空間内のアプリケーションの障害耐性スコアの CloudWatch メトリクスを公開します。
- Amazon Data Lifecycle Manager – AWS アカウントに関連付けられている Amazon Data Lifecycle Manager リソースのDescribeアクセス許可を取得して提供します。
- Amazon DevOpsGuru – AWS アカウントに関連付けられている Amazon DevOpsGuru リソースのDescribeアクセス許可を一覧表示して提供します。
- Amazon DocumentDB – アカウント AWS に関連付けられている Amazon DocumentDB リソースのDescribeアクセス許可を一覧表示して提供します。
- 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) – AWS アカウントに関連付けられている ElastiCache リソースのDescribeアクセス許可を提供します。
- Amazon Elastic Compute Cloud (Amazon EC2) – アカウント AWS に関連付けられている Amazon EC2リソースのDescribeアクセス許可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リソースのDescribeアクセス許可を提供します。
- Amazon Elastic Container Service (Amazon ECS) – AWS アカウントに関連付けられている Amazon ECSリソースのDescribeアクセス許可を提供します。
- Amazon Elastic File System (Amazon EFS) – AWS アカウントに関連付けられている Amazon EFS リソースのDescribeアクセス許可を提供します。
- Amazon Elastic Kubernetes Service (Amazon EKS) – アカウント AWS に関連付けられている Amazon EKSリソースのDescribeアクセス許可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 リソースのDescribeアクセス許可を一覧表示して提供します。
- Amazon EC2 Systems Manager (SSM) – AWS アカウントに関連付けられているSSMリソースのDescribeアクセス許可を提供します。

- Amazon Fault Injection Service (AWS FIS) – AWS アカウントに関連付けられている AWS FIS 実験と実験テンプレートのDescribeアクセス許可を一覧表示して提供します。
- Amazon FSx for Windows File Server (Amazon FSx) – アカウント AWS に関連付けられている Amazon FSxリソースのDescribeアクセス許可を一覧表示して提供します。
- Amazon RDS – AWS アカウントに関連付けられている Amazon RDSリソースのDescribeアクセス許可を一覧表示して提供します。
- 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 – AWS アカウントに関連付けられている Amazon Route 53 Resolver リソースのDescribeアクセス許可を一覧表示して提供します。
- Amazon Simple Notification Service (Amazon SNS) – アカウント AWS に関連付けられている Amazon SNSリソースのDescribeアクセス許可を一覧表示して提供します。
- Amazon Simple Queue Service (Amazon SQS) – アカウント AWS に関連付けられている Amazon SQSリソースのDescribeアクセス許可を一覧表示して提供します。
- Amazon Simple Storage Service (Amazon S3) – アカウント AWS に関連付けられている Amazon S3 リソースのDescribeアクセス許可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があるアクセス許可が欠落している場合、 AWS Resilience Hub は s3:GetBucketLogging permission を使用して評価を正常に完了します。ただし、 AWS Resilience Hub は、不足しているアクセス許可を一覧表示する警告メッセージを表示し、それを追加する猶予期間を提供します。指定された猶予期間内に不足しているアクセス許可を追加しないと、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 リソースのDescribeアクセス許可を一覧表示して取得します。
- AWS CloudFormation – アカウントに関連付けられている AWS CloudFormation スタック上のリソースのDescribeアクセス許可を一覧表示して取得します AWS 。
- AWS DataSync – AWS アカウントに関連付けられている AWS DataSync リソースのDescribeアクセス許可を一覧表示して提供します。
- AWS Directory Service – AWS アカウントに関連付けられている AWS Directory Service リソースのDescribeアクセス許可を一覧表示して提供します。
- 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 Recovery リソースのDescribeアクセス許可を提供します。

- AWS Lambda (Lambda) – アカウント AWS に関連付けられている Lambda リソースのDescribeアクセス許可を一覧表示して提供します。
- AWS Resource Groups （ リソースグループ) — アカウント AWS に関連付けられている Resource Groups リソースのDescribeアクセス許可を一覧表示して提供します。
- AWS Service Catalog (Service Catalog) — アカウント AWS に関連付けられている Service Catalog リソースのDescribeアクセス許可を一覧表示して提供します。
- AWS Step Functions – AWS アカウントに関連付けられている AWS Step Functions リソースのDescribeアクセス許可を一覧表示して提供します。
- Elastic Load Balancing – AWS アカウントに関連付けられている Elastic Load Balancing リソースのDescribeアクセス許可を一覧表示して提供します。
- ssm:GetParametersByPath – このアクセス許可は、アプリケーション用に設定された CloudWatch アラーム、テスト、または SOPs を管理するために使用されます。

評価の実行中にチームから AWS のサービスにアクセスするために必要なアクセス許可を付与するユーザー、ユーザーグループ、ロールのアクセス許可を AWS アカウントに追加するには、次のIAMポリシーが必要です。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSResilienceHubFullResourceStatement",
            "Effect": "Allow",
            "Action": [
                "application-autoscaling:DescribeScalableTargets",
                "autoscaling:DescribeAutoScalingGroups",
                "backup:DescribeBackupVault",
                "backup:GetBackupPlan",
                "backup:GetBackupSelection",
                "backup:ListBackupPlans",
                "backup:ListBackupSelections",
                "cloudformation:DescribeStacks",
                "cloudformation:ListStackResources",
                "cloudformation:ValidateTemplate",
                "cloudwatch:DescribeAlarms",
                "cloudwatch:GetMetricData",
                "cloudwatch:GetMetricStatistics",
                "datasync:DescribeTask",
                "datasync:ListLocations",
```

```
                "datasync:ListTasks",
                "devops-guru:ListMonitoredResources",
                "dlm:GetLifecyclePolicies",
                "dlm:GetLifecyclePolicy",
                "docdb-elastic:GetCluster",
                "docdb-elastic:GetClusterSnapshot",
                "docdb-elastic:ListClusterSnapshots",
                "docdb-elastic:ListTagsForResource",
                "drs:DescribeJobs",
                "drs:DescribeSourceServers",
                "drs:GetReplicationConfiguration",
                "ds:DescribeDirectories",
                "dynamodb:DescribeContinuousBackups",
                "dynamodb:DescribeGlobalTable",
                "dynamodb:DescribeLimits",
                "dynamodb:DescribeTable",
                "dynamodb:ListGlobalTables",
                "dynamodb:ListTagsOfResource",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeFastSnapshotRestores",
                "ec2:DescribeFleets",
                "ec2:DescribeHosts",
                "ec2:DescribeInstances",
                "ec2:DescribeNatGateways",
                "ec2:DescribePlacementGroups",
                "ec2:DescribeRegions",
                "ec2:DescribeSnapshots",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeVolumes",
                "ec2:DescribeVpcEndpoints",
                "ecr:DescribeRegistry",
                "ecs:DescribeCapacityProviders",
                "ecs:DescribeClusters",
                "ecs:DescribeContainerInstances",
                "ecs:DescribeServices",
                "ecs:DescribeTaskDefinition",
                "ecs:ListContainerInstances",
                "ecs:ListServices",
                "eks:DescribeCluster",
                "eks:DescribeFargateProfile",
                "eks:DescribeNodegroup",
                "eks:ListFargateProfiles",
                "eks:ListNodegroups",
```

```
                "elasticache:DescribeCacheClusters",
                "elasticache:DescribeGlobalReplicationGroups",
                "elasticache:DescribeReplicationGroups",
                "elasticache:DescribeSnapshots",
                "elasticfilesystem:DescribeFileSystems",
                "elasticfilesystem:DescribeLifecycleConfiguration",
                "elasticfilesystem:DescribeMountTargets",
                "elasticfilesystem:DescribeReplicationConfigurations",
                "elasticloadbalancing:DescribeListeners",
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticloadbalancing:DescribeTargetGroups",
                "elasticloadbalancing:DescribeTargetHealth",
                "fis:GetExperimentTemplate",
                "fis:ListExperimentTemplates",
                "fis:ListExperiments",
                "fsx:DescribeFileSystems",
                "lambda:GetFunctionConcurrency",
                "lambda:GetFunctionConfiguration",
                "lambda:ListAliases",
                "lambda:ListEventSourceMappings",
                "lambda:ListFunctionEventInvokeConfigs",
                "lambda:ListVersionsByFunction",
                "rds:DescribeDBClusterSnapshots",
                "rds:DescribeDBClusters",
                "rds:DescribeDBInstanceAutomatedBackups",
                "rds:DescribeDBInstances",
                "rds:DescribeDBProxies",
                "rds:DescribeDBProxyTargets",
                "rds:DescribeDBSnapshots",
                "rds:DescribeGlobalClusters",
                "rds:ListTagsForResource",
                "resource-groups:GetGroup",
                "resource-groups:ListGroupResources",
                "route53-recovery-control-config:ListClusters",
                "route53-recovery-control-config:ListControlPanels",
                "route53-recovery-control-config:ListRoutingControls",
                "route53-recovery-readiness:GetReadinessCheckStatus",
                "route53-recovery-readiness:GetResourceSet",
                "route53-recovery-readiness:ListReadinessChecks",
                "route53:GetHealthCheck",
                "route53:ListHealthChecks",
                "route53:ListHostedZones",
                "route53:ListResourceRecordSets",
                "route53resolver:ListResolverEndpoints",
```

```
                "route53resolver:ListResolverEndpointIpAddresses",
                "s3:ListBucket",
                "servicecatalog:GetApplication",
                "servicecatalog:ListAssociatedResources",
                "sns:GetSubscriptionAttributes",
                "sns:GetTopicAttributes",
                "sns:ListSubscriptionsByTopic",
                "sqs:GetQueueAttributes",
                "sqs:GetQueueUrl",
                "ssm:DescribeAutomationExecutions",
                "states:DescribeStateMachine",
                "states:ListStateMachineVersions",
                "states:ListStateMachineAliases",
                "tag:GetResources"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AWSResilienceHubApiGatewayStatement",
            "Effect": "Allow",
            "Action": [
                "apigateway:GET"
            ],
            "Resource": [
                "arn:aws:apigateway:*::/apis/*",
                "arn:aws:apigateway:*::/restapis/*",
                "arn:aws:apigateway:*::/usageplans"
            ]
        },
        {
            "Sid": "AWSResilienceHubS3ArtifactStatement",
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:PutObject",
                "s3:GetObject"
            ],
            "Resource": "arn:aws:s3:::aws-resilience-hub-artifacts-*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
        },
```

```
        {
            "Sid": "AWSResilienceHubS3AccessStatement",
            "Effect": "Allow",
            "Action": [
                "s3:GetBucketLocation",
                "s3:GetBucketLogging",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketTagging",
                "s3:GetBucketVersioning",
                "s3:GetMultiRegionAccessPointRoutes",
                "s3:GetReplicationConfiguration",
                "s3:ListAllMyBuckets",
                "s3:ListMultiRegionAccessPoints"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
        },
        {
            "Sid": "AWSResilienceHubCloudWatchStatement",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": "ResilienceHub"
                }
            }
        },
        {
            "Sid": "AWSResilienceHubSSMStatement",
            "Effect": "Allow",
            "Action": [
                "ssm:GetParametersByPath"
            ],
            "Resource": "arn:aws:ssm:*:*:parameter/ResilienceHub/*"
        }
    ]
```

```
}
```

AWS Resilience HubAWS 管理ポリシーの更新

このサービスがこれらの変更の追跡を開始した AWS Resilience Hub 以降の の AWS マネージドポリシーの更新に関する詳細を表示します。このページの変更に関する自動アラートを受け取るには、AWS Resilience Hub ドキュメント履歴ページのRSSフィードにサブスクライブします。

変更	説明	日付
AWSResilienceHubAssessmentExecutionPolicy – 変更	AWS Resilience Hub はAWSResilienceHubAssessmentExecutionPolicy 、評価の実行 AWS Lambda 中に Amazon DocumentDB 、Elastic Load Balancing 、および のリソースと設定にアクセスできるようにするアクセスDescribe許可を付与するように更新されました。Elastic Load Balancing	2024 年 8 月 1 日
AWSResilienceHubAssessmentExecutionPolicy – 変更	AWS Resilience Hub はAWSResilienceHubAssessmentExecutionPolicy 、評価の実行中に Amazon FSx for Windows File Server の設定を読み取るためのDescribeアクセス許可を付与するように更新されました。	2024 年 3 月 26 日
AWSResilienceHubAssessmentExecutionPolicy – 変更	AWS Resilience Hub は AWSResilienceHubAssessmentExecutionPolicy を更新し、評価の	2023 年 10 月 30 日

変更	説明	日付
	実行中に設定を読み取るためのDescribeアクセス許可を付与しました AWS Step Functions 。	
AWSResilienceHubAssessmentExecutionPolicy – 変更	AWS Resilience Hub はAWSResilienceHubAssessmentExecutionPolicy 、評価の実行RDS中に Amazon のリソースにアクセスできるようにするアクセスDescribe許可を付与するように更新されました。	2023 年 10 月 5 日
AWSResilienceHubAssessmentExecutionPolicy – 新規	この AWS Resilience Hub ポリシーは、評価を実行するための他の AWS 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 が変更の追跡を開始しました	AWS Resilience Hub が AWS マネージドポリシーの変更の追跡を開始しました。	2023 年 6 月 15 日

AWS Resilience Hub ペルソナとIAMアクセス許可のリファレンス

AWSResilienceHubAsssessmentExecutionPolicy AWS 管理ポリシーと次のいずれかのペルソナ固有のポリシー AWS Resilience Hub を使用して、 の操作に必要なペルソナにアクセスIAM許可を付与できます。 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”。

によって提案されるペルソナのポリシー AWS Resilience Hub：

- IAM インフラストラクチャアプリケーションマネージャーペルソナの アクセス許可
- IAM ビジネス継続性マネージャーペルソナの アクセス許可
- IAM アプリケーション所有者ペルソナの アクセス許可
- IAM 読み取り専用アクセスを付与するための アクセス許可

IAM インフラストラクチャアプリケーションマネージャーペルソナの アクセス許可

次のポリシーは、インフラストラクチャアプリケーションマネージャーペルソナに必要なアクセス許可を付与します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "InfrastructureApplicationManager",
      "Effect": "Allow",
      "Action": [
        "resiliencehub:AddDraftAppVersionResourceMappings",
        "resiliencehub:CreateAppVersionAppComponent",
        "resiliencehub:CreateAppVersionResource",
        "resiliencehub:CreateRecommendationTemplate",
        "resiliencehub:DeleteAppAssessment",
        "resiliencehub:DeleteAppInputSource",
        "resiliencehub:DeleteAppVersionAppComponent",
        "resiliencehub:DeleteAppVersionResource",
        "resiliencehub:DeleteRecommendationTemplate",
        "resiliencehub:Describe*",
        "resiliencehub:List*",
        "resiliencehub:PublishAppVersion",
        "resiliencehub:PutDraftAppVersionTemplate",
        "resiliencehub:RemoveDraftAppVersionResourceMappings",
        "resiliencehub:ResolveAppVersionResources",
        "resiliencehub:StartAppAssessment",
        "resiliencehub:TagResource",
        "resiliencehub:UntagResource",
        "resiliencehub:UpdateAppVersion",
        "resiliencehub:UpdateAppVersionAppComponent",
        "resiliencehub:UpdateAppVersionResource"
      ],
      "Resource": "*"
    }
  ]
}
```

IAM ビジネス継続性マネージャーペルソナの アクセス許可

次のポリシーは、ビジネス継続性マネージャーペルソナに必要なアクセス許可を付与します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "BusinessContinuityManager",
      "Effect": "Allow",
      "Action": [
        "resiliencehub:CreateResiliencyPolicy",
        "resiliencehub:DeleteResiliencyPolicy",
        "resiliencehub:Describe*",
        "resiliencehub:List*",
        "resiliencehub:ResolveAppVersionResources",
        "resiliencehub:TagResource",
        "resiliencehub:UntagResource",
        "resiliencehub:UpdateAppVersion",
        "resiliencehub:UpdateAppVersionAppComponent",
        "resiliencehub:UpdateAppVersionResource",
        "resiliencehub:UpdateResiliencyPolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

IAM アプリケーション所有者ペルソナの アクセス許可

次のポリシーは、アプリケーション所有者ペルソナに必要なアクセス許可を付与します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ApplicationOwner",
      "Effect": "Allow",
      "Action": [
        "resiliencehub:AddDraftAppVersionResourceMappings",
        "resiliencehub:BatchUpdateRecommendationStatus",
        "resiliencehub:CreateApp",
        "resiliencehub:CreateAppVersionAppComponent",
        "resiliencehub:CreateAppVersionResource",
        "resiliencehub:CreateRecommendationTemplate",
        "resiliencehub:CreateResiliencyPolicy",
        "resiliencehub:DeleteApp",
```

```
        "resiliencehub:DeleteAppAssessment",
        "resiliencehub:DeleteAppInputSource",
        "resiliencehub:DeleteAppVersionAppComponent",
        "resiliencehub:DeleteAppVersionResource",
        "resiliencehub:DeleteRecommendationTemplate",
        "resiliencehub:DeleteResiliencyPolicy",
        "resiliencehub:Describe*",
        "resiliencehub:ImportResourcesToDraftAppVersion",
        "resiliencehub:List*",
        "resiliencehub:PublishAppVersion",
        "resiliencehub:PutDraftAppVersionTemplate",
        "resiliencehub:RemoveDraftAppVersionResourceMappings",
        "resiliencehub:ResolveAppVersionResources",
        "resiliencehub:StartAppAssessment",
        "resiliencehub:TagResource",
        "resiliencehub:UntagResource",
        "resiliencehub:UpdateApp",
        "resiliencehub:UpdateAppVersion",
        "resiliencehub:UpdateAppVersionAppComponent",
        "resiliencehub:UpdateAppVersionResource",
        "resiliencehub:UpdateResiliencyPolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

IAM 読み取り専用アクセスを付与するための アクセス許可

次のポリシーは、読み取り専用アクセスに必要なアクセス許可を付与します。

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

```
    }
  ]
}
```

Terraform 状態ファイルの へのインポート AWS Resilience Hub

AWS Resilience Hub は、Amazon Simple Storage Service マネージドキー (-SSE-S3SSE) または AWS Key Management Service マネージドキー (-) によるサーバー側の暗号化 () を使用して暗号化された Terraform 状態ファイルのインポートをサポートしますSSEKMS。Terraform 状態ファイルが、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、 を使用してインポートすることはできません AWS Resilience Hub。

Terraform 状態ファイルを にインポートするには、状態ファイルの場所に応じて以下のIAMポリシー AWS Resilience Hub 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 状態ファイルへの AWS Resilience Hub 読み取りアクセスを許可するには、次の Amazon S3 バケットIAMポリシーと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呼び出しロール、またはプライマリ AWS アカウントの AWS 現在のIAMロールに関連付けられた ID AWS Resilience Hub 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",
      "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 状態ファイルが を使用して暗号化されている場合はKMS、次の`kms:Decrypt`アクセス許可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 – プライマリアカウント AWS Resilience Hub で実行されている AWS アカウントロールに関連付けられた AWS ID 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>"
    }
  ]
}
```

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 状態ファイルが を使用して暗号化されている場合はKMS、次のkms:Decryptアクセス許可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 クラスター AWS Resilience Hub へのアクセスの有効化

AWS Resilience Hub は、Amazon クラスターのインフラストラクチャを分析して Amazon Elastic Kubernetes Service (Amazon EKS) EKSクラスターの耐障害性を評価します。 は、Kubernetes ロールベースのアクセスコントロール (RBAC) 設定 AWS Resilience Hub を使用して、Amazon EKS クラスターの一部としてデプロイされる他の Kubernetes (K8) ワークロードを評価します。 AWS Resilience Hub がワークロードの分析と評価のために Amazon EKSクラスターにクエリを実行するには、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。
- 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許可を付与します。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 AWS IAM コントロールプレーンで実行される Authenticator for Kubernetes によって有効になります。 EKS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。

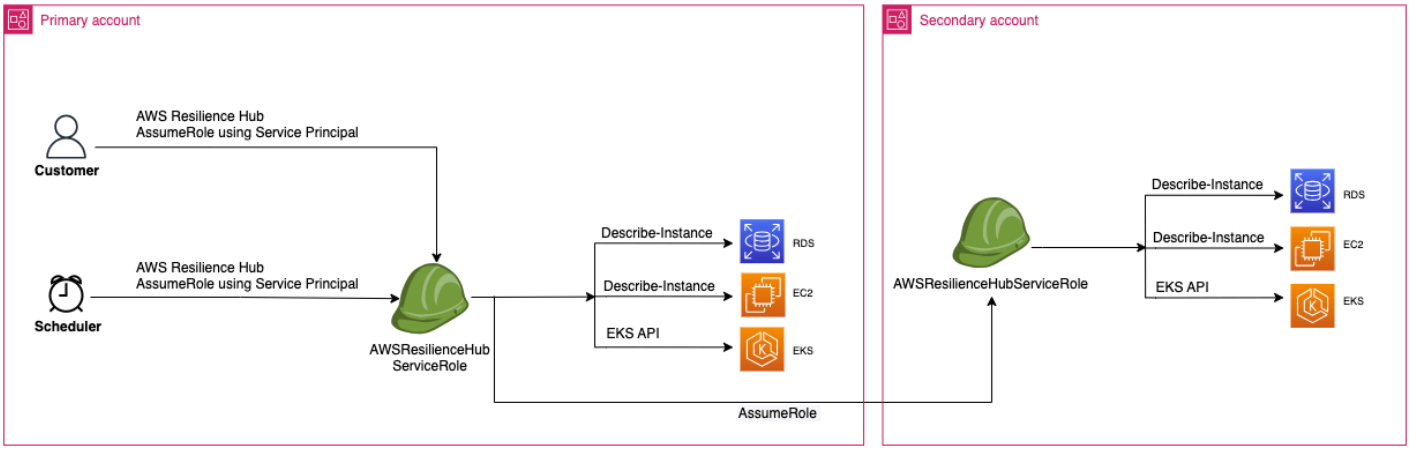
> **Note**
>
> - すべての`aws-auth ConfigMap`設定の詳細については、「」の「フル設定形式」を参照してください GitHub。
> - さまざまな ID の詳細については、IAM「 ユーザーガイド」の「ID (ユーザー、グループ、ロール)」を参照してください。 IAM
> - Kubernetes ロールベースのアクセスコントロール (RBAC) 設定の詳細については、RBAC「認可の使用」を参照してください。

AWS Resilience Hub は、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。 AWS Resilience Hub が Amazon EKS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に対する十分な読み取り専用アクセス許可を持つ Kubernetes グループにマッピング AWS Resilience Hub する必要があります。

AWS Resilience Hub は、次のいずれかのIAMロールオプションを使用して、Amazon EKSクラスターリソースへのアクセスを許可します。

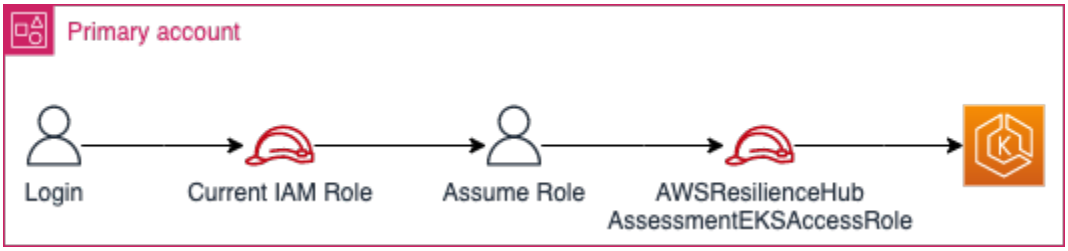
- アプリケーションが リソースへのアクセスにロールベースのアクセスを使用するように設定されている場合、アプリケーションの作成時に に渡 AWS Resilience Hub された呼び出しロールまたはセカンダリアカウントロールは、評価中に Amazon EKSクラスターへのアクセスに使用されます。

  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が Amazon EKSクラスター AWS Resilience Hub にアクセスする方法を示しています。

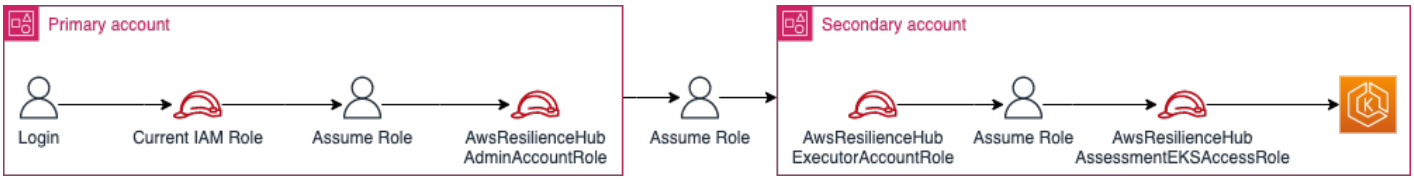


- アプリケーションがリソースへのアクセスに現在のIAMユーザーを使用するように設定されている場合は、Amazon EKSクラスターと同じアカウントに`AwsResilienceHubAssessmentEKSAccessRole`で という名前の新しいIAMロールを作成する必要があります。その後、このIAMロールは Amazon EKSクラスターへのアクセスに使用されます。

  次の概念図は、アプリケーションが現在のIAMユーザーアクセス許可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 EKSクラスターに が AWS Resilience Hub 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ユーザーアクセス許可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 EKSクラスターに が AWS Resilience Hub アクセスする方法を示しています。



Amazon EKSクラスター内のリソース AWS Resilience Hub へのアクセスの許可

AWS Resilience Hub では、必要なアクセス許可を設定している限り、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を検出および評価 AWS Resilience Hub するために必要なアクセス許可を に付与するには

1. Amazon EKSクラスターにアクセスするように 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。がロール AWS Resilience Hub を使用する方法の詳細については、IAM「」を参照してくださいthe section called “AWS Resilience Hub と の連携方法 IAM”。

   現在のIAMユーザーアクセス許可を使用してアプリケーションを設定した場合は、Amazon EKSクラスターのロールと同じアカウントに`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ときに使用されます。

   アプリケーションのインポートと評価中に、 IAMロール AWS Resilience Hub 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、Amazon EKSクラスターの評価に必要なアクセス許可を含む Kubernetes グループ AWS Resilience Hub でマッピングされます。

Amazon EKSクラスターが AWS Resilience Hub 呼び出し元のアカウントと同じアカウントにある場合は、次のIAM信頼ポリシーを使用してロールを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`は現在のアカウントで APIsの を呼び出すために使用されます AWS Resilience Hub。

> **Note**
>
> `caller_IAM_role` は、 AWS 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 呼び出し元のアカウントとは異なるアカウント) にある場合は、次のIAM信頼ポリシーを使用してAwsResilienceHubAssessmentEKSAccessRoleIAM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異なる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. AWS Resilience Hub アプリケーションの ClusterRoleおよび ClusterRoleBinding (または RoleBinding) ロールを作成します。

   ClusterRole と を作成するとClusterRoleBinding、Amazon EKSクラスター内の特定の名前空間の一部であるリソースを分析および評価 AWS Resilience Hub するために必要な読み取り専用アクセス許可が に付与されます。

   AWS Resilience Hub では、次のいずれかを完了することで、障害耐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。

      が Amazon EKSクラスター内のすべての名前空間のリソースの耐障害性を評価する AWS Resilience Hub には、次の ClusterRoleと を作成する必要がありますClusterRoleBinding。

      - resilience-hub-eks-access-cluster-role (ClusterRole) — Amazon EKSクラスターを評価する AWS Resilience Hub ために が必要とするアクセス許可を定義します。
      - resilience-hub-eks-access-cluster-role-binding (ClusterRoleBinding) — Amazon EKSクラスターresilience-hub-eks-access-groupで という名前のグループを定義し、そのユーザーに、 で障害耐性評価を実行するために必要なアクセス許可を付与します AWS Resilience Hub。

      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
    - nodepools
  verbs:
    - get
    - list
- apiGroups:
    - karpenter.k8s.aws
  resources:
    - awsnodetemplates
    - ec2nodeclasses
  verbs:
    - get
    - list
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: resilience-hub-eks-access-cluster-role-binding
subjects:
  - kind: Group
    name: resilience-hub-eks-access-group
    apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
  name: resilience-hub-eks-access-cluster-role
  apiGroup: rbac.authorization.k8s.io
---
EOF
```

b. 特定の名前空間 AWS Resilience Hub を読み取るためのアクセス許可を付与します。

を使用して、特定の名前空間セット内のリソースへのアクセス AWS Resilience Hub 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 – が 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、その障害耐性を評価する AWS Resilience Hub には、次のClusterRoleロールを作成する必要があります。
  - 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 clusters 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許可を指定します。 AWS Resilience Hub は、Amazon EKSクラスターのクラスタースコープのリソース (ノードなど) にアクセスしてアプリケーションの耐障害性を評価するためのアクセス許可を必要とします。

`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
      - nodepools
    verbs:
      - get
      - list
  - apiGroups:
      - karpenter.k8s.aws
    resources:
      - awsnodetemplates
      - ec2nodeclasses
    verbs:
      - get
      - list

---
EOF
```

- RoleBinding role – このロールは、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許可 AWS Resilience Hub を に付与します。つまり、 が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には AWS Resilience Hub 、各名前空間にRoleBindingロールを作成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クラスターの評価中にkube-system名前空間内のリソースを評価する AWS Resilience Hub ために必要なアクセス許可を付与します。

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 role – このロールは、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許可 AWS Resilience Hub を に付与します。

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. を更新aws-auth ConfigMapして、 を Amazon EKSクラスターへのアクセスに使用されるIAMロールresilience-hub-eks-access-groupにマッピングします。

   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 グループ間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許可を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 AWS Resilience Hub 時に渡される呼び出し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。
   >   - 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設定されている場合は、 である必要がありますAwsResilienceHubAssessmentEKSAccessRole。

- ACCOUNT-ID は Amazon EKSクラスターの AWS 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 の使用

  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
```

- 手動で を編集するには、 ConfigMapのアンダーデータの mapRolesセクションにIAMロールの詳細aws-authConfigMapを追加します。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 – 追加する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ロールにマッピングされる Kubernetes 内のユーザー名 (AwsResilienceHubAssessmentEKSAccessRole) 。
  - 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。

次のテンプレートを使用して、ConfigMapアンダーデータの mapRolesセクションにIAM ロールの詳細を追加します。

```
    - groups:
      - resilience-hub-eks-access-group
      rolearn: arn:aws:iam::<ACCOUNT-ID>:role/<ROLE-NAME>
      username: AwsResilienceHubAssessmentEKSAccessRole
```

AWS Resilience Hub を有効にして Amazon Simple Notification Service トピックに発行する

このセクションでは、 AWS Resilience Hub が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、以下があることを確認します。

- アクティブな AWS Resilience Hub アプリケーション。
- が通知を送信 AWS Resilience Hub 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 トピックの作成SNS」を参照してください。

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 を使用してオプトインリージョンから、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メッセージを発行する場合は、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。

Server Side Encrypted (SSE) Amazon SNSトピックを使用している場合は、 に Amazon SNS暗号化キーへの `Decrypt`および `GenerateDataKey*` アクセス AWS Resilience Hub があることを確認する必要があります。

`Decrypt` と `GenerateDataKey*`へのアクセスを提供するには AWS Resilience Hub、 アクセスポリシーに次の AWS Key Management Service アクセス許可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 レコメンデーションを含めるまたは除外するためのアクセス許可の制限

AWS Resilience Hub では、アプリケーションごとにレコメンデーションを含めるか除外するアクセス許可を制限できます。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レコメンデーションを含めるか除外するかのアクセス許可を制限できます。このIAM信頼ポリシーでは、

`caller_IAM_role` (AWS ユーザーアカウントに関連付けられている) が現在のアカウントで使用され、 APIs の 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セキュリティ AWS Resilience Hub

マネージドサービスである AWS Resilience Hub は、ホワイトペーパー「Amazon Web Services: セキュリティプロセスの概要」に記載されている AWS グローバルネットワークセキュリティの手順で保護されています。

が AWS 公開したAPI呼び出しを使用して、ネットワーク AWS Resilience Hub 経由で にアクセスします。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。1.3 TLS 以降をお勧めします。クライアントは、エフェメラル Diffie-Hellman (PFS) や楕円曲線エフェメラル Diffie-Hellman () などの完全前方秘匿性 (DHE) を持つ暗号スイートもサポートする必要がありますECDHE。これらのモードは、Java 7 以降など、ほとんどの最新システムでサポートされています。

さらに、リクエストは、 IAMプリンシパルに関連付けられたアクセスキー ID と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 Service (AWS STS) を使用して、一時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。

AWS サービスの耐障害性チェック

この章では、アプリケーションの耐障害性体制に影響が及ばないように、サポートされている AWS のサービス AWS Resilience Hub に対して によって実行されるさまざまな耐障害性チェックの詳細について説明します。これらのチェックでは、目標復旧時間 (RTO) と目標復旧時点 () を、各アプリケーションコンポーネント (RPO) の耐障害性ポリシーで定義されている値と照らし合わせて推定しますAppComponent。評価には、アプリケーション、インフラストラクチャの障害、AZ の停止、リージョンの障害など、さまざまなタイプの中断が含まれます。ただし、これらのチェックを実行するには、 リソースへのアクセスを許可 AWS Resilience Hub するために、 に関連するアクセスIAM許可を付与する必要があります。この章で が リソースにアクセスし、レジリエンスチェックを実行するために必要なアクセスIAM許可 AWS Resilience Hub の詳細については、「」を参照してくださいAWS の マネージドポリシー AWS Resilience Hub。

AWS サービス

- Amazon Elastic File System
- Amazon Relational Database Service と Amazon Aurora
- Amazon Simple Storage Service
- Amazon DynamoDB
- Amazon Elastic Compute Cloud
- Amazon EBS
- AWS Lambda
- Amazon Elastic Kubernetes Service
- Amazon Simple Notification Service
- Amazon Simple Queue Service
- Amazon Elastic Container Service
- Elastic Load Balancing
- Amazon API Gateway
- Amazon DocumentDB
- NAT ゲートウェイ
- Amazon Route 53
- Amazon Route 53 Application Recovery Controller

- Amazon FSx for Windows File Server
- AWS Step Functions

Amazon Elastic File System

このセクションでは、Amazon Elastic File System に固有のすべてのレジリエンスチェックと推奨事項を一覧表示します。

Amazon Elastic File System の詳細については、Amazon Elastic File Systemドキュメント」を参照してください。

ファイルシステムタイプ

AWS Resilience Hub は、ファイルシステムタイプがリージョンまたは 1 ゾーンであることを確認します。ファイルシステムタイプは、インフラストラクチャまたは AZ の中断が発生した場合の耐障害性に影響します。ファイルシステムタイプの詳細については、「Amazon EFS ファイルシステムの可用性と耐久性」を参照してください。

ファイルシステムのバックアップ

AWS Resilience Hub は、デプロイされたファイルシステムに AWS Backup 計画が定義されているかどうかを確認します。さらに、Cross-Regionバックアップオプションが有効になっているかどうかを検証し、顧客ポリシーで必要な場合にリージョンレベルの中断を確実にカバーします。

データレプリケーション

AWS Resilience Hub は、デプロイされたファイルシステムにリージョン内またはクロスリージョンの Amazon EFS データレプリケーションが定義されているかどうかを確認します。Amazon EFS データレプリケーションは、RPOアプリケーションRTO、インフラストラクチャ、AZ、リージョンレベルでの推定と推定を改善するのに役立ちます。さらに、アプリケーションが中断した場合にファイルシステムの回復性を有効にする AWS Backup ために、 がリージョン内の と組み合わ AWS Resilience Hub されているかどうかを確認します。

Amazon Relational Database Service と Amazon Aurora

このセクションでは、Amazon Relational Database Service と Amazon Aurora に固有のすべてのレジリエンスチェックとレコメンデーションを一覧表示します。

Amazon Relational Database Service と Amazon Aurora の詳細については、「Amazon Amazon Relational Database Serviceのドキュメント」を参照してください。

シングル AZ デプロイ

AWS Resilience Hub は、データベースが 1 つのインスタンスとしてデプロイされているかどうかを確認し、決定された場合は、セカンダリインスタンスとリードレプリカをサポートしていないことを示します。

マルチ AZ デプロイ

AWS Resilience Hub は、データベースがセカンダリインスタンスまたはリードレプリカでデプロイされているかどうかを確認します。データベースがリードレプリカでデプロイされている場合、 は別の AZ にデプロイされているかどうか AWS Resilience Hub を検証し、AZ が中断した場合にフェイルオーバーを許可します。

バックアップ

AWS Resilience Hub は、デプロイされたデータベースインスタンスに次のバックアップ機能が適用されているかどうかを確認します。

- AWS Backup 自動バックアップオプションを使用した プラン
- AWS Backup カスタマーポリシーで必要な場合は、クロスリージョンバックアップコピーを使用して計画する
- サードパーティーのバックアップシステムの手動スナップショット

クロスリージョンフェイルオーバー

AWS Resilience Hub は、リージョンの中断から回復するために、障害耐性ポリシーで定義されている RTOとRPOターゲットをチェックします。さらに、 は、リージョンの中断に対応するために、次のクロスリージョンアーキテクチャを特定 AWS Resilience Hub できます。

- クロスリージョンスナップショットのコピーを含むリージョン内バックアップ
- 別のリージョンのリードレプリカ
- 別のリージョンにセカンダリクラスターを持つ Amazon Aurora グローバルデータベース
- 別のリージョンにヘッドレスセカンダリクラスターを持つ Amazon Aurora グローバルデータベース

リージョン内フェイルオーバーの高速化

AWS Resilience Hub はRTO、インフラストラクチャまたは AZ の中断中に障害耐性ポリシーで定義された とRPOターゲットをチェックします。さらに、 は、アプリケーション、インフラストラクチャ、AZ の中断をカバーする以下のリージョン内アーキテクチャを特定 AWS Resilience Hub できます。

- リージョン内バックアップ
- 別の AZ のリードレプリカ
- 別の AZ にリードレプリカがある Aurora クラスター
- Amazon Relational Database Service (Amazon RDS) のマルチ AZ インスタンス
- Amazon RDS マルチ AZ クラスター
- 別の AZ のリードレプリカRDSを持つ Amazon の単一のインスタンス

Amazon Simple Storage Service

このセクションでは、Amazon Simple Storage Service (Amazon S3) に固有のすべてのレジリエンスチェックと推奨事項を一覧表示します。

Amazon S3 の詳細については、Amazon S3ドキュメント」を参照してください。

バージョニング

AWS Resilience Hub は、Amazon S3 バケットでバージョニングが有効になっているかどうかを確認します。

スケジュールされたバックアップ

AWS Resilience Hub は、デプロイされた Amazon Simple Storage Service (Amazon S3) バケットに対して AWS Backup プランが定義されているかどうかを確認します。さらに、ポリシーでリージョンレベルの中断に対するカバレッジが必要かどうかも、クロスリージョンバックアップオプションが有効になっているかどうかを確認します。

P oint-in-time リカバリ

データレプリケーション

AWS Resilience Hub デプロイされた Amazon S3 バケットに同じリージョンレプリケーション (SRR) とクロスリージョンレプリケーション (CRR) が定義されている場合。 Amazon S3

Amazon S3 データレプリケーションはRTO、アプリケーション、インフラストラクチャ、AZ、リージョンレベルで推定ワークロードと推定ワークロードを改善RPOします。さらに、オブジェクトバージョンの削除はターゲット Amazon S3 バケットにレプリケートされないため、オブジェクトの物理的な削除からも保護されます。さらに、障害耐性ポリシーで定義されているRTOターゲットに基づいて、Amazon S3 レプリケーションタイムコントロール (S3 RTC) を有効にするかどうか AWS Resilience Hub をチェックします。この請求可能な機能は、15 分以内にレプリケート元バケットオブジェクトの 99.99% をレプリケートします。

- AWS Backup 自動バックアップオプションを使用した プラン
- AWS Backup カスタマーポリシーで必要な場合は、クロスリージョンバックアップコピーを使用して計画する
- サードパーティーのバックアップシステムの手動スナップショット

Amazon DynamoDB

このセクションでは、Amazon DynamoDB に固有のすべてのレジリエンスチェックと推奨事項を一覧表示します。

Amazon DynamoDB の詳細については、「Amazon DynamoDB ドキュメント」を参照してください。

スケジュールされたバックアップ

AWS Resilience Hub は、デプロイされたテーブルにバックアップが既に定義されているかどうかを確認します。さらに、リージョンレベルの中断をカバーする必要がある場合に、ポリシーにクロスリージョンバックアップを設定する必要があるかどうかも確認します。

P oint-in-time リカバリ

AWS Resilience Hub は、障害耐性ポリシーのRPOターゲットに従って point-in-time 復旧 (PITR) が必要かどうかを確認します。ただし、クロスリージョンバックアップは ではサポートされていませ

んPITR。したがって、クロスリージョンバックアップオプションを有効にした既存のスケジュールされた AWS Backup 計画を使用するか、新しい計画を作成します。

グローバルテーブル

Amazon Elastic Compute Cloud

このセクションでは、Amazon Elastic Compute Cloud に固有のすべてのレジリエンスチェックと推奨事項を一覧表示します。

Amazon Elastic Compute Cloud の詳細については、「Amazon Elastic Compute Cloud のドキュメント」を参照してください。

ステートフルインスタンス

AWS Resilience Hub は、次のいずれかの基準が満たされた場合、Amazon EC2インスタンスをステートフルインスタンスとして識別します。

- このインスタンスにアタッチされている少なくとも 1 つの Amazon Elastic Block Store (Amazon EBS) ボリュームの `DeleteOnTermination` 属性が false に設定されている場合。
- Amazon Data Lifecycle Manager または AWS Backup プランが Amazon EC2インスタンスまたは少なくとも 1 つの Amazon EBSボリュームにアタッチされている場合。
- AWS Elastic Disaster Recovery を使用して Amazon EC2インスタンスストレージボリュームをレプリケートする場合。

> **Note**
>
> Amazon EC2インスタンスが上記のいずれの基準も満たしていない場合、 はそれをステートレス Amazon EC2インスタンスとして AWS Resilience Hub 扱います。

「Auto Scaling グループ」

AWS Resilience Hub はステートレス Amazon EC2インスタンスのグループをチェックします。検出された場合は、マルチ AZ 設定で Auto Scaling グループ (ASG) を使用して同じ をオーケストレーションすることをお勧めします。

既存の が特定されると、 ASGは複数のアベイラビリティーゾーンにまたがって設定されているARH かどうかを確認します。スポット Amazon EC2インスタンスのみを使用して ASGも定義されている場合は、障害耐性を向上させるために、オンデマンド Amazon EC2インスタンスで容量を拡張することをお勧めします。

スポット Amazon EC2インスタンスが使用できない場合。

Amazon EC2 フリート

AWS Resilience Hub は Amazon EC2 フリートを識別し、マルチ AZ 配置として定義されているかどうか、およびスポット Amazon EC2インスタンスのみを使用しているかどうかを確認します。

Amazon EC2 フリートをマルチ AZ 配置として定義すると、AZ が中断した場合の耐障害性が向上します。

オンデマンドインスタンスで Amazon EC2 フリート を拡張すると、スポットインスタンスが使用できない場合の耐障害性が向上します。

Amazon EBS

このセクションでは、Amazon に固有のすべてのレジリエンスチェックとレコメンデーションを一覧表示しますEBS。

Amazon の詳細についてはEBS、「Amazon EBSドキュメント」を参照してください。

スケジュールされたバックアップ

AWS Resilience Hub は、Amazon EBSボリュームに対して次のいずれかまたは両方が定義されているかどうかを確認します。

- Amazon EC2インスタンスにアタッチされた特定の Amazon EBSボリュームのバックアップルール。
- Amazon AMIEC2インスタンスに Amazon EBS-backed を作成するバックアップルール。
- サードパーティーのバックアップシステムの手動スナップショット。

さらに、ポリシーでリージョンレベルの中断に対応する必要がある場合、 はバックアップルールでクロスリージョンバックアップオプションが有効になっている AWS Resilience Hub かどうかを確認します。

データのバックアップとレプリケーション

AWS Resilience Hub は、次のいずれかの基準が満たされた場合に、Amazon EBSボリュームがステートフルボリュームと見なされることを識別します。

- この Amazon EBSボリュームの `DeleteOnTermination` 属性が false に設定されている場合。
- Amazon Data Lifecycle Manager または AWS Backup プランがこの Amazon EBSボリュームまたはアタッチされている Amazon EC2インスタンスに関連付けられている場合。
- AWS Elastic Disaster Recovery を使用して Amazon EC2インスタンスストレージボリュームをレプリケートする場合。

AWS Lambda

このセクションでは、 に固有のすべてのレジリエンスチェックとレコメンデーションを一覧表示します AWS Lambda。

の詳細については AWS Lambda、「 AWS Lambda ドキュメント」を参照してください。

カスタマー Amazon VPC アクセス

AWS Resilience Hub は、顧客 に接続された AWS Lambda 関数を識別しますVPC。異なる Amazon AZsのサブネット AWS Lambda に接続するとVPC、AZ が中断した場合に関数の回復性が得られます。

デッドレターキュー

AWS Resilience Hub は、失敗したリクエストを保存するために、 AWS Lambda 関数にデッドレターキュー (DLQ) がアタッチされているかどうかを確認します。 AWS Lambda 関数DLQに をアタッチすると、 はリクエストのデータ損失を防ぎ、失敗したリクエストを後の段階で処理しようとできます。

Amazon Elastic Kubernetes Service

このセクションでは、Amazon Elastic Kubernetes Service (Amazon) に固有のすべてのレジリエンスチェックと推奨事項を一覧表示しますEKS。

Amazon の詳細についてはEKS、「Amazon EKSドキュメント」を参照してください。

マルチ AZ デプロイ

AWS Resilience Hub は、ポッドデプロイが複数の の複数のワーカーノードで実行されているかどうかを識別しますAZs。

リージョンで障害が発生した場合に障害耐性ポリシーでカバレッジが必要な場合は、別のリージョンに追加の Amazon EKSクラスターが必要です。この追加の Amazon EKSクラスターは、複数の の複数のワーカーノード間に分散されるポッドデプロイについても検証されますAZs。

デプロイと ReplicaSet

AWS Resilience Hub は、デプロイメントの代わりに ReplicaSets または ポッドオブジェクトを使用しているかどうかを確認します。 ReplicaSets または ポッドオブジェクトをデプロイに置き換えると、ポッドの更新がソフトウェアの新しいバージョンに簡素化され、その他の便利な機能が含まれています。

デプロイのメンテナンス

AWS Resilience Hub は、デプロイに次のベストプラクティスが使用されているかどうかを確認します。

- Pod Disruption Budget (PDB) の使用 – PDBを使用すると、いつでも中断される可能性のあるワークロード内のポッド数に制限を設定することで、可用性を向上させることができます。
- セルフマネージド型ノードグループを Amazon EKSマネージド型ノードグループに置き換える – この置き換えにより、メンテナンス中のワーカーノードイメージの更新が簡単になります。
- デプロイごとの動的リクエストCPUとメモリリクエストのサポート — これらのリクエストは、Kubernetes がポッドのニーズに合わせてノードを選択するのに役立ちます。
- すべてのコンテナのライブネスプローブと準備状況プローブの設定 – ライブネスプローブを設定すると、機能していないポッドを再起動することで回復性が向上します。準備状況プローブを設定すると、トラフィックをビジーポッドから遠ざけることで可用性を向上させることができます。
- Karpenter、Cluster Autoscaler、または の設定 AWS Fargate – これらの設定により、Amazon EKSクラスターのインフラストラクチャが拡張され、ワークロードの需要を満たすことができます。
- 水平ポッドオートスケーラーの設定 — この設定は、Amazon EKSクラスターがリクエスト処理の需要に合わせてワークロードを自動的にスケーリングするのに役立ちます。

Amazon Simple Notification Service

このセクションでは、Amazon Simple Notification Service (Amazon) に固有のすべてのレジリエンスチェックと推奨事項を一覧表示しますSNS。

Amazon の詳細についてはSNS、「Amazon SNSドキュメント」を参照してください。

トピックサブスクリプション

AWS Resilience Hub は、受信メッセージが失われないように、Amazon SNSトピックに少なくとも 1 つのサブスクリプションがアタッチされているかどうかを確認します。

Amazon Simple Queue Service

このセクションでは、Amazon Simple Queue Service (Amazon) に固有のすべてのレジリエンスチェックとレコメンデーションを一覧表示しますSQS。

Amazon の詳細についてはSQS、「Amazon SQSドキュメント」を参照してください。

デッドレターキュー

AWS Resilience Hub は、受信者に正常に配信できないメッセージを処理するために、Amazon SQS キューに がDLQ関連付けられているかどうかを確認します。

Amazon Elastic Container Service

このセクションでは、Amazon Elastic Container Service (Amazon) に固有のすべてのレジリエンスチェックとレコメンデーションを一覧表示しますECS。

Amazon の詳細についてはECS、「Amazon ECSドキュメント」を参照してください。

マルチ AZ デプロイ

AWS Resilience Hub は、Amazon ECS タスクまたはサービスが Amazon EC2または AWS Fargate 起動タイプAZsに基づいて複数の で実行されているかどうかを確認します。ポリシーでリージョンの中断に対するカバレッジが必要な場合は、別のリージョンに追加の Amazon ECSクラスターが必要です。追加のクラスターは、複数の でタスクまたはサービスの実行についても検証されますAZs。

Elastic Load Balancing

このセクションでは、Elastic Load Balancing に固有のすべてのレジリエンスチェックとレコメンデーションを一覧表示します。

Elastic Load Balancing の詳細については、Elastic Load Balancing」を参照してください。

マルチ AZ デプロイ

AWS Resilience Hub は、Elastic Load Balancing が複数の で実行されているかどうかを確認しますAZs。

ポリシーでリージョンの中断に対応する必要がある場合は、別のリージョンに追加の Elastic Load Balancing が必要です。別のリージョンにある追加の Elastic Load Balancing も、複数の にデプロイされるかどうかが確認されますAZs。

Amazon API Gateway

このセクションでは、Amazon API Gateway に固有のすべてのレジリエンスチェックとレコメンデーションを一覧表示します。

Amazon API Gateway の詳細については、「Amazon API Gateway のドキュメント」を参照してください。

クロスリージョンデプロイ

ポリシーでリージョンの中断を検討する必要がある場合、 は別のリージョンに Amazon API Gateway APIリソースを追加デプロイしているかどうか AWS Resilience Hub をチェックします。

プライベートAPIマルチ AZ 配置

AWS Resilience Hub は、 APIが Amazon API Gateway 内でプライベートとして定義されているかどうかを確認します。プライベートは、複数の にデプロイされた Amazon VPCインターフェイスエンドポイントを介してトラフィックを受信APIsする必要がありますAZs。

Amazon DocumentDB

このセクションでは、Amazon DocumentDB に固有のすべてのチェックと推奨事項を一覧表示します。

Amazon DocumentDB の詳細については、Amazon DocumentDBドキュメント」を参照してください。

マルチ AZ デプロイ

AWS Resilience Hub はAmazon DocumentDB クラスターが複数の にデプロイされているかどうかを確認しますAZs。ポリシーでリージョンの中断に対するカバレッジが必要な場合は、別のリージョンに追加のセカンダリ Amazon DocumentDB クラスターが必要です。別のリージョンにある追加の Amazon DocumentDB クラスターも、複数の で実行されていることが確認されますAZs。

Elastic クラスターとマルチ AZ 配置

AWS Resilience Hub は、Amazon DocumentDB Elastic クラスターシャードが異なる にデプロイされたリードレプリカを使用しているかどうかを確認しますAZs。

Elastic クラスターと手動スナップショット

AWS Resilience Hub は、Amazon DocumentDB Elastic クラスターに対して手動スナップショットが定期的に作成されているかどうかを確認します。手動スナップショットを使用すると、永続性が長くなり、ビジネスニーズに合わせてスナップショットの頻度を柔軟に設定できます。

NAT ゲートウェイ

このセクションでは、NATゲートウェイに固有のすべてのチェックと推奨事項を一覧表示します。NAT ゲートウェイの詳細については、NAT「ゲートウェイ」を参照してください。

マルチ AZ デプロイ

AWS Resilience Hub は、NATゲートウェイが複数の にデプロイされているかどうかを確認しますAZs。

ポリシーでリージョンの中断に対応する必要がある場合は、別のリージョンに追加のNATゲートウェイデプロイが必要です。別の リージョンにある追加のNATゲートウェイも、複数の にデプロイされていることが確認されますAZs。

Amazon Route 53

このセクションでは、Amazon Route 53 に固有のすべてのチェックと推奨事項を一覧表示します。

Amazon Route 53 の詳細については、「Amazon Route 53 ドキュメント」を参照してください。

マルチ AZ デプロイ

AWS Resilience Hub は、Amazon Route 53 ホストゾーンレコードが同じリージョン内の複数のターゲットで定義されているかどうか、およびこれらのターゲットが複数の にデプロイされているかどうかを確認しますAZs。ポリシーでリージョンの中断に対するカバレッジが必要な場合、 AWS Resilience Hub は、Amazon Route 53 ホストゾーンレコードがリージョンごとに複数のターゲットを持つ複数のリージョンで定義されているかどうか、およびこれらのターゲットが複数の にデプロイされているかどうかを確認しますAZs。

Amazon Route 53 Application Recovery Controller

このセクションでは、Amazon Route 53 Application Recovery Controller (Route 53) に固有のすべてのチェックと推奨事項を一覧表示しますARC。

Route 53 の詳細についてはARC、Route 53ARCドキュメント」を参照してください。

マルチ AZ デプロイ

AWS Resilience Hub は、同様のリソースが複数のリージョンにデプロイされているかどうかをチェックし、リージョンの中断が発生した場合に可用性と準備状況を向上させるために Route 53 ARCの準備状況チェックを定義するベストプラクティスとして を推奨します。時間単位の追加料金が発生することが通知されます。

Amazon FSx for Windows File Server

このセクションでは、Amazon FSx for Windows File Server に固有のすべてのチェックと推奨事項を一覧表示します。Amazon FSx for Windows File Server の詳細については、「Amazon FSx for Windows File Server のドキュメント」を参照してください。

ファイルシステムタイプ

AWS Resilience Hub はファイルシステムタイプ `Regional`または をチェックします`One Zone`。ファイルシステムのタイプは、インフラストラクチャまたは AZ の中断が発生した場合の回復性に影響します。ファイルシステムタイプの詳細については、「Amazon EFS」を参照してください。

ファイルシステムのバックアップ

AWS Resilience Hub AWS Backup は、デプロイされたファイルシステムに が定義されているかどうかを確認します。さらに、ポリシーでリージョンレベルの中断に対するカバレッジが必要な場合に、`cross-Region backup`オプションが有効になっているかどうかも確認します。

データレプリケーション

AWS Resilience Hub は、デプロイされたファイルシステムにリージョン内またはリージョン間のスケジュールされた AWS DataSync データレプリケーションタスクが定義されているかどうかを確認します。

AWS DataSync スケジュールされたデータレプリケーションタスクは、RPOインフラストラクチャRTO、AZ、およびリージョンレベルで推定ワークロードと推定ワークロードを改善できます。さらに、リージョン内の と組み合わせて AWS Backup 、アプリケーションの中断時に復旧することもできます。

AWS Step Functions

このセクションでは、 に固有のすべてのチェックと推奨事項を一覧表示します AWS Step Functions。

の詳細については AWS Step Functions、「 AWS Step Functions ドキュメント」を参照してください。

バージョニングとエイリアス

AWS Resilience Hub AWS Step Functions ワークフローがバージョニングとエイリアスを使用して再デプロイ時間を短縮しているかどうかをチェックします。

クロスリージョンデプロイ

AWS Resilience Hub は、同じ AWS Step Functions ワークフロータイプのワークフローが別のリージョンにデプロイされているかどうかをチェックし、リージョンの中断が発生した場合に復旧します。

他の サービスでの使用

このセクションでは、 とやり取り AWS 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 は、ユーザー AWS CloudTrail、ロール、または のサービスによって実行されたアクションを記録する AWS サービスである と統合されています AWS Resilience Hub。 は、 のすべての API コールをイベント AWS Resilience Hub として CloudTrail 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。証跡を作成する場合は、 の CloudTrail イベントなど、Amazon S3 バケットへのイベントの継続的な配信を有効にすることができます AWS Resilience Hub。証跡を設定しない場合でも、 CloudTrail コンソールのイベント履歴で最新のイベントを表示できます。によって収集された情報を使用して CloudTrail、 に対するリクエスト AWS Resilience Hub、リクエスト元の IP アドレス、リクエスト者、リクエスト日時などの詳細を確認できます。

の詳細については 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、SOPs 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、SOPs。

AWS Resilience Hub には、異なる Systems Manager ドキュメントを実行するために必要な IAM ロールを含む AWS CloudFormation テンプレートが用意されています。各ドキュメントには 1 つのロールと、特定のドキュメントに必要なアクセス許可があります。 AWS CloudFormation テンプレートを使用してスタックを作成すると、IAM ロールがセットアップされ、Systems Manager オー

トメーションドキュメントのメタデータが Systems Manager パラメータに保存され、さまざまな復旧手順で実行されます。

SOP の使い方については、標準運用手順の管理を参照してください。

AWS Trusted Advisor

AWS Trusted Advisor は、 でのデプロイを特定、優先順位付け、最適化するのに役立つ AWS ベストプラクティスのレコメンデーションの一元的な拠点です AWS。 は AWS 、環境 AWS Trusted Advisor を検査し、コストを節約したり、システムの可用性とパフォーマンスを向上させたり、セキュリティギャップを埋めたりする機会が存在する場合にチェックを通じてレコメンデーションを作成します。これらのチェックは、目的に基づいて複数のカテゴリに分けられます。でのさまざまなチェックカテゴリの詳細については AWS Trusted Advisor、「 AWS Supportユーザーガイド」を参照してください。

AWS Trusted Advisor は、障害耐性カテゴリ AWS Resilience Hub の にある各アプリケーションの障害耐性チェックを通じて、複数の高レベルの障害耐性に関する推奨事項を提供します。耐障害性カテゴリには、アプリケーションの耐障害性と信頼性を判断するためにアプリケーションをテストするすべてのチェックが一覧表示されます。これらのチェックでは、障害 AppComponent やポリシー違反が発生して障害耐性リスクが発生し、ビジネス継続性のアプリケーションの可用性に影響する可能性がある場合に警告が表示されます。また、 で対処する必要がある推奨アクションセクションで、これらのリスクを軽減する可能性を高める障害耐性に関する推奨事項も提供します AWS Resilience Hub。の各アプリケーションのレコメンデーションの詳細については AWS Trusted Advisor、「」に記載されている詳細なレコメンデーションを参照してください AWS Resilience Hub。

AWS Trusted Advisor では、 内の各アプリケーションに対して次のチェックが行われます AWS Resilience Hub。

- AWS Resilience Hub アプリケーションの耐障害性スコア – 最新の の評価からアプリケーションの耐障害性スコアをチェック AWS Resilience Hub し、その耐障害性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障害耐性スコアが 70 以上であることを示します。
  - 黄 — アプリケーションの障害耐性スコアが 40 ~ 69 であることを示します。
  - 赤 — アプリケーションの障害耐性スコアが 40 未満であることを示します。

  推奨されるアクション

障害耐性体制を改善し、アプリケーションの可能な限り最適な障害耐性スコアを取得するには、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評価を実行し、該当する場合は、推奨される運用上の推奨事項を実装します。評価の実行、レビュー、実装、運用上の推奨事項の確認と除外、およびそれらの実装の詳細については、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 および 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 および RPO の目標を達成していない場合に警告します。

  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 — 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ないことを示します。

  推奨されるアクション

  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、定義された RTO と RPO の目標を満たしていることを確認するには、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行します。さらに、アプリケーションの障害耐性ポリシーに違反していないことを確認する場合は、評価レポートを確認し、推奨される障害耐性の推奨事項を実装することをお勧めします。ユーザーに代わって AWS Resilience Hub が評価を毎日実行できるようにする方法、評価を実行する方法、障害耐性に関する推奨事項を確認する方法、およびそれらを実装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。

  - the section called “のアプリケーションリソースの編集” (AWS Resilience Hub が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、「アプリケーションプロシージャのドリフト通知設定を編集するには」のステップを完了し、「毎日の自動評価」チェックボックスを選択します。)
  - 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の経過時間 — で各アプリケーションの評価を最後に実行してからの時間を確認します 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 — 過去 30 日間にアプリケーションの評価を実行していないことを示します。

  推奨されるアクション

  評価を定期的に実行して、 上のアプリケーションのレジリエンス体制を管理および改善します AWS。ユーザーに代わってアプリケーションを毎日 AWS Resilience Hub 評価する場合は、 AWS Resilience Hub ドリフト通知でこのアプリケーションの日次自動評価チェックボックスをオンにすることで、同じことを有効にできます。このアプリケーションの日次自動評価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ドリフト通知を編集する」を完了します???。

  > **Note**
  >
  > このチェックでは、 で少なくとも 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確認します。つまり、中断イベントが発生しても復旧 AppComponent しない場合、不明なデータ損失やシステムのダウンタイムが発生する可能性があります。アラート条件が赤に設定されている場合、 AppComponent は回復不能であることを示します。

  推奨されるアクション

  AppComponent が回復可能であることを確認するには、障害耐性に関する推奨事項を確認して実装し、新しい評価を実行します。障害耐性に関する推奨事項の確認の詳細については、「」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”。

の使用の詳細については 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

次の表に、 の今回のリリースのドキュメントを示します AWS Resilience Hub。

- API バージョン: 最新
- ドキュメントの最終更新日： 2024 年 8 月 1 日

変更	説明	日付
AWS Resilience Hub にグループ化に関する推奨事項を導入	AWS Resilience Hub では、アプリケーションのオンボーディング中にリソースをアプリケーションコンポーネント (AppComponents) にグループ化する新しいスマートグループオプションが導入されました。でレジリエンス評価を実行する場合 AWS Resilience Hub、最適で実用的なレコメンデーションを受け取る AppComponents には、リソースが正確に適切なグループにグループ化されていることが重要です。このオプションは、アプリケーションのオンボーディングにかかる時間を短縮するために、複雑なアプリケーションやクロスリージョンアプリケーションに最適です。また、現在利用可能な既存のアプリケーションオンボーディングワークフローを補完します。 詳細については、次のトピックを参照してください。	2024 年 8 月 1 日

	• the section called “アプリケーションコンポーネントの管理” • the section called “AWS Resilience Hub リソースのグループ化に関する推奨事項”	
AWS Resilience Hub に新しい評価概要ウィジェットが導入されました	AWS Resilience Hub では、Amazon Bedrock の生成 AI 機能を使用して、複雑な耐障害性データを非常に実用的なインサイトに変換する新しい評価概要ウィジェットが導入されました。これらの評価の概要では、重要な結果を抽出し、リスクに優先順位を付け、レジリエンスを向上させるためのステップを推奨します。最も影響の大きい要素に焦点を当てることで、評価をより簡単に理解できるため、レジリエンス体制の最も重要な要素に焦点を当てた影響の大きい情報を得ることができます。 詳細については、「the section called “評価の概要”」を参照してください。	2024 年 8 月 1 日

AWS Resilience Hub が Amazon DocumentDB のサポートを拡張	この AWS Resilience Hub ポリシーでは、評価の実行 AWS Lambda 中に Amazon DocumentDB 、Elastic Load Balancing 、および のリソースと設定にアクセスするためのアクセス`Describe`許可を付与できます。 Elastic Load Balancing 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”。	2024 年 8 月 1 日

AWS Resilience Hub アプリケーションの耐障害性ドリフト検出機能を拡張	AWS Resilience Hub は、新しいタイプのドリフト検出 — アプリケーションリソースドリフトを導入することで、ドリフト検出機能を拡張しました。この拡張機能は、アプリケーションの入力ソース内のリソースの追加や削除などの変更を検出します。スケジュールされた AWS Resilience Hub 評価とドリフト通知サービスを有効にし、ドリフトが発生するたびに通知を受け取ることができます。最新の障害耐性評価では、ドリフトを特定し、アプリケーションを回復力ポリシーに準拠させるための修復アクションを提示します。 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 “ドリフト検出” • the section called “ステップ 5: スケジュールされた評価とドリフト通知を設定する”	2024 年 5 月 8 日

AWS Trusted Advisor の機能強化	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 () を識別するためのチェックを追加 AWS Trusted Advisor することで、の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 が推奨アラームのサポートを拡張	AWS Resilience Hub は、README.md テンプレートファイルを更新し、 AWS Resilience Hub の内部 AWS (Amazon など CloudWatch) または外部 で推奨されるアラームを作成できる値を指定しましたAWS。 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 が Amazon FSx for Windows File Server のサポートを拡張	AWS Resilience Hub は、Amazon FSx for Windows File Server リソースの評価サポートを拡張し、アプリケーションの耐障害性を評価します。Amazon FSx for Windows File Server を使用するアプリケーションの場合、 は、アベイラビリティーゾーン (AZ) とマルチ AZ 配置、バックアッププラン、およびデータレプリケーションに関する新しい一連の耐障害性に関する推奨事項 AWS Resilience Hub を提供します。 は、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で、Microsoft Active Directory へのファイルシステムの依存関係を含む Amazon FSx for Windows File Server AWS Resilience Hub をサポートします。 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 “サポートされている AWS Resilience Hub リソース” • the section called “AWSResilienceHubAssessmentExecutionPolicy” • the section called “アプリケーションコンポーネントのリソースのグループ化”	2024 年 3 月 26 日

AWS Resilience Hub は、障害耐性スコアに関する追加情報を提供します。	AWS Resilience Hub は、アプリケーションの耐障害性体制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、障害耐性スコアのユーザーエクスペリエンスを更新しました。 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 は、Amazon Elastic Kubernetes Service (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 は、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行する際に、アプリケーションの耐障害性体制を改善するためにテストとアラームを実行することが推奨されます。 詳細については、「the section called “Amazon Fault Injection Service 実験の管理”」を参照してください。	2023 年 11 月 9 日

AWS Resilience Hub は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 は、推定ワークロード RTOと推定ワークロード に関する追加情報をアプリケーションレベルで提供しますRPO。この追加情報は、最新の成功した評価から、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の最大可能性を示します。この値は、RPOすべての中断タイプの最大推定ワークロードRTOと推定ワークロードです。 詳細については、「the section called “アプリケーションの管理”」を参照してください。	2023 年 10 月 30 日

AWS Resilience Hub が AWS Step Functions リソースの評価サポートを拡張	AWS Resilience Hub は、AWS Step Functions リソースの評価サポートを拡張し、アプリケーションの障害耐性を評価します。 AWS Resilience Hub は、ステートマシンタイプ (標準ワークフローまたは Express ワークフロー) を含む AWS Step Functions 設定を分析します。さらに、AWS Resilience Hub は、推定ワークロード復旧時間目標 (RTO) と推定ワークロード復旧時間目標 () を満たすのに役立つレコメンデーションも提供しますRPO。 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、 が設定を読み AWS Step Functions 取る AWS Resilience Hub ための特定のアクセス許可を手動で追加して、必要なアクセス許可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 は運用上の推奨事項の除外を許可します	AWS Resilience Hub では、アラーム、標準操作手順 (SOPs ）、Amazon Fault Injection Service (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ました。で評価を実行する際 AWS Resilience Hub、推定復旧時間と、評価されたアプリケーションの耐障害性を向上させる方法に関する推奨事項が提供されます。レコメンデーションの除外ワークフローを使用して、レコメンデーションに関連しないレコメンデーションアラーム、SOPs、および AWS FIS 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

のアクセス許可設計の改善 AWS Resilience Hub	AWS Resilience Hub では、の AWS Identity and Access Management （ IAM) ロールを柔軟に設定するための新しいアクセス許可設計が導入されました 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。の新しい マネージドポリシーにより AWS Resilience Hub 、サポートされているサービスに対する適切なアクセス許可を持つことができます。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の耐障害性ドリフト検出 AWS Resilience Hub	AWS Resilience Hub を使用すると、アプリケーションのレジリエンスを解決するために必要なアクションを事前に検出して理解できます。Amazon Simple Notification Service (Amazon SNS) が、ワークロードの目標復旧時間 (RTO) またはワークロードの目標復旧時点 (RPO) が目標の達成から組織のビジネス目標の達成につながらなくなったときに通知を受信できるようにします。評価を手動で実行しながらレジリエンスの問題を積極的に検出することから、Amazon SNSトピックを通じて事前に通知を受けるようにすることで、潜在的な中断を早期に予測し、復旧目標を達成できるという自信を高めることができます。 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 5: スケジュールされた評価とドリフト通知を設定する” • the section called “のアプリケーションリソースの編集”	2023 年 8 月 2 日

AWS Resilience Hub で Amazon Relational Database Service と Amazon Aurora のサポートを改善	AWS Resilience Hub は、Amazon Relational Database Service プロキシ、ヘッドレスおよび Amazon Aurora DB データベース設定の評価サポートを拡張します。さらに、Amazon を含むアプリケーションを評価する際にRDS、異なるデータベースエンジンを区別して、より正確な推定ワークロード復旧時間目標 () を提供するようになりましたRTOs。 AWS Resilience Hub は、 AWS 環境内で回復力のベストプラクティスを実装するための追加のアクションも提供します。ベストプラクティスには、DevOps Gru for Amazon によるパフォーマンスに関するインサイトRDS、拡張モニタリング、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。 が、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 AWS Resilience Hub ために必要なアクセス許可の詳細については、「」を参照してくださいthe section called “AWSResilienceHubAsssessmentExecutionPolicy”。	2023 年 8 月 2 日

AWS Resilience Hub が Amazon Elastic Block Store スナップショットのサポートを拡張	AWS Resilience Hub は、Amazon Elastic Block Store (Amazon EBS) の評価サポートを拡張して、直接 を使用して同じ Amazon EBS リージョン内で作成された Amazon EBSスナップショットを認識しますAPIs。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加えて提供されます。 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 は、Amazon Elastic Compute Cloud (Amazon) のサポートを拡張しましたEC2。さまざまなサイズのアプリケーションの場合、 AWS では、Amazon を使用するお客様がユースケースに適した設定EC2を選択できます。 は、次の Amazon EC2設定の評価 AWS Resilience Hub 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) による自動スケーリンググループのサポート ARC 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 アクセス許可リファレンス”」を参照してください。	2023 年 6 月 27 日

AWS マネージドポリシーの更新	評価を実行するための他の AWS 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の場合、 は、オンデマンドおよびプロビジョニングされたキャパシティモードとグローバルテーブルの耐障害性リスクを警告する新しいアラームセットを提供する AWS Resilience Hub 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 アクセス許可リファレンス”」を参照してください。	2023 年 5 月 2 日

AWS Trusted Advisor の機能強化	AWS Resilience Hub は、Amazon DynamoDB を使用する AWS Trusted Advisor および アプリケーションのサポートを拡張しました。 AWS Trusted Advisor で 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とき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	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 バックアップの現在のサポートに加えて、マルチリージョンアクセスポイント、Amazon S3 レプリケーション時間制御 (Amazon S3 RTC) 、 AWS バックアップ point-in-time リカバリ (PITR) 設定について Amazon S3 を評価する AWS Resilience Hub ようになりました。 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 アクセス許可リファレンス” • 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されているリソースとして Amazon EKS クラスターを追加しました。お客様は、新規または既存のアプリケーションに Amazon EKSクラスターを追加し、障害耐性を向上させるための評価とレコメンデーションを受け取ることができます。お客様は、、Terraform AWS CloudFormation、AWS Resource Groupsおよび を使用してアプリケーションリソースを追加できます AppRegistry。さらに、お客様は、各EKSクラスターに 1 つ以上の名前空間を持つ 1 つ以上のリージョンに 1 つ以上の Amazon クラスターを直接追加できます。これにより、 AWS Resilience Hub は単一リージョンおよびクロスリージョンの評価とレコメンデーションを提供できます。デプロイ、 レプリカ、ReplicationControllers、ポッドを調べるだけでなく、 AWS Resilience Hub はクラスター全体の耐障害性を分析します。 はステートレス Amazon EKSクラスターワークロード AWS Resilience Hub をサポートします。新機能は、 AWS	2023 年 3 月 21 日

	Resilience Hub がサポートされているすべての AWS 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 クラスターの追加” • the section called “AWS Resilience Hub アクセス許可リファレンス” • AWS リージョンサービス	
Amazon Elastic File System の追加サポート	Amazon Elastic File System (Amazon EFS) バックアップの現在のサポートに加えて、 AWS Resilience Hub は Amazon レEFSプリケーションと AZ 設定EFSについて Amazon を評価するようになりました。 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 “サポートされている AWS Resilience Hub 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 は、アプリケーションソースに関する透明性を提供するようになりました。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 “のアプリケーションリソースの編集”」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 は、アプリケーションに関連付けられたリソースに関する追加情報を収集する入力メカニズムを提供するようになりました。この情報 AWS Resilience Hub により、 は リソースをより深く理解し、耐障害性に関する推奨事項を提供します。 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 “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、 AWS Resilience Hub は Amazon Data Lifecycle Manager と Amazon EBS Fast snapshot restore () EBSによって Amazon スナップショットを評価できるようになりましたFSR。 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 アクセス許可リファレンス” • 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、 によって評価されたアカウントに関連付けられたアプリケーションを表示できます AWS Resilience Hub。は最新の耐障害性スコア AWS Trusted Advisor を表示し、ターゲットの耐障害性ポリシー (RTO および RPO) が満たされているかどうかを示すステータスを提供します。評価を実行するたびに、 は最新の結果 AWS Trusted Advisor で AWS Resilience Hub 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レコメンデーション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 は、サブスクライバーを含む Amazon SNS設定を分析しSNSて Amazon を使用してアプリケーションを評価し、アプリケーションの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) を満たすためのレコメンデーションを提供するようになりました。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 “サポートされている AWS Resilience Hub リソース” • the section called “Identity and Access Management” • the section called “アプリケーションコンポーネントのリソースのグループ化”	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 は、Elastic Load Balancing と Amazon Relational Database Service (Amazon) について Amazon Route 53 を評価するようになりました。これには、Amazon Route 53 ARCが有益なタイミングに関するアドバイスが含まれます。 ARC Elastic Load Balancing Amazon Relational Database Service RDS を拡張して AWS Resilience Hub、Amazon Route 53 ARC 評価は AWS Auto Scaling Group (AWS ASG) と Amazon DynamoDB を超えてサポートされます。Amazon Route 53 ARCはアプリケーションの高可用性を提供するため、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 “サポートされている AWS Resilience Hub リソース” • the section called “Identity and Access Management”	2022 年 11 月 16 日

Backup の追加サポート AWS	AWS Resilience Hub は、Elastic Load Balancing と Amazon Relational Database Service (Amazon) について Amazon Route 53 を評価するようになりました。これには、Amazon Route 53 ARC が有益なタイミングに関するアドバイスが含まれます。ARC Elastic Load Balancing Amazon Relational Database Service RDS を拡張して AWS Resilience Hub、Amazon Route 53 ARC評価は AWS Auto Scaling Group (AWS ASG) と Amazon DynamoDB を超えてサポートされています。Amazon Route 53 ARCはアプリケーションの高可用性を提供するため、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 “サポートされている AWS Resilience Hub 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	Route53 と AWS Backup が、AppComponent グループ化セクションでサポートされているアプリケーションコンポーネントリソースのリストに追加されました。	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
の紹介 AWS Resilience Hub	AWS Resilience Hub が利用可能になりました。このガイドでは、 AWS Resilience Hub を使用してインフラストラクチャを分析し、 AWS アプリケーションの耐障害性を向上させるためのレコメンデーションを取得し、耐障害性スコアを確認する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。