Guida per l'utente

AWS Hub di resilienza

AWS Hub di resilienza: Guida per l'utente

Table of Contents

Che cos'è AWS Resilience Hub?

AWS Resilience Hub è una posizione centrale su cui gestire e migliorare il livello di resilienza delle applicazioni. AWS AWS Resilience Hub ti consente di definire i tuoi obiettivi di resilienza, valutare la tua posizione di resilienza rispetto a tali obiettivi e implementare raccomandazioni per il miglioramento basate sul Well-Architected AWS Framework. All'interno AWS Resilience Hub, puoi anche creare ed eseguire esperimenti di Amazon Fault Injection Service, che imitano le interruzioni reali della tua applicazione per aiutarti a comprendere meglio le dipendenze e scoprire potenziali punti deboli. AWS Resilience Hub fornisce una posizione centrale con tutti i AWS servizi e gli strumenti necessari per rafforzare continuamente la tua posizione di resilienza. AWS Resilience Hub collabora con altri servizi per fornire consigli e aiutarti a gestire le risorse delle applicazioni. Per ulteriori informazioni, consulta Utilizzo di altri servizi .

La tabella seguente fornisce i collegamenti alla documentazione di tutti i servizi di resilienza correlati.

Servizi e riferimenti di AWS resilienza correlati

AWS servizio di resilienza	Collegamento alla documentazione
AWS Elastic Disaster Recovery	Che cos'è Elastic Disaster Recovery
AWS Backup	Che cos'è AWS Backup
Controller di ripristino delle applicazioni Amazon Route 53 (Route 53ARC)	Cos'è Amazon Route 53 Application Recovery Controller

Argomenti

- AWS Resilience Hub — Gestione della resilienza
- AWS Resilience Hub — Test di resilienza
- AWS Resilience Hub concetti
- AWS Resilience Hub persone
- AWS Resilience Hub risorse supportate

AWS Resilience Hub — Gestione della resilienza

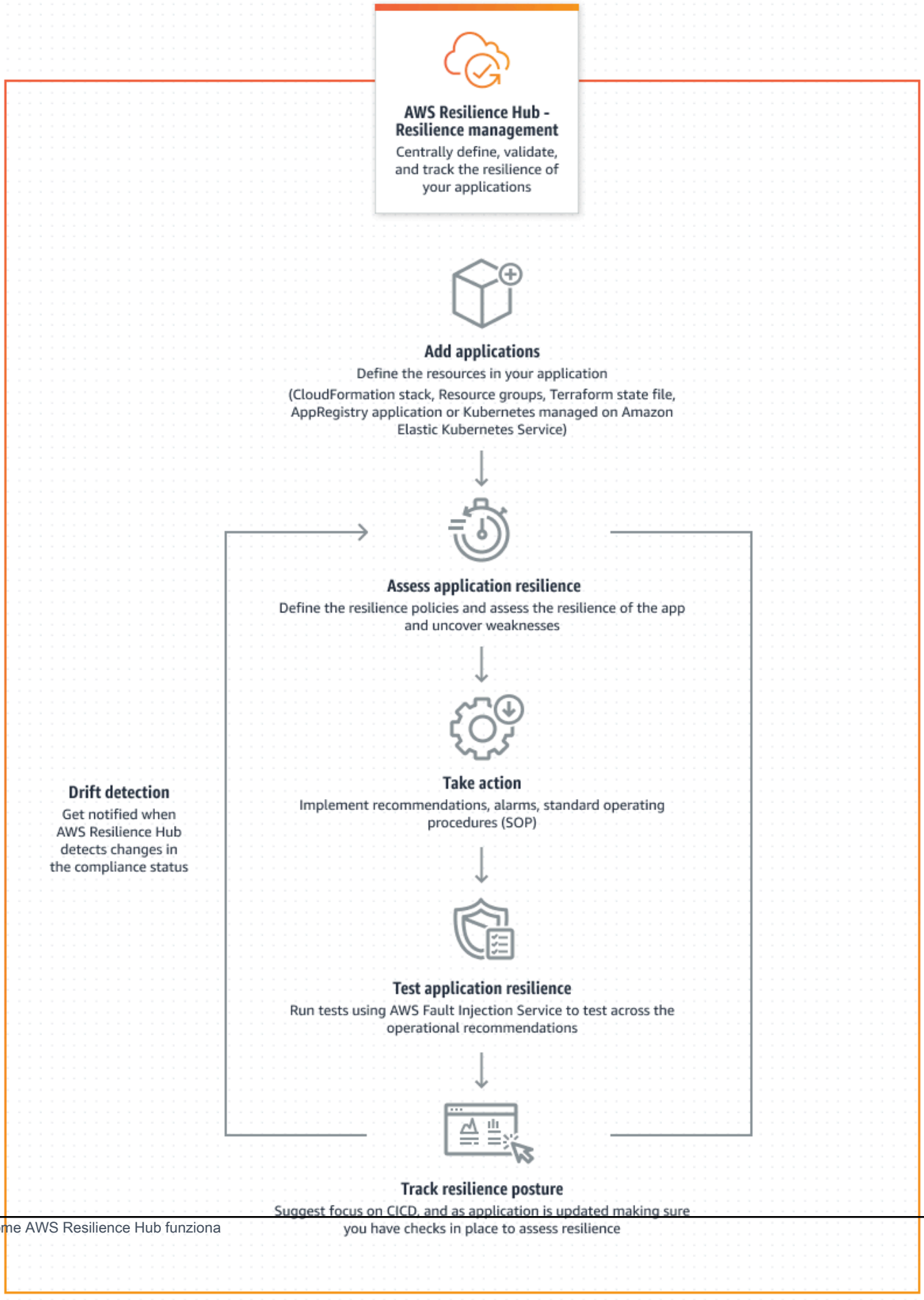
AWS Resilience Hub ti offre una posizione centrale per definire, convalidare e monitorare la resilienza della tua applicazione. AWS AWS Resilience Hub aiuta a proteggere le applicazioni dalle interruzioni e a ridurre i costi di ripristino per ottimizzare la continuità aziendale e contribuire a soddisfare i requisiti normativi e di conformità. È possibile utilizzare AWS Resilience Hub per effettuare le seguenti operazioni:

- Analizza la tua infrastruttura e ottieni consigli per migliorare la resilienza delle tue applicazioni. Oltre alle linee guida sull'architettura per migliorare la resilienza delle applicazioni, i consigli forniscono il codice per soddisfare le politiche di resilienza, implementare test, allarmi e procedure operative standard (SOPs) che è possibile implementare ed eseguire con l'applicazione nella pipeline di integrazione e distribuzione (CI/CD).
- Valuta gli obiettivi del tempo di ripristino (RTO) e dell'obiettivo del punto di ripristino () in condizioni diverse. RPO
- Ottimizza la continuità aziendale riducendo al contempo i costi di ripristino.
- Identifica e risolvi i problemi prima che si verifichino in produzione.

Dopo aver distribuito un'applicazione in produzione, puoi aggiungerla AWS Resilience Hub alla tua pipeline CI/CD per convalidare ogni build prima che venga rilasciata in produzione.

Come funziona AWS Resilience Hub

Il diagramma seguente fornisce una panoramica di alto livello di come funziona. AWS Resilience Hub


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

Describe

Descrivi la tua applicazione importando risorse da AWS CloudFormation stack, file di stato Terraform AWS Resource Groups, cluster Amazon Elastic Kubernetes Service oppure puoi scegliere tra applicazioni già definite in. AWS Service Catalog AppRegistry

Definisci

Definisci le politiche di resilienza per le tue applicazioni. Queste politiche includono RPO gli obiettivi per RTO le interruzioni delle applicazioni, dell'infrastruttura, della zona di disponibilità e della regione. Questi obiettivi vengono utilizzati per stimare se l'applicazione soddisfa la politica di resilienza.

Valutazione

Dopo aver descritto l'applicazione e aver associato una policy di resilienza, esegui una valutazione della resilienza. La AWS Resilience Hub valutazione utilizza le migliori pratiche del AWS Well-Architected Framework per analizzare i componenti di un'applicazione e scoprire potenziali punti deboli in termini di resilienza. Questi punti deboli possono essere causati da una configurazione incompleta dell'infrastruttura, da una configurazione errata o da situazioni in cui sono necessari ulteriori miglioramenti della configurazione. Per migliorare la resilienza, aggiorna l'applicazione e la politica di resilienza in base alle raccomandazioni del rapporto di valutazione. I consigli includono configurazioni di componenti, allarmi, test e ripristino. SOPs Quindi, puoi eseguire un'altra valutazione e confrontare i risultati con il rapporto precedente per vedere quanto migliora la resilienza. Ripeti questo processo finché il carico di lavoro stimato RTO e il carico di lavoro stimato non raggiungono gli obiettivi RPO prefissati. RTO RPO

Convalida

Esegui test per misurare la resilienza delle AWS risorse e il tempo necessario per il ripristino da applicazioni, infrastrutture, zone di disponibilità e Regione AWS incidenti. Per misurare la resilienza, questi test simulano le interruzioni delle risorse. AWS Esempi di interruzioni includono errori di rete non disponibili, failover, processi interrotti, ripristino all'RDSavvio di Amazon e problemi con la tua zona di disponibilità.

Visualizza e monitora

Dopo aver distribuito un' AWS applicazione in produzione, puoi continuare AWS Resilience Hub a monitorare lo stato di resilienza dell'applicazione. Se si verifica un'interruzione, l'operatore può visualizzarla AWS Resilience Hub e avviare il processo di ripristino associato.

AWS Resilience Hub — Test di resilienza

AWS Resilience Hub ti consente di eseguire test ed esperimenti di Amazon Fault Injection Service (AWS FIS) sui tuoi AWS carichi di lavoro e mantenere una resilienza ottimale. Questi test stressano un'applicazione creando eventi dirompenti in modo da poter osservare come risponde l'applicazione. AWS FIS offre diversi scenari predefiniti e un'ampia selezione di azioni che generano interruzioni. Inoltre, include anche i controlli e i guardrail necessari per eseguire gli esperimenti in produzione. I controlli e i guardrail includono opzioni per eseguire il rollback automatico o interrompere l'esperimento se vengono soddisfatte condizioni specifiche. Per iniziare a utilizzare l'opzione AWS FIS per eseguire esperimenti dalla AWS Resilience Hub console, completa i prerequisiti definiti nella sezione. the section called “Prerequisiti”

La tabella seguente elenca tutte le AWS FIS opzioni disponibili dal riquadro di navigazione e i collegamenti alla AWS FIS documentazione associata che contiene le procedure per iniziare a utilizzare AWS FIS i test dalla AWS Resilience Hub console.

AWS FIS opzioni e riferimenti del menu di navigazione

AWS FIS opzione del menu di navigazione	AWS FIS documentazione
test di resilienza	Crea un modello di esperimento
Libreria di scenari	AWS FIS libreria
modelli di esperimenti	Modelli di esperimenti per AWS FIS

La tabella seguente elenca tutte le AWS FIS opzioni disponibili dal menu a discesa nella sezione Resilience testing e i collegamenti alla AWS FIS documentazione associata che contiene le procedure per iniziare a utilizzare AWS FIS i test dalla AWS Resilience Hub console.

AWS FIS opzioni e riferimenti del menu a discesa

AWS FIS opzione del menu a discesa	AWS FIS documentazione
Crea un modello di esperimento	Crea un modello di esperimento
Crea un esperimento partendo da uno scenario	Utilizzo di uno scenario

AWS Resilience Hub concetti

Questi concetti possono aiutarvi a comprendere meglio l' AWS Resilience Hub approccio adottato per migliorare la resilienza delle applicazioni e prevenire le interruzioni delle applicazioni.

Resilienza

La capacità di mantenere la disponibilità e di riprendersi da interruzioni del software e dell'operatività in un determinato periodo di tempo.

Obiettivo del punto di ripristino () RPO

Il periodo di tempo massimo accettabile dall'ultimo punto di ripristino dei dati. Ciò determina quella che viene considerata una perdita di dati accettabile tra l'ultimo punto di ripristino e l'interruzione del servizio.

Obiettivo del tempo di ripristino () RTO

Il ritardo massimo accettabile tra l'interruzione del servizio e il ripristino del servizio. Ciò determina quale finestra temporale è considerata accettabile quando il servizio non è disponibile.

Obiettivo stimato del tempo di ripristino del carico di lavoro

L'obiettivo stimato in termini di tempo di ripristino del carico di lavoro (carico di lavoro stimatoRTO) è l'obiettivo stimato RTO che l'applicazione raggiungerà in base alla definizione dell'applicazione importata e quindi eseguirà una valutazione.

Obiettivo stimato del punto di ripristino del carico di lavoro

L'obiettivo stimato del punto di ripristino del carico di lavoro (carico di lavoro stimatoRPO) è l'obiettivo stimato RPO che l'applicazione raggiungerà in base alla definizione dell'applicazione importata e quindi eseguirà una valutazione.

Applicazione

Un' AWS Resilience Hub applicazione è una raccolta di risorse AWS supportate che vengono continuamente monitorate e valutate per gestirne il livello di resilienza.

Componente dell'applicazione

Un gruppo di AWS risorse correlate che funzionano e falliscono come unità singola. Ad esempio, se avete un database primario e uno di replica, entrambi i database appartengono allo stesso componente applicativo (AppComponent).

AWS Resilience Hub determina quali AWS risorse possono appartenere a quale tipo di AppComponent. Ad esempio, a `DBInstance` può appartenere a `AWS::ResilienceHub::DatabaseAppComponent` ma non a`AWS::ResilienceHub::ComputeAppComponent`.

Stato di conformità dell'applicazione

AWS Resilience Hub riporta i seguenti tipi di stato di conformità per le applicazioni.

Politica soddisfatta

Si stima che l'applicazione soddisfi gli RPO obiettivi RTO e gli obiettivi definiti nella politica. Tutti i suoi componenti soddisfano gli obiettivi politici definiti. Ad esempio, hai selezionato un RTO RPO obiettivo di 24 ore per le interruzioni in tutte le AWS regioni. AWS Resilience Hub puoi vedere che i tuoi backup vengono copiati nella tua regione di riserva. È comunque necessario mantenere un ripristino da una procedura operativa standard di backup (SOP) e testarlo e cronometrarlo. Questo è incluso nelle raccomandazioni operative e fa parte del punteggio di resilienza complessivo.

Politica violata

Non è stato possibile stimare che l'applicazione soddisfi RTO gli RPO obiettivi definiti nella politica. Uno o più di essi AppComponents non soddisfano gli obiettivi politici. Ad esempio, è stato selezionato un RTO RPO obiettivo di 24 ore per le interruzioni tra le AWS regioni, ma la configurazione del database non include alcun metodo di ripristino interregionale, come la replica globale e le copie di backup.

Non valutato

La domanda richiede una valutazione. Al momento non è valutata o tracciata.

Modifiche rilevate

Esiste una nuova versione pubblicata dell'applicazione che non è stata ancora valutata.

Rilevamento delle deviazioni

AWS Resilience Hub esegue una notifica di drift mentre esegue una valutazione dell'applicazione per verificare se le modifiche alle AppComponent configurazioni hanno influito sullo stato di conformità dell'applicazione. Inoltre, controlla e rileva anche modifiche come l'aggiunta o l'eliminazione di risorse all'interno delle fonti di input dell'applicazione e invia notifiche in merito. Per fare un confronto, AWS Resilience Hub utilizza la valutazione precedente in cui il componente dell'applicazione soddisfaceva la politica. AWS Resilience Hub rileva i seguenti tipi di derive:

- Deviazione delle politiche applicative: questo tipo di deriva identifica tutte quelle AppComponents che erano conformi alla policy nella valutazione precedente ma che non erano conformi nella valutazione corrente.
- Deriva delle risorse dell'applicazione: questo tipo di deriva identifica tutte le risorse alla deriva nella versione corrente dell'applicazione.

Valutazione della resilienza

AWS Resilience Hub utilizza un elenco di lacune e potenziali rimedi per misurare l'efficacia di una politica selezionata per riprendersi e continuare dopo un disastro. Valuta ogni componente dell'applicazione o lo stato di conformità dell'applicazione alla policy. Questo rapporto include raccomandazioni per l'ottimizzazione dei costi e riferimenti a potenziali problemi.

Punteggio di resilienza

AWS Resilience Hub genera un punteggio che indica quanto attentamente l'applicazione segue i nostri consigli per soddisfare la politica di resilienza, gli allarmi, le procedure operative standard (SOPs) e i test dell'applicazione.

Tipo di interruzione

AWS Resilience Hub ti aiuta a valutare la resilienza rispetto ai seguenti tipi di interruzioni:

Applicazione

L'infrastruttura è integra, ma lo stack di applicazioni o software non funziona come necessario. Ciò può verificarsi dopo l'implementazione di nuovo codice, le modifiche alla configurazione, il danneggiamento dei dati o il malfunzionamento delle dipendenze a valle.

Infrastruttura cloud

L'infrastruttura cloud non funziona come previsto a causa di un'interruzione. Un'interruzione può verificarsi a causa di un errore locale in uno o più componenti. Nella maggior parte dei casi, questo tipo di interruzione viene risolto riavviando, riciclando o ricaricando i componenti difettosi.

Interruzione dell'infrastruttura Cloud AZ

Una o più zone di disponibilità non sono disponibili. Questo tipo di interruzione può essere risolto passando a una zona di disponibilità diversa.

Incidente relativo alla regione dell'infrastruttura cloud

Una o più regioni non sono disponibili. Questo tipo di incidente può essere risolto passando a un altro Regione AWS.

Esperimenti di iniezione di errori

AWS Resilience Hub consiglia di eseguire test per verificare la resilienza delle applicazioni rispetto a diversi tipi di interruzioni. Queste interruzioni includono applicazioni, infrastrutture, zone di disponibilità (AZ) o Regione AWS incidenti relativi ai componenti dell'applicazione.

Questi esperimenti consentono di effettuare le seguenti operazioni:

- Iniettare un errore.
- Verifica che gli allarmi siano in grado di rilevare un'interruzione.
- Verificate che le procedure di ripristino, o le procedure operative standard (SOPs), funzionino correttamente per ripristinare l'applicazione dall'interruzione.

Test per SOPs misurare il carico di lavoro stimato RTO e il carico di lavoro stimato. RPO È possibile testare diverse configurazioni delle applicazioni e misurare se l'output RTO RPO soddisfa gli obiettivi definiti nella politica.

SOP

Una procedura operativa standard (SOP) è una serie di passaggi prescrittivi progettati per ripristinare in modo efficiente l'applicazione in caso di interruzione o allarme. In base alla valutazione dell'applicazione, AWS Resilience Hub consiglia una serie di opzioni SOPs e si consiglia di prepararle, testarle e SOPs misurarle prima di un'interruzione per garantire un ripristino tempestivo.

AWS Resilience Hub persone

La creazione di un'applicazione aziendale richiede uno sforzo collaborativo da parte di diversi team interfunzionali come l'infrastruttura, la continuità aziendale, il proprietario dell'applicazione e altre parti interessate responsabili del monitoraggio delle applicazioni. Le diverse personalità dei diversi team contribuiscono alla creazione e alla gestione delle applicazioni AWS Resilience Hub, ognuna con un ruolo e responsabilità diversi. Per ulteriori informazioni sulla concessione di autorizzazioni a diversi utenti, consulta. the section called “AWS Resilience Hub riferimenti a personaggi e IAM autorizzazioni”

Per iniziare a creare applicazioni ed eseguire valutazioni in AWS Resilience Hub, ti consigliamo di creare i seguenti personaggi:

- Gestore delle applicazioni dell'infrastruttura: gli utenti con questa persona sono responsabili della configurazione, della configurazione e della manutenzione delle risorse dell'infrastruttura e delle applicazioni, garantendo l'affidabilità e la sicurezza dell'applicazione. Le loro responsabilità includono quanto segue:
  - Garantire che le applicazioni vengano distribuite e aggiornate regolarmente
  - Monitoraggio delle prestazioni del sistema
  - Risoluzione dei problemi
  - Implementazione di piani di backup e disaster recovery
- Responsabile della continuità operativa: gli utenti con questa personalità sono responsabili della definizione delle politiche applicative e della determinazione della criticità aziendale delle applicazioni. Le loro responsabilità includono quanto segue:
  - Prendere decisioni chiave nella definizione delle politiche
  - Valutazione della criticità aziendale
  - Allocazione delle risorse per le applicazioni critiche
  - Valutazione e gestione dei rischi
- Proprietario dell'applicazione: gli utenti con questa persona hanno la responsabilità di garantire applicazioni altamente disponibili e affidabili. Le loro responsabilità includono quanto segue:
  - Definizione di identificatori prestazionali chiave per misurare e monitorare le prestazioni delle applicazioni e identificare i punti deboli
  - Organizzazione di corsi di formazione per più parti interessate
  - Garantire che la seguente documentazione sia up-to-date:

    - Architettura dell'applicazione
    - Processi di implementazione
    - Configurazioni di monitoraggio
    - Tecniche di ottimizzazione delle prestazioni
- Accesso in sola lettura: gli utenti con questa persona sono limitati alle autorizzazioni di sola lettura. Le loro responsabilità includono il mantenimento della visibilità e della supervisione delle prestazioni e dello stato di un'applicazione monitorando il punteggio di resilienza, le raccomandazioni operative e le raccomandazioni sulla resilienza. Inoltre, sono anche responsabili dell'identificazione di problemi, tendenze e aree di miglioramento per garantire che l'applicazione soddisfi gli obiettivi dell'organizzazione.

AWS Resilience Hub risorse supportate

Le risorse che influiscono sulle prestazioni delle applicazioni in caso di interruzione sono pienamente supportate da risorse di AWS Resilience Hub alto livello come `AWS::RDS::DBInstance` e. `AWS::RDS::DBCluster`

Per ulteriori informazioni sulle autorizzazioni necessarie AWS Resilience Hub per includere nella valutazione le risorse di tutti i servizi supportati, consulta. the section called “AWSResilienceHubAsssessmentExecutionPolicy”

AWS Resilience Hub supporta le risorse dei seguenti AWS servizi:

- Calcolo
    - Amazon Elastic Compute Cloud (AmazonEC2)

> **Note**
>
> AWS Resilience Hub non supporta il vecchio formato Amazon Resource Name (ARN) per l'accesso alle EC2 risorse Amazon. Il nuovo ARN formato utilizza l'ID AWS dell'account e consente una maggiore capacità di etichettare le risorse nel cluster, oltre a tenere traccia del costo dei servizi e delle attività in esecuzione nel cluster.
>
> - Vecchio formato (obsoleto): `arn:aws:ec2:<region>::instance/<instance-id>`
> - Nuovo formato — `arn:aws:ec2:<region>:<account-id>:instance/<instance-id>`

Per ulteriori informazioni sul nuovo ARN formato, consulta Migrazione della ECS distribuzione Amazon al nuovo ARN formato Resource ID.

- AWS Lambda
- Servizio Amazon Elastic Kubernetes (Amazon) EKS
- Amazon Elastic Container Service (AmazonECS)
- AWS Step Functions

- Database
  - Amazon Relational Database Service (AmazonRDS)
  - Amazon DynamoDB
  - Amazon DocumentDB
- Reti e distribuzione di contenuti
  - Amazon Route 53
  - Sistema di bilanciamento del carico elastico
  - Traduzione degli indirizzi di rete () NAT
- Storage
  - Amazon Elastic Block Store (AmazonEBS)
  - Amazon Elastic File System (AmazonEFS)
  - Amazon Simple Storage Service (Amazon S3)
  - File server Amazon FSx per Windows
- Altri
  - Amazon API Gateway
  - Controller di ripristino delle applicazioni Amazon Route 53 (Amazon Route 53ARC)
  - Amazon Simple Notification Service
  - Amazon Simple Queue Service
  - AWS Auto Scaling
  - AWS Backup
  - AWS Ripristino di emergenza elastico

Note

- AWS Resilience Hub fornisce ulteriore trasparenza per le risorse dell'applicazione, consentendoti di visualizzare le istanze supportate di ciascuna risorsa. Inoltre, AWS Resilience Hub fornisce consigli di resilienza più accurati identificando un'istanza unica di ogni risorsa e individuando le istanze della risorsa durante il processo di valutazione. Per ulteriori informazioni sull'aggiunta di istanze di risorse all'applicazione, consulta. Modifica delle risorse delle AWS Resilience Hub applicazioni
- AWS Resilience Hub supporta Amazon EKS e Amazon ECS su AWS Fargate.
- AWS Resilience Hub supporta la valutazione delle AWS Backup risorse come parte dei seguenti servizi:
  - Amazon EBS
  - Amazon EFS
  - Amazon S3
  - Database globale Amazon Aurora
  - Amazon DynamoDB
  - RDSServizi Amazon
  - File server Amazon FSx per Windows
- Amazon Route 53 ARC AWS Resilience Hub valuta solo Amazon DynamoDB global, Elastic Load Balancing, Amazon e gruppi. RDS AWS Auto Scaling
- AWS Resilience Hub Per valutare le risorse interregionali, raggruppa le risorse in un unico componente applicativo. Per ulteriori informazioni sulle risorse supportate da ciascuno dei componenti dell' AWS Resilience Hub applicazione e sulle risorse di raggruppamento, vedere. Raggruppamento di risorse in un componente applicativo
- Attualmente, AWS Resilience Hub non supporta le valutazioni interregionali per i EKS cluster Amazon se il EKS cluster Amazon si trova o se l'applicazione è creata in una regione abilitata all'opt-in. AWS
- Attualmente, AWS Resilience Hub valuta solo i seguenti tipi di risorse Kubernetes:
  - Distribuzioni
  - ReplicaSets
  - Cialde

AWS Resilience Hub ignora i seguenti tipi di risorse:

- Risorse che non influiscono sul carico di lavoro stimato RTO o sul carico di lavoro stimato RPO: le risorse che non influiscono sul carico di lavoro stimato RTO o sul carico di lavoro RPO stimato vengono ignorate da. `AWS::RDS::DBParameterGroup` AWS Resilience Hub
- Risorse non di primo livello: importano AWS Resilience Hub solo risorse di primo livello, poiché possono derivare altre proprietà interrogando le proprietà delle risorse di primo livello. Ad esempio, `AWS::ApiGateway::RestApi` e `AWS::ApiGatewayV2::Api` sono risorse supportate per Amazon API Gateway. Tuttavia, non `AWS::ApiGatewayV2::Stage` è una risorsa di primo livello. Pertanto, non viene importata da AWS Resilience Hub.

> **Note**
>
> Risorse non supportate
>
> - Non è possibile identificare più risorse utilizzando AWS Resource Groups (Amazon Route 53 RecordSets e API -GWHTTP) e le risorse Amazon Aurora Global. Se desideri analizzare queste risorse come parte della valutazione, devi aggiungere manualmente la risorsa all'applicazione. Tuttavia, quando aggiungi risorse Amazon Aurora Global per la valutazione, queste devono essere raggruppate con il componente applicativo dell'RDSistanza Amazon. Per ulteriori informazioni sulla modifica delle risorse, consulta. the section called “Modifica delle risorse delle applicazioni”
> - Queste risorse possono influire sul ripristino delle applicazioni, ma AWS Resilience Hub al momento non sono completamente supportate da. AWS Resilience Hub si sforza di avvisare gli utenti delle risorse non supportate se l'applicazione è supportata da uno AWS CloudFormation stack, da un file di stato Terraform o da un'applicazione. AWS Resource Groups AppRegistry

Nozioni di base

Questa sezione descrive come iniziare a utilizzare AWS Resilience Hub. Ciò include la creazione di autorizzazioni AWS Identity and Access Management (IAM) per un account.

Argomenti

Prerequisiti

Prima di poter utilizzare il AWS Resilience Hub, è necessario completare i seguenti prerequisiti:

- AWS account: crea uno o più AWS account per ogni tipo di account (account primari/secondari/di risorse) in cui desideri utilizzare. AWS Resilience Hub Per ulteriori informazioni sulla creazione e la gestione AWS degli account, consulta quanto segue:
  - AWS Utente per la prima volta — Guida introduttiva: sei un AWS utente alle prime armi?
  - Gestione dell' AWS account — https://docs.aws.amazon.com/accounts/latest/reference/managing-accounts.html
- AWS Identity and Access Management Autorizzazioni (IAM): dopo aver creato gli AWS account, devi configurare i ruoli e le autorizzazioni IAM richiesti per ciascuno degli account che hai creato. Ad esempio, se hai creato un AWS account per accedere alle risorse dell'applicazione, devi impostare un nuovo ruolo e configurare le autorizzazioni IAM necessarie per accedere AWS Resilience Hub alle risorse dell'applicazione dal tuo account. Per ulteriori informazioni sulle autorizzazioni IAM, consulta the section called “Come funziona AWS Resilience Hub con IAM” e per ulteriori informazioni sull'aggiunta di una policy al ruolo, consulta. the section called “Definizione della politica di fiducia tramite JSON file”

  Per iniziare rapidamente ad aggiungere autorizzazioni IAM a utenti, gruppi e ruoli, puoi utilizzare le nostre politiche AWS gestite ()the section called “AWS politiche gestite”. È più facile utilizzare le policy AWS gestite per coprire i casi d'uso comuni disponibili in azienda Account AWS piuttosto che scrivere policy da soli. AWS Resilience Hub aggiunge autorizzazioni aggiuntive a una policy AWS gestita per estendere il supporto ad altri AWS servizi e includere nuove funzionalità. Quindi:

- Se sei un cliente esistente e desideri che la tua applicazione utilizzi gli ultimi miglioramenti inclusi nella valutazione, devi pubblicare una nuova versione dell'applicazione e quindi eseguire una nuova valutazione. Per ulteriori informazioni, consulta i seguenti argomenti:
  - the section called “Pubblica una nuova versione dell'applicazione”
  - the section called “Esecuzione di valutazioni della resilienza”
- Se non utilizzi policy AWS gestite per assegnare le autorizzazioni IAM appropriate a utenti, gruppi e ruoli, devi configurare manualmente queste autorizzazioni. Per ulteriori informazioni sulle politiche AWS gestite, consulta. the section called “AWSResilienceHubAsssessmentExecutionPolicy”

Aggiungere un'applicazione a AWS Resilience Hub

AWS Resilience Hub offre una valutazione e una convalida della resilienza che si integrano nel ciclo di vita dello sviluppo del software. AWS Resilience Hub ti aiuta a preparare e proteggere in modo proattivo le tue applicazioni dalle interruzioni mediante: AWS

- Individuazione dei punti deboli in termini di resilienza.
- Stimare se l'obiettivo prefissato in termini di tempo di ripristino (RTO) e l'obiettivo del punto di ripristino (RPO) possono essere raggiunti.
- Risoluzione dei problemi prima che vengano messi in produzione.

Questa sezione guida l'utente nell'aggiunta di un'applicazione. Raccogli risorse da un'applicazione, da uno AWS CloudFormation stack o da uno stack esistenti AppRegistry e crei una politica di resilienza appropriata. AWS Resource Groups Dopo aver descritto un'applicazione, è possibile pubblicarla e generare un rapporto di valutazione sulla resilienza dell'applicazione. AWS Resilience HubÈ quindi possibile utilizzare i consigli della valutazione per migliorare la resilienza. È possibile eseguire un'altra valutazione, confrontare i risultati e quindi iterare fino a RPO raggiungere gli obiettivi prefissati con il carico di lavoro stimato RTO e il carico di lavoro stimato. RTO RPO

Argomenti

- Fase 1: Inizia aggiungendo un'applicazione
- Fase 2: Come viene gestita l'applicazione?
- Fase 3: Aggiungere risorse all'applicazione AWS Resilience Hub
- Fase 4: Impostare e RTO RPO

Fase 1: Inizia aggiungendo un'applicazione

Inizia AWS Resilience Hub descrivendo i dettagli della tua AWS applicazione ed eseguendo un rapporto per valutare la resilienza.

Per iniziare, nella AWS Resilience Hub home page sotto Guida introduttiva, scegli Aggiungi applicazione.

Per ulteriori informazioni sui costi e sulla fatturazione associati AWS Resilience Hub, consulta la pagina AWS Resilience Hub dei prezzi.

Descrivi i dettagli della tua candidatura in AWS Resilience Hub

Questa sezione mostra come descrivere i dettagli della tua AWS candidatura esistente in AWS Resilience Hub.

Per descrivere i dettagli della tua candidatura

1. Immetti un nome per l'applicazione.
2. (Facoltativo) Inserisci una descrizione per l'applicazione.

Next

Fase 2: Come viene gestita l'applicazione?

Fase 2: Come viene gestita l'applicazione?

Oltre a AWS CloudFormation stack AWS Resource Groups, AppRegistry applicazioni e file di stato Terraform, puoi aggiungere risorse che si trovano nei cluster Amazon Elastic Kubernetes Service (Amazon). EKS Cioè, AWS Resilience Hub ti consente di aggiungere risorse che si trovano nei

tuoi EKS cluster Amazon come risorse opzionali. Questa sezione fornisce le seguenti opzioni, che consentono di determinare la posizione delle risorse dell'applicazione.

- Raccolte di risorse: selezionate questa opzione se desiderate scoprire le risorse da una delle raccolte di risorse. Le raccolte di risorse includono AWS CloudFormation pile AWS Resource Groups, AppRegistry applicazioni e file di stato Terraform.

  Se si seleziona questa opzione, è necessario completare una delle procedure in. the section called “Aggiungere raccolte di risorse”
- EKSsolo: seleziona questa opzione se desideri scoprire risorse dai namespace all'interno dei cluster Amazon. EKS

  Se selezioni questa opzione, devi completare la procedura in the section called “Aggiungi cluster EKS”
- Raccolte di risorse e EKS: seleziona questa opzione se desideri scoprire risorse da una delle raccolte di risorse e dai EKS cluster Amazon.

  Se selezioni questa opzione, completa una delle procedure in, the section called “Aggiungere raccolte di risorse” quindi completa la procedura inthe section called “Aggiungi cluster EKS”.

> **Note**
>
> Per informazioni sul numero di risorse supportate per applicazione, vedere Service Quotas.

Next

Fase 3: Aggiungere risorse all'applicazione AWS Resilience Hub

Fase 3: Aggiungere risorse all'applicazione AWS Resilience Hub

Questa sezione illustra le seguenti opzioni che è possibile utilizzare per costituire la base della struttura dell'applicazione:

- the section called “Aggiungere raccolte di risorse”
- the section called “Aggiungi cluster EKS”

Aggiungere raccolte di risorse

Questa sezione illustra i seguenti metodi utilizzati per costituire la base della struttura dell'applicazione:

- Utilizzo delle pile AWS CloudFormation
- Usando AWS Resource Groups
- Utilizzo AppRegistry delle applicazioni
- Utilizzo dei file di stato Terraform
- Utilizzando un'applicazione esistente AWS Resilience Hub

Utilizzo delle AWS CloudFormation pile

Scegli gli AWS CloudFormation stack che contengono le risorse che desideri utilizzare nell'applicazione che stai descrivendo. Gli stack possono provenire da Account AWS quelli utilizzati per descrivere l'applicazione oppure possono provenire da account o regioni diverse.

Per scoprire le risorse che costituiscono la base della struttura dell'applicazione

1. Seleziona CloudFormation gli stack per scoprire le tue risorse basate sullo stack.
2. Scegli le pile dall'elenco a discesa Seleziona le pile associate alla tua regione e alla tua regione. Account AWS

   Per utilizzare stack che si trovano in una regione diversa Account AWS, diversa o entrambe, inserisci il nome Amazon Resource Name (ARN) dello stack nella casella Aggiungi stack al di fuori della AWS regione, quindi scegli Aggiungi stack. ARN Per ulteriori informazioni in meritoARNs, consulta Amazon Resource Names (ARNs) nella AWS Guida generale.

Usando AWS Resource Groups

Scegli quella AWS Resource Groups che contiene le risorse che desideri utilizzare nell'applicazione che stai descrivendo.

Per scoprire le risorse che costituiscono la base della struttura della tua applicazione

1. Seleziona Gruppi di risorse per scoprire AWS Resource Groups quelli che contengono le risorse.
2. Scegli le risorse dall'elenco a discesa Seleziona gruppi di risorse.

Per utilizzarli AWS Resource Groups in una regione diversa Account AWS, diversa o in entrambe, inserisci il nome Amazon Resource Name (ARN) dello stack nella ARN casella Gruppo di risorse, quindi scegli Aggiungi gruppo ARN di risorse. Per ulteriori informazioni in meritoARNs, consulta Amazon Resource Names (ARNs) nella AWS Guida generale.

Utilizzo AppRegistry delle applicazioni

È possibile aggiungere una sola AppRegistry applicazione alla volta.

Scegli le AppRegistry applicazioni che contengono le risorse che desideri utilizzare nell'applicazione che stai descrivendo.

Per scoprire le risorse che costituiscono la base della struttura della tua applicazione

1. Seleziona AppRegistryper selezionare da un elenco di applicazioni create in AppRegistry.
2. Scegli le applicazioni, che sono state create in AppRegistry, dall'elenco a discesa Seleziona applicazione. Puoi scegliere solo un'applicazione alla volta.

Utilizzo dei file di stato Terraform

Scegli il file di stato Terraform che contiene le risorse del bucket S3 che desideri utilizzare nell'applicazione che stai descrivendo. Puoi accedere alla posizione del tuo file di stato Terraform o fornire un collegamento a un file di stato Terraform a cui hai accesso che si trova in una regione diversa.

> **Note**
>
> AWS Resilience Hub supporta la versione `0.12` del file di stato Terraform e successive.

Per scoprire le risorse che costituiscono la base della struttura della tua applicazione

1. Seleziona i file di stato Terraform per scoprire le risorse del tuo bucket S3.
2. Dalla sezione Seleziona i file di stato, scegli Browse S3 per accedere alla posizione del tuo file di stato Terraform.

   Per utilizzare i file di stato Terraform situati in una regione diversa, fornisci il link alla posizione del file di stato Terraform nel URL campo S3 e scegli Aggiungi S3. URL

Il limite per i file di stato Terraform è di 4 megabyte (MB).

3. Seleziona il tuo bucket S3 dalla sezione Bucket.
4. Dalla sezione Oggetti, seleziona una chiave e scegli Scegli.

Utilizzando un' AWS Resilience Hub applicazione esistente

Per iniziare, usa un'applicazione esistente.

Per scoprire le risorse che costituiscono la base della struttura della tua applicazione

1. Seleziona Applicazione esistente per creare l'applicazione da un'applicazione esistente.
2. Seleziona un'applicazione dall'elenco a discesa Seleziona applicazione esistente.

Aggiungi cluster EKS

Questa sezione illustra l'utilizzo dei EKS cluster Amazon per costituire la base della struttura dell'applicazione.

> **Note**
>
> È necessario disporre EKS delle autorizzazioni Amazon e di IAM ruoli aggiuntivi per connettersi al EKS cluster Amazon. Per ulteriori informazioni sull'aggiunta di EKS autorizzazioni Amazon per account singolo e multiaccount e IAM ruoli aggiuntivi per la connessione al cluster, consulta i seguenti argomenti:
>
> - AWS Resilience Hub riferimento alle autorizzazioni di accesso
> - the section called “Abilitare AWS Resilience Hub l'accesso al tuo EKS cluster Amazon”

Scegli EKS i cluster e i namespace Amazon che contengono le risorse che desideri utilizzare nell'applicazione che stai descrivendo. EKSI cluster Amazon possono provenire da Account AWS quello che stai utilizzando per descrivere l'applicazione oppure possono provenire da account diversi o regioni diverse.

> **Note**
>
> AWS Resilience Hub Per valutare i tuoi EKS cluster Amazon, devi aggiungere manualmente i namespace pertinenti a ciascuno dei EKS cluster Amazon nella EKS sezione cluster e namespaces. Il nome dello spazio dei nomi deve corrispondere esattamente al nome dello spazio dei nomi sui cluster Amazon. EKS

Per aggiungere EKS cluster Amazon

1. Scegli EKS i cluster Amazon dall'elenco a discesa Scegli EKS i cluster associati alla tua Account AWS regione.
2. Per utilizzare EKS cluster Amazon che si trovano in una regione diversa Account AWS, diversa o in entrambe, inserisci l'Amazon Resource Name (ARN) dello stack nella casella Cross account or Region, quindi scegli Aggiungi. EKS ARN Per ulteriori informazioni in meritoARNs, consulta Amazon Resource Names (ARNs) nella AWS Guida generale.

   Per ulteriori informazioni sull'aggiunta di autorizzazioni per accedere a cluster Amazon Elastic Kubernetes Service interregionali, consulta. the section called “Abilitare AWS Resilience Hub l'accesso al tuo EKS cluster Amazon”

Per aggiungere namespace dai cluster Amazon selezionati EKS

1. Nella sezione Aggiungi namespace, dalla tabella EKScluster e namespace, seleziona il pulsante di opzione situato a sinistra del nome del EKS cluster Amazon, quindi scegli Aggiorna namespace.

   Puoi identificare i EKS cluster Amazon in base a quanto segue:

   - EKSnome del cluster: indica il nome dei EKS cluster Amazon selezionati.
   - Numero di namespace: indica il numero di namespace selezionati nei cluster Amazon. EKS
   - Stato: indica se AWS Resilience Hub ha incluso i namespace dei EKS cluster Amazon selezionati nella tua applicazione. Puoi identificare lo stato utilizzando le seguenti opzioni:
     - Namespace obbligatorio: indica che non hai incluso alcun namespace dal cluster Amazon. EKS
     - Namespace aggiunti: indica che hai incluso uno o più namespace dal cluster Amazon. EKS

2. Per aggiungere un namespace, nella finestra di dialogo Aggiorna namespaces, scegli Aggiungi un nuovo spazio dei nomi.

   La finestra di dialogo Aggiorna namespaces mostra tutti i namespace che hai selezionato dal tuo EKS cluster Amazon, come opzione modificabile.

3. Nella finestra di dialogo Aggiorna namespaces, sono disponibili le seguenti opzioni di modifica:

   - Per aggiungere un nuovo spazio dei nomi, scegliete Aggiungi un nuovo spazio dei nomi, quindi immettete il nome dello spazio dei nomi nella casella dello spazio dei nomi.

     Il nome dello spazio dei nomi deve corrispondere esattamente al nome dello spazio dei nomi sul tuo cluster Amazon. EKS
   - Per rimuovere uno spazio dei nomi, scegli Rimuovi situato accanto allo spazio dei nomi.
   - Per applicare i namespace selezionati a tutti i EKS cluster Amazon, scegli Applica namespace a tutti i cluster. EKS

     Se scegli questa opzione, la tua selezione di namespace precedente negli EKS altri cluster Amazon verrà sostituita dalla selezione attuale dello spazio dei nomi.

4. Per includere i namespace aggiornati nella tua applicazione, scegli Aggiorna.

Next

Fase 4: Impostare e RTO RPO

Fase 4: Impostare e RTO RPO

È possibile definire una nuova politica di resilienza con i propriRTO/RPOtarget oppure scegliere una politica di resilienza esistente con obiettivi/predefinitiRTO. RPO Se desideri utilizzare una delle politiche di resilienza esistenti, seleziona Scegli un'opzione di politica esistente e seleziona un'applicazione di destinazione esistente dall'elenco a discesa della voce Opzione.

Per definire i tuoi/obiettivi RTO RPO

1. Seleziona l'opzione Crea una nuova politica di resilienza.
2. Inserisci un nome per la politica di resilienza.
3. (Facoltativo) Inserisci una descrizione per la politica di resilienza.
4. Definisci il tuoRTO/RPOnella sezione RTO/RPOtargets.

> **Note**
>
> - Abbiamo compilato un file predefinito RPO per RTO la tua applicazione. Puoi modificare l'RTOe RPO ora o dopo aver valutato l'applicazione.
> - AWS Resilience Hub consente di inserire un valore zero nei RPOcampi RTOe della politica di resilienza. Tuttavia, durante la valutazione della domanda, il risultato di valutazione più basso possibile è vicino allo zero. Pertanto, se inserisci un valore zero nei RPOcampi RTOand, il carico di lavoro stimato RTO e i RPO risultati del carico di lavoro stimato saranno vicini allo zero e lo stato di conformità dell'applicazione verrà impostato su Policy violata.

5. Per definireRTO/RPOper la tua infrastruttura e AZ, scegli la freccia destra per espandere la sezione Infrastruttura RTO e. RPO
6. In RTO/RPOtargets, inserisci un valore numerico nella casella, quindi scegli l'unità di tempo che il valore rappresenta per entrambi RTOe RPO.

   Ripeti queste voci per Infrastruttura e zona di disponibilità nella RPO sezione Infrastruttura RTO e.
7. (Facoltativo) Se disponi di un'applicazione multiregionale e desideri definire una regione RTORPO, attiva Regione - Facoltativo.

   In RTOe RPO, inserisci un valore numerico nella casella, quindi scegli l'unità di tempo che il valore rappresenta per entrambi RTOe. RPO

Next

the section called “Fase 5: Impostazione della valutazione programmata e della notifica di deviazione”

Fase 5: Imposta le valutazioni programmate e la notifica delle deviazioni

AWS Resilience Hub consente di impostare valutazioni pianificate e notifiche di deviazione per valutare l'applicazione ogni giorno e ricevere notifiche quando viene rilevata una deriva.

Per impostare la notifica di deriva

1. Per valutare la tua applicazione ogni giorno, attiva Valuta automaticamente ogni giorno.

Se questa opzione è attivata, il programma di valutazione giornaliero inizia solo dopo quanto segue:

- L'applicazione viene valutata manualmente con successo per la prima volta.
- L'applicazione è configurata con un IAM ruolo appropriato.
- Se l'applicazione è configurata con le autorizzazioni IAM utente correnti, è necessario creare il `AWSResilienceHubAsssessmentExecutionPolicy`

  ruolo utilizzando la procedura appropriata inthe section called “Come funziona AWS Resilience Hub con IAM”.

2. Per ricevere una notifica quando AWS Resilience Hub rileva eventuali deviazioni dalle politiche di resilienza o quando le relative risorse si sono spostate, attiva Ricevi una notifica quando l'applicazione si discosta.

   Se questa opzione è attivata, per ricevere notifiche di deviazione, devi specificare un argomento di Amazon Simple Notification Service (AmazonSNS). Per fornire un SNS argomento Amazon, nella sezione Fornisci un SNS argomento, seleziona l'opzione Scegli un SNS argomento e seleziona un SNS argomento Amazon dall'elenco a discesa Scegli un SNS argomento.

   > **Note**
   >
   > - AWS Resilience Hub Per consentire la pubblicazione di notifiche sui tuoi SNS argomenti Amazon, l'SNSargomento Amazon deve essere configurato con le autorizzazioni appropriate. Per ulteriori informazioni sulla configurazione delle autorizzazioni, consulta. the section called “Attivazione AWS Resilience Hub della pubblicazione sui tuoi SNS argomenti Amazon”
   > - Le valutazioni giornaliere possono avere un impatto sulla quota di esecuzioni. Per ulteriori informazioni sulle quote, consulta AWS Resilience Hub endpoint e quote nella Guida generale.AWS

   Per utilizzare SNS argomenti Amazon che si trovano in una regione diversa Account AWS o diversa, o entrambi, seleziona Inserisci SNS argomento ARN e inserisci il nome della risorsa Amazon (ARN) dell'SNSargomento Amazon nella casella Fornisci un SNS argomento. Per ulteriori informazioni in meritoARNs, consulta Amazon Resource Names (ARNs) nella AWS Guida generale.

Next

Fase 6: Configurazione delle autorizzazioni

Fase 6: Configurazione delle autorizzazioni

AWS Resilience Hub consente di configurare le autorizzazioni necessarie per l'account primario e l'account secondario per scoprire e valutare le risorse. Tuttavia, è necessario eseguire la procedura separatamente per configurare le autorizzazioni per ogni account.

Per configurare IAM ruoli e IAM autorizzazioni

1. Per selezionare un IAM ruolo esistente che verrà utilizzato per accedere alle risorse nell'account corrente, seleziona un IAM ruolo dall'elenco a discesa Seleziona un IAM ruolo.

   > **Note**
   >
   > Per una configurazione su più account, se non specifichi Amazon Resource Names (ARNs) del IAM ruolo nella ARN casella Inserisci un IAM ruolo, AWS Resilience Hub utilizzerà il IAM ruolo che hai selezionato dall'elenco a discesa Seleziona un IAM ruolo per tutti gli account.

   Se non ci sono IAM ruoli esistenti collegati al tuo account, puoi creare un IAM ruolo utilizzando una delle seguenti opzioni:

   - AWS IAMconsole: se scegli questa opzione, devi completare la procedura in Per creare il ruolo dell'hub AWS Resilience nella IAM console.
   - AWS CLI— Se scegli questa opzione, devi completare tutti i passaggi indicati in AWS CLI.
   - CloudFormation modello: se scegli questa opzione, a seconda del tipo di account (account principale o account secondario), devi creare i ruoli utilizzando il AWS CloudFormation modello appropriato.
2. Scegli la freccia destra per espandere la sezione Aggiungi IAM ruolo/i da un account incrociato - Facoltativo.
3. Per selezionare IAM i ruoli da un account incrociato, inserisci il ARNs IAM ruolo nella ARN casella Inserisci un IAM ruolo. Assicurati che ARNs i IAM ruoli che stai inserendo non appartengano all'account corrente.

4. Se desideri utilizzare l'IAMutente corrente per scoprire le risorse dell'applicazione, scegli la freccia destra per espandere Usa la sezione Usa le autorizzazioni IAM dell'utente corrente e seleziona Capisco che devo configurare manualmente le autorizzazioni per abilitare la funzionalità richiesta all'interno. AWS Resilience Hub

   Se selezionate questa opzione, alcune AWS Resilience Hub funzionalità (come la notifica di deviazione) potrebbero non funzionare come previsto e gli input forniti nei passaggi 1 e 3 verranno ignorati.

Next

Fase 7: Configurazione dei parametri di configurazione dell'applicazione

Fase 7: Configurazione dei parametri di configurazione dell'applicazione

Questa sezione consente di fornire i dettagli del supporto per il failover tra regioni utilizzando. AWS Elastic Disaster Recovery AWS Resilience Hub utilizzerà queste informazioni per fornire raccomandazioni sulla resilienza.

Per ulteriori informazioni sui parametri di configurazione dell'applicazione, vedereParametri di configurazione dell'applicazione.

Per aggiungere parametri di configurazione dell'applicazione (facoltativo)

1. Per espandere la sezione Parametri di configurazione dell'applicazione, fate clic sulla freccia destra.
2. Immettete l'ID dell'account di failover nella casella Account ID. Per impostazione predefinita, abbiamo precompilato questo campo con l'ID dell'account per cui viene utilizzato AWS Resilience Hub, che può essere modificato.
3. Seleziona una regione di failover dall'elenco a discesa Regione.

> **Note**
>
> Se desideri disabilitare questa funzionalità, seleziona "—" dall'elenco a discesa.

Next

Passaggio 8: Aggiungere tag

Passaggio 8: Aggiungere tag

Assegna un tag o un'etichetta a una AWS risorsa per cercare e filtrare le risorse o tenere traccia AWS dei costi.

(Facoltativo) Per aggiungere tag alla tua applicazione, scegli Aggiungi nuovo tag se desideri associare uno o più tag all'applicazione. Per ulteriori informazioni sui tag, consulta Etichettatura delle risorse nella Guida AWS generale.

Scegli Aggiungi applicazione per creare la tua applicazione.

Next

Passaggio 9: Rivedi e pubblica la tua AWS Resilience Hub applicazione

Passaggio 9: Rivedi e pubblica la tua AWS Resilience Hub applicazione

Dopo la pubblicazione, puoi comunque rivedere l'applicazione e modificarne le risorse. Al termine, scegliete Pubblica per pubblicare l'applicazione.

Per ulteriori informazioni sulla revisione dell'applicazione e sulla modifica delle relative risorse, consultate quanto segue:

- the section called “Visualizzazione del riepilogo dell'applicazione”
- the section called “Modifica delle risorse delle applicazioni”

Next

Fase 10: Eseguite una valutazione dell' AWS Resilience Hub applicazione

Fase 10: Eseguite una valutazione dell' AWS Resilience Hub applicazione

L'applicazione che hai pubblicato è elencata nella pagina di riepilogo.

Dopo aver pubblicato l' AWS Resilience Hub applicazione, si viene reindirizzati alla pagina di riepilogo dell'applicazione in cui è possibile eseguire una valutazione della resilienza. La valutazione valuta la configurazione dell'applicazione rispetto alla politica di resilienza allegata all'applicazione. Viene generato un rapporto di valutazione che mostra in che modo l'applicazione si colloca rispetto agli obiettivi della politica di resilienza.

Per eseguire una valutazione della resilienza

1. Nella pagina di riepilogo delle applicazioni, scegli Valuta la resilienza.
2. Nella finestra di dialogo Esegui valutazione della resilienza, inserisci un nome univoco per il rapporto o utilizza il nome generato nella casella Nome rapporto.
3. Seleziona Esegui.
4. Dopo aver ricevuto la notifica che il rapporto di valutazione è stato generato, scegli la scheda Valutazioni e la valutazione per visualizzare il rapporto.
5. Scegli la scheda Revisione per visualizzare il rapporto di valutazione della tua candidatura.

Usando AWS Resilience Hub

AWS Resilience Hub aiuta a migliorare la resilienza delle applicazioni AWS e a ridurre i tempi di ripristino in caso di interruzioni delle applicazioni.

Argomenti:

AWS Resilience Hub cruscotto

La dashboard offre una visione completa dello stato di resilienza del portafoglio di applicazioni. La dashboard aggrega e organizza eventi di resilienza (ad esempio, database non disponibile o convalida della resilienza non riuscita), avvisi e approfondimenti provenienti da servizi come CloudWatch Amazon Fault Injection Service ().AWS FIS

La dashboard genera anche un punteggio di resilienza per ogni applicazione valutata. Questo punteggio indica le prestazioni dell'applicazione rispetto alle politiche di resilienza, agli allarmi, alle procedure operative standard di ripristino (SOP) e ai test consigliati. È possibile utilizzare questo punteggio per misurare i miglioramenti della resilienza nel tempo.

Per visualizzare la AWS Resilience Hub dashboard, scegli Dashboard dal menu di navigazione. La pagina Dashboard mostra le seguenti sezioni:

Stato della domanda

Gli stati delle applicazioni indicano se le applicazioni sono state valutate per verificarne la conformità alla politica di resilienza allegata o meno. Inoltre, una volta completata una valutazione, lo stato indica

anche se le fonti di input delle applicazioni sono state modificate o meno. Scegli un numero sotto ciascuno dei seguenti stati per visualizzare tutte le candidature che condividono lo stesso stato nella pagina Applicazioni:

- Applicazioni incluse nella policy: indica tutte le applicazioni conformi alla policy di resilienza allegata.
- Policy di violazione delle applicazioni: indica tutte le applicazioni che non sono conformi alla politica di resilienza allegata.
- Applicazioni non valutate: indica tutte le applicazioni la cui conformità non è stata ancora valutata o monitorata.
- Applicazioni deviate: indica tutte le applicazioni che si sono allontanate dalla politica di resilienza o se le relative risorse si sono discostate.

Punteggio di resilienza delle applicazioni nel tempo

Con il punteggio di resilienza dell'applicazione nel tempo, puoi visualizzare un grafico della resilienza dell'applicazione negli ultimi 30 giorni. Sebbene il menu a discesa possa elencare 10 delle tue applicazioni, mostra AWS Resilience Hub solo un grafico con un massimo di quattro applicazioni alla volta. Per ulteriori informazioni sul punteggio di resilienza, vedere. Comprendere i punteggi di resilienza

> **Note**
>
> AWS Resilience Hub non esegue valutazioni pianificate contemporaneamente. Di conseguenza, potrebbe essere necessario tornare al grafico del punteggio di resilienza nel tempo in un secondo momento per visualizzare la valutazione giornaliera delle applicazioni.

AWS Resilience Hub utilizza anche Amazon CloudWatch per generare questi grafici. Scegli Visualizza metriche CloudWatch per creare e visualizzare informazioni più granulari sulla resilienza dell'applicazione nella dashboard. CloudWatch Per ulteriori informazioni CloudWatch, consulta Using dashboards nella Amazon CloudWatch User Guide.

Allarmi implementati

Questa sezione elenca tutti gli allarmi che hai configurato in Amazon CloudWatch per monitorare tutte le applicazioni. Per ulteriori informazioni, consulta la sezione Visualizzazione degli allarmi.

Esperimenti implementati

Questa sezione elenca tutti gli esperimenti di iniezione dei guasti implementati in tutte le applicazioni. Per ulteriori informazioni, consulta Visualizzazione degli esperimenti di iniezione dei guasti.

Descrizione e gestione delle applicazioni AWS Resilience Hub

Un' AWS Resilience Hub applicazione è una raccolta di AWS risorse strutturate per prevenire e ripristinare le interruzioni delle AWS applicazioni.

Per descrivere un' AWS Resilience Hub applicazione, è necessario fornire un nome di applicazione, risorse da uno o più AWS CloudFormation stack e una politica di resilienza appropriata. È inoltre possibile utilizzare qualsiasi AWS Resilience Hub applicazione esistente come modello per descrivere l'applicazione.

Dopo aver descritto un' AWS Resilience Hub applicazione, è necessario pubblicarla in modo da poter eseguire una valutazione della resilienza su di essa. È quindi possibile utilizzare i consigli della valutazione per migliorare la resilienza eseguendo un'altra valutazione, confrontando i risultati e quindi ripetendo il processo fino a quando il carico di lavoro stimato e il carico di lavoro stimato non soddisfano gli obiettivi RTO prefissati. RPO RTO RPO

Per visualizzare la pagina Applicazioni, scegli Applicazioni dal pannello di navigazione. È possibile identificare le applicazioni nella pagina Applicazioni in base a quanto segue:

- Nome: il nome dell'applicazione che hai fornito durante la definizione AWS Resilience Hub.
- Descrizione: la descrizione dell'applicazione fornita durante la definizione AWS Resilience Hub.
- Stato di conformità: AWS Resilience Hub imposta lo stato dell'applicazione su Valutata, Non valutata, Politica violata o Rilevata modifiche.
  - Valutata: AWS Resilience Hub ha esaminato la tua richiesta.
  - Non valutata: non AWS Resilience Hub ha valutato la tua candidatura.
  - Policy violata: AWS Resilience Hub ha stabilito che l'applicazione non ha soddisfatto gli obiettivi della politica di resilienza per Recovery Time Objective (RTO) e Recovery Point Objective (). RPO Esamina e utilizza i consigli forniti da AWS Resilience Hub prima di rivalutare la tua applicazione per quanto riguarda la resilienza. Per ulteriori informazioni sui consigli, consulta. Aggiungere un'applicazione a AWS Resilience Hub

  - Modifiche rilevate: AWS Resilience Hub ha rilevato le modifiche apportate alla politica di resilienza associata all'applicazione. È necessario rivalutare l'applicazione AWS Resilience Hub per determinare se soddisfa gli obiettivi della politica di resilienza.
- Valutazioni pianificate: il tipo di risorsa identifica la risorsa componente per l'applicazione. Per ulteriori informazioni sulle valutazioni pianificate, consulta. Resilienza delle applicazioni
  - Attivo: indica che la tua candidatura viene valutata automaticamente ogni giorno da. AWS Resilience Hub
  - Disabilitato: indica che la domanda non viene valutata automaticamente ogni giorno da AWS Resilience Hub e che è necessario valutare manualmente la domanda.
- Stato di deviazione: indica se la domanda si è allontanata o meno dalla valutazione precedente con esito positivo e imposta uno dei seguenti stati:
  - Drifted: indica che l'applicazione, che era conforme alla politica di resilienza nella precedente valutazione positiva, ha ora violato la politica di resilienza e l'applicazione è a rischio. Inoltre, indica anche se le risorse all'interno delle fonti di input, incluse nella versione corrente dell'applicazione, sono state aggiunte o rimosse.
  - Not drifted: indica che si stima che l'applicazione soddisfi ancora RTO gli RPO obiettivi definiti nella policy. Inoltre, indica anche che le risorse all'interno delle sorgenti di input, incluse nella versione corrente dell'applicazione, non sono state aggiunte o rimosse.
- Carico di lavoro stimatoRTO: indica il carico di lavoro stimato massimo possibile RTO dell'applicazione. Questo valore è il carico di lavoro massimo stimato per tutti i tipi RTO di interruzione in base all'ultima valutazione riuscita.
- Carico di lavoro stimatoRPO: indica il carico di lavoro RPO stimato massimo possibile dell'applicazione. Questo valore è il carico di lavoro massimo stimato per tutti i tipi RTO di interruzione in base all'ultima valutazione riuscita.
- Ora dell'ultima valutazione: indica la data e l'ora in cui la domanda è stata valutata con successo l'ultima volta.
- Ora di creazione: data e ora di creazione dell'applicazione.
- ARN— L'Amazon Resource Name (ARN) della tua applicazione. Per ulteriori informazioni in meritoARNs, consulta Amazon Resource Names (ARNs) nella AWS Guida generale.

> **Note**
>
> AWS Resilience Hub è in grado di valutare appieno la resilienza delle ECS risorse Amazon interregionali solo se utilizzi Amazon ECR per l'archivio di immagini.

Inoltre, puoi anche filtrare l'elenco delle applicazioni utilizzando una delle seguenti opzioni nella pagina Applicazioni:

- Trova applicazioni: inserisci il nome dell'applicazione per filtrare i risultati in base al nome dell'applicazione.
- Filtra l'ora dell'ultima valutazione per una data e un intervallo di tempo: per applicare questo filtro, scegli l'icona del calendario e seleziona una delle seguenti opzioni per filtrare in base ai risultati che corrispondono all'intervallo di tempo:
  - Intervallo relativo: seleziona una delle opzioni disponibili e scegli Applica.

    Se scegli l'opzione Intervallo personalizzato, inserisci una durata nella casella Inserisci durata e seleziona l'unità di tempo appropriata dall'elenco a discesa Unità di tempo, quindi scegli Applica.
  - Intervallo assoluto: per specificare l'intervallo di data e ora, fornisci l'ora di inizio e l'ora di fine, quindi scegli Applica.

Negli argomenti seguenti vengono illustrati i diversi approcci per descrivere un' AWS Resilience Hub applicazione e come gestirli.

Argomenti

Visualizzazione del riepilogo di un' AWS Resilience Hub applicazione

La pagina di riepilogo dell'applicazione nella AWS Resilience Hub console fornisce una panoramica delle informazioni sull'applicazione e sullo stato della resilienza.

Per visualizzare un riepilogo dell'applicazione

1. Scegli Applicazioni dal pannello di navigazione.
2. Nella pagina Applicazioni, scegli il nome dell'applicazione che desideri visualizzare.

La pagina di riepilogo delle applicazioni contiene le seguenti sezioni.

Argomenti

Riepilogo della valutazione

Questa sezione fornisce un riepilogo dell'ultima valutazione riuscita ed evidenzia i consigli critici come approfondimenti attuabili. AWS Resilience Hub utilizza le funzionalità di intelligenza artificiale generativa di Amazon Bedrock per aiutare a concentrare gli utenti sui consigli di resilienza più importanti forniti da. AWS Resilience Hub Concentrandoti sugli elementi critici, puoi concentrarti sui consigli più importanti che migliorano la resilienza della tua applicazione. Scegli un consiglio per visualizzarne il riepilogo e scegli Visualizza dettagli per visualizzare ulteriori dettagli sui consigli nella sezione pertinente del rapporto di valutazione. Per ulteriori informazioni sulla revisione del rapporto di valutazione, consultathe section called “Revisione dei rapporti di valutazione”.

> **Note**
>
> - Questo riepilogo della valutazione è disponibile solo nella regione Stati Uniti orientali (Virginia settentrionale).
> - Il riepilogo della valutazione generato da modelli linguistici di grandi dimensioni (LLMs) su Amazon Bedrock sono solo suggerimenti. L'attuale livello di tecnologia di intelligenza

artificiale generativa non è perfetto e non è LLMs infallibile. Ci si dovrebbe aspettare parzialità e risposte errate, anche se rare. Esamina ogni consiglio nel riepilogo della valutazione prima di utilizzare l'output di unLLM.

Riepilogo

Questa sezione fornisce un riepilogo dell'applicazione selezionata nelle seguenti sezioni:

- Informazioni sull'applicazione: questa sezione fornisce le seguenti informazioni sull'applicazione selezionata:
  - Stato dell'applicazione: indica lo stato dell'applicazione.
  - Descrizione: la descrizione dell'applicazione.
  - Versione: indica la versione attualmente valutata dell'applicazione.
  - Politica di resilienza: indica la politica di resilienza allegata all'applicazione. Per ulteriori informazioni sulle politiche di resilienza, vedere. Gestione delle politiche di resilienza
- Derive delle applicazioni: questa sezione evidenzia le deviazioni rilevate durante l'esecuzione di una valutazione per l'applicazione selezionata per verificare se è conforme alla relativa politica di resilienza. Inoltre, controlla anche se alcune risorse sono state aggiunte o rimosse dall'ultima volta che è stata pubblicata la versione dell'applicazione. Questa sezione mostra le seguenti informazioni:
  - Modifiche delle politiche: scegliete il numero seguente per visualizzare tutti i componenti dell'applicazione che erano conformi alla politica nella valutazione precedente ma che non erano conformi nella valutazione corrente.
  - Variazioni delle risorse: scegliete il numero seguente per visualizzare tutte le risorse modificate nell'ultima valutazione.

Resilienza delle applicazioni

Le metriche mostrate nella sezione relativa al punteggio di resilienza provengono dalla valutazione di resilienza più recente dell'applicazione.

Punteggio di resilienza

Il punteggio di resilienza ti aiuta a quantificare la tua preparazione a gestire una potenziale interruzione. Questo punteggio riflette la precisione con cui l'applicazione ha seguito AWS Resilience

Hub le raccomandazioni per soddisfare la politica di resilienza, gli allarmi, le procedure operative standard () e i test dell'applicazione. SOPs

Il punteggio di resilienza massimo che l'applicazione può raggiungere è del 100%. Il punteggio rappresenta tutti i test consigliati eseguiti in un periodo di tempo predefinito. Indica che i test stanno avviando l'allarme corretto e che l'allarme avvia quello corretto. SOP

Ad esempio, supponiamo che ciò AWS Resilience Hub raccomandi un test con un allarme e uno. SOP Quando il test viene eseguito, l'allarme avvia quello associato e SOP quindi viene eseguito correttamente. Per ulteriori informazioni sul punteggio di resilienza, vedere. Comprendere i punteggi di resilienza

Allarmi implementati

La sezione Allarmi implementati di riepilogo dell'applicazione elenca gli allarmi che configuri in Amazon CloudWatch per monitorare l'applicazione. Per ulteriori informazioni sugli allarmi, consulta. Gestione degli allarmi

Esperimenti implementati

La sezione Esperimenti di iniezione di errori di riepilogo dell'applicazione mostra un elenco degli esperimenti di iniezione dei guasti. Per ulteriori informazioni sugli esperimenti di iniezione dei guasti, vedereGestione degli esperimenti di Amazon Fault Injection Service.

Modifica delle risorse delle AWS Resilience Hub applicazioni

Per ricevere valutazioni di resilienza accurate e utili, assicuratevi che la descrizione dell'applicazione sia aggiornata e corrisponda all' AWS applicazione e alle risorse effettive. I rapporti di valutazione, la convalida e i consigli si basano sulle risorse elencate. Se aggiungi o rimuovi risorse da un' AWS applicazione, dovresti inserire tali modifiche in AWS Resilience Hub.

AWS Resilience Hub fornisce trasparenza sui sorgenti delle applicazioni. È possibile identificare e modificare le risorse e le fonti dell'applicazione nell'applicazione.

> **Note**
>
> La modifica delle risorse modifica solo il AWS Resilience Hub riferimento dell'applicazione. Non viene apportata alcuna modifica alle risorse effettive.

Puoi aggiungere risorse mancanti, modificare risorse esistenti o rimuovere risorse che non ti servono. Le risorse sono raggruppate in componenti logici dell'applicazione (AppComponents). È possibile modificarli AppComponents per rispecchiare meglio la struttura dell'applicazione.

Aggiungete o aggiornate le risorse dell'applicazione modificando una bozza dell'applicazione e pubblicando le modifiche in una nuova versione (release). AWS Resilience Hub utilizza la versione di rilascio (che include le risorse aggiornate) dell'applicazione per eseguire le valutazioni della resilienza.

Per valutare la resilienza dell'applicazione

1. Nel riquadro di navigazione, scegliere Applications (Applicazioni).
2. Nella pagina Applicazioni, scegli il nome dell'applicazione che desideri modificare.
3. Dal menu Azioni, scegli Valuta la resilienza.
4. Nella finestra di dialogo Esegui valutazione della resilienza, inserisci un nome univoco per il rapporto o utilizza il nome generato nella casella Nome rapporto.
5. Seleziona Esegui.
6. Dopo aver ricevuto la notifica che il rapporto di valutazione è stato generato, scegli la scheda Valutazioni e la valutazione per visualizzare il rapporto.
7. Scegli la scheda Revisione per visualizzare il rapporto di valutazione della tua candidatura.

Per abilitare la valutazione pianificata

1. Nel riquadro di navigazione, scegliere Applications (Applicazioni).
2. Nella pagina Applicazioni, seleziona l'applicazione per la quale desideri abilitare la valutazione pianificata.
3. Attiva Valuta automaticamente ogni giorno.

Per disabilitare la valutazione pianificata

1. Nel riquadro di navigazione, scegliere Applications (Applicazioni).
2. Nella pagina Applicazioni, seleziona l'applicazione per la quale desideri abilitare la valutazione pianificata.
3. Disattiva la valutazione automatica giornaliera.

> **Note**
>
> La disabilitazione della valutazione pianificata disattiverà la notifica di deviazione.

4. Scegli Disattiva.

Per abilitare la notifica di deviazione per la tua applicazione

1. Nel riquadro di navigazione, scegliere Applications (Applicazioni).
2. Nella pagina Applicazioni, seleziona l'applicazione per la quale desideri abilitare la notifica di deriva o modifica le impostazioni della notifica di deriva.
3. È possibile modificare la notifica di deriva scegliendo una delle seguenti opzioni:
   - Da Azioni, scegli Abilita notifica di deriva.
   - Scegli Abilita notifica nella sezione Application drifts.
4. Completa i passaggi indicatiFase 5: Imposta le valutazioni programmate e la notifica delle deviazioni, quindi torna a questa procedura.
5. Scegli Abilita .

   L'attivazione della notifica della deriva consentirà anche la valutazione pianificata.

Per modificare la notifica di deriva per la tua applicazione

> **Note**
>
> Questa procedura è applicabile se hai abilitato la valutazione pianificata (la funzione Valutazione automatica giornaliera è attivata) e la notifica di deviazione.

1. Nel riquadro di navigazione, scegliere Applications (Applicazioni).
2. Nella pagina Applicazioni, seleziona l'applicazione per la quale desideri abilitare la notifica di deriva o modifica le impostazioni della notifica di deriva.
3. È possibile modificare la notifica di deriva scegliendo una delle seguenti opzioni:
   - Da Azioni, scegli Modifica notifica di deriva.

- Scegli Modifica notifica nella sezione Application drifts.

4. Completa i passaggi indicatiFase 5: Imposta le valutazioni programmate e la notifica delle deviazioni, quindi torna a questa procedura.
5. Selezionare Salva.

Per aggiornare le autorizzazioni di sicurezza dell'applicazione

1. Nel riquadro di navigazione, scegliere Applications (Applicazioni).
2. Nella pagina Applicazioni, seleziona l'applicazione per la quale desideri aggiornare le autorizzazioni di sicurezza.
3. Da Azioni, scegli Aggiorna autorizzazioni.
4. Per aggiornare le autorizzazioni di sicurezza, completa i passaggi indicati inFase 6: Configurazione delle autorizzazioni, quindi torna a questa procedura.
5. Scegli Salva e aggiorna.

Per allegare una politica di resilienza alla tua applicazione

1. Nel riquadro di navigazione, scegliere Applications (Applicazioni).
2. Nella pagina Applicazioni, scegli il nome dell'applicazione che desideri modificare.
3. Dal menu Azioni, scegli Allega politica di resilienza.
4. Nella finestra di dialogo Allega politica, seleziona una politica di resilienza dall'elenco a discesa Seleziona una politica di resilienza.
5. Scegli Collega.

Per modificare le fonti di input, le risorse e l'applicazione AppComponents

1. Nel riquadro di navigazione, scegliere Applications (Applicazioni).
2. Nella pagina Applicazioni, scegli il nome dell'applicazione che desideri modificare.
3. Scegli la scheda Struttura dell'applicazione.
4. Scegli il segno più + prima di Version, quindi seleziona la versione dell'applicazione con lo stato Bozza.
5. Per modificare le fonti di input, le risorse e AppComponents l'applicazione, completate i passaggi indicati nelle seguenti procedure.

Per modificare le fonti di input dell'applicazione

1. Per modificare le sorgenti di input dell'applicazione, scegliete la scheda Fonti di input.

   La sezione Sorgenti di input elenca tutte le fonti di input delle risorse dell'applicazione. È possibile identificare le fonti di input in base a quanto segue:

   - Nome della sorgente: il nome della sorgente di ingresso. Scegliete il nome della sorgente per visualizzarne i dettagli nella rispettiva applicazione. Per le sorgenti di input aggiunte manualmente, il collegamento non sarà disponibile. Ad esempio, se scegli il nome della sorgente che viene importato da uno AWS CloudFormation stack, verrai reindirizzato alla pagina dei dettagli dello stack sulla console. AWS CloudFormation
   - ARN di origine: Amazon Resource Name (ARN) della sorgente di input. Scegliete un ARN per visualizzarne i dettagli nella rispettiva applicazione. Per le sorgenti di input aggiunte manualmente, il collegamento non sarà disponibile. Ad esempio, se scegli un ARN importato da uno AWS CloudFormation stack, verrai reindirizzato alla pagina dei dettagli dello stack sulla console. AWS CloudFormation
   - Tipo di sorgente: il tipo di sorgente di input. Le fonti di input includono cluster Amazon EKS, AWS CloudFormation stack, AppRegistry applicazioni AWS Resource Groups, file di stato Terraform e risorse aggiunte manualmente.
   - Risorse associate: il numero di risorse associate alla sorgente di input. Scegli un numero per visualizzare tutte le risorse associate a una fonte di input nella scheda Risorse.
2. Per aggiungere sorgenti di input all'applicazione, nella sezione Sorgenti di input, scegli Aggiungi fonti di input. Per ulteriori informazioni sull'aggiunta di sorgenti di input, consultathe section called “Fase 3: Aggiungere risorse all' AWS Resilience Hub applicazione”.
3. Per modificare le sorgenti di input, selezionate le sorgenti di input e scegliete una delle seguenti opzioni da Azioni:

   - Reimporta le sorgenti di input (fino a 5): reimporta fino a cinque sorgenti di input selezionate.
   - Elimina sorgenti di input: elimina le sorgenti di input selezionate.

     Per pubblicare un'applicazione, deve contenere almeno una fonte di input. Se elimini tutte le fonti di input, Pubblica nuova versione verrà disattivata.

Per modificare le risorse della tua applicazione

1. Per modificare le risorse dell'applicazione, scegli la scheda Risorse.

> **Note**
>
> Per visualizzare l'elenco delle risorse non valutate, scegli Visualizza risorse non valutate.

La sezione Risorse elenca le risorse dell'applicazione che hai scelto di utilizzare come modello per la descrizione dell'applicazione. Per migliorare l'esperienza di ricerca, AWS Resilience Hub ha raggruppato le risorse in base a più criteri di ricerca. Questi criteri di ricerca includono AppComponent tipi, risorse non supportate e risorse escluse. Per filtrare le risorse in base a un criterio di ricerca nella tabella Risorse, scegliete il numero sotto ogni criterio di ricerca.

È possibile identificare le risorse in base a quanto segue:

- ID logico: un ID logico è un nome utilizzato per identificare le risorse nello AWS CloudFormation stack, nel file di stato Terraform, nell'applicazione aggiunta manualmente, nell' AppRegistry applicazione o. AWS Resource Groups

  > **Note**
  >
  > - Terraform ti consente di utilizzare lo stesso nome per diversi tipi di risorse. Pertanto, viene visualizzato "- tipo di risorsa" alla fine dell'ID logico per le risorse che condividono lo stesso nome.
  > - Per visualizzare le istanze di tutte le risorse dell'applicazione, scegliete il segno più (+) prima dell'ID logico. Per visualizzare tutte le istanze di una risorsa dell'applicazione, scegliete il segno più (+) prima dell'ID logico di ciascuna risorsa.
  >
  >   Per ulteriori informazioni sulle risorse supportate, vederethe section called “ AWS Resilience Hub risorse supportate”.

- Tipo di risorsa: il tipo di risorsa identifica la risorsa componente per l'applicazione. Ad esempio, `AWS::EC2::Instance` dichiara un'istanza Amazon EC2. Per ulteriori informazioni sul raggruppamento AppComponent delle risorse, consulta. Raggruppamento di risorse in un componente applicativo
- Nome sorgente: il nome della sorgente di input. Scegliete il nome della sorgente per visualizzarne i dettagli nella rispettiva applicazione. Per le sorgenti di input aggiunte manualmente, il collegamento non sarà disponibile. Ad esempio, se scegli il nome della fonte

che viene importato da uno AWS CloudFormation stack, verrai reindirizzato alla pagina dei dettagli dello stack sul. AWS CloudFormation

- Tipo di sorgente: il tipo di sorgente di input. Le fonti di input includono AWS CloudFormation pile, AppRegistry applicazioni AWS Resource Groups, file di stato Terraform e risorse aggiunte manualmente.

> **Note**
>
> Per modificare i cluster Amazon EKS, completa i passaggi in Modificare le fonti di input della procedura AWS Resilience Hub applicativa.

- Source stack: lo AWS CloudFormation stack che contiene la risorsa. Questa colonna dipende dal tipo di struttura dell'applicazione selezionata.
- ID fisico: l'identificatore effettivo assegnato a quella risorsa, ad esempio un ID di istanza Amazon EC2 o il nome di un bucket S3.
- Incluso: indica se queste risorse sono AWS Resilience Hub incluse nell'applicazione.
- Valutabile: indica se AWS Resilience Hub valuterà la resilienza della risorsa.
- AppComponents— Il AWS Resilience Hub componente assegnato a questa risorsa quando è stata scoperta la relativa struttura applicativa.
- Nome: nome della risorsa dell'applicazione.
- Account: l' AWS account proprietario della risorsa fisica.

2. Per trovare una risorsa che non è elencata, inserisci l'ID logico della risorsa nella casella di ricerca.
3. Per rimuovere una risorsa dall'applicazione, selezionate la risorsa, quindi scegliete Escludi risorsa dalle azioni.
4. Per risolvere le risorse dell'applicazione, scegli Aggiorna risorse.
5. Per modificare le risorse applicative esistenti, completa i seguenti passaggi:

   a. Seleziona una risorsa, quindi scegli Aggiorna pile da Azioni.

   b. Nella pagina Update stacks, per aggiornare le risorse, completate le procedure appropriate inFase 3: Aggiungere risorse all'applicazione AWS Resilience Hub, quindi tornate a questa procedura.

   c. Selezionare Salva.

6. Per aggiungere una risorsa all'applicazione, da Azioni, scegli Aggiungi risorsa e completa i seguenti passaggi:

    a. Seleziona un tipo di risorsa dall'elenco a discesa Tipo di risorsa.

    b. Seleziona un AppComponent dall'AppComponentelenco a discesa.

    c. Immettete l'ID logico della risorsa nella casella Nome risorsa.

    d. Immettere l'ID o il nome della risorsa fisica o l'ARN della risorsa nella casella Identificatore risorsa.

    e. Scegli Aggiungi.

7. Per modificare il nome della risorsa, seleziona una risorsa, scegli Modifica nome risorsa da Azioni, quindi completa i seguenti passaggi:

    a. Immettete l'ID logico della risorsa nella casella Nome risorsa.

    b. Selezionare Salva.

8. Per modificare l'identificatore della risorsa, selezionate una risorsa, scegliete Modifica identificatore di risorsa da Azioni, quindi completate i seguenti passaggi:

    a. Immettere l'ID o il nome della risorsa fisica o l'ARN della risorsa nella casella Identificatore risorsa.

    b. Selezionare Salva.

9. Per modificare il AppComponent, seleziona una risorsa, scegli Cambia AppComponent da Azioni e completa i seguenti passaggi:

    a. Seleziona una AppComponent dall'elenco a AppComponentdiscesa.

    b. Scegli Aggiungi.

10. Per eliminare una risorsa, selezionala, quindi scegli Elimina risorsa da Azioni.

11. Per includere una risorsa, selezionatela, quindi scegliete Includi risorsa dalle azioni.

Per modificare AppComponents la tua applicazione

1. Per modificare AppComponents la tua applicazione, scegli la AppComponentsscheda.

> **Note**
>
> Per ulteriori informazioni sul raggruppamento AppComponent delle risorse, consultaRaggruppamento di risorse in un componente applicativo.

La AppComponentssezione elenca tutti i componenti logici in cui sono raggruppate le risorse. È possibile identificarli in AppComponents base a quanto segue:

- AppComponent name: il nome del AWS Resilience Hub componente assegnato a questa risorsa quando è stata scoperta la relativa struttura applicativa.
- AppComponent type — Il tipo di AWS Resilience Hub componente.
- Nome sorgente: il nome della sorgente di input. Scegliete il nome della sorgente per visualizzarne i dettagli nella rispettiva applicazione. Ad esempio, se scegli il nome sorgente importato da uno AWS CloudFormation stack, verrai reindirizzato alla pagina dei dettagli dello stack sul. AWS CloudFormation
- Numero di risorse: il numero di risorse associate alla sorgente di input. Scegliete un numero per visualizzare tutte le risorse associate a una fonte di input nella scheda Risorse.

2. Per creare un AppComponent, dal menu Azioni, scegli Crea nuovo AppComponent e completa i seguenti passaggi:

   a. Inserisci un nome per la AppComponent nella casella del AppComponentnome. Per riferimento, abbiamo precompilato questo campo con un nome di esempio.
   b. Seleziona il tipo di AppComponent dall'elenco a discesa del AppComponenttipo.
   c. Selezionare Salva.

3. Per modificarne uno AppComponent, selezionalo AppComponent, quindi scegli Modifica AppComponent da Azioni.
4. Per eliminarne uno AppComponent, selezionatene uno AppComponent, quindi scegliete Elimina AppComponent da Azioni.

Dopo aver apportato modifiche all'elenco delle risorse, riceverai un avviso che indica che sono state apportate modifiche alla versione bozza dell'applicazione. Per eseguire una valutazione accurata della resilienza, è necessario pubblicare una nuova versione dell'applicazione. Per ulteriori informazioni su come pubblicare una nuova versione, consultaPubblicazione di una nuova versione AWS Resilience Hub dell'applicazione.

Gestione dei componenti dell'applicazione

Un componente applicativo (AppComponent) è un gruppo di AWS risorse correlate che funzionano e falliscono come una singola unità. Ad esempio, se avete un database primario e uno di replica, entrambi i database appartengono allo stesso AppComponent. AWS Resilience Hub dispone di regole che stabiliscono quali AWS risorse possono appartenere a quale AppComponent tipo. Ad esempio, un `DBInstance` può appartenere `AWS::ResilienceHub::DatabaseAppComponent` e non appartenere a`AWS::ResilienceHub::ComputeAppComponent`.

AWS Resilience Hub AppComponents Supportano le seguenti risorse:

- `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**
    >
    > Attualmente AWS Resilience Hub supporta solo Amazon FSx for Windows File Server.

  - `AWS::S3::Bucket`

Argomenti

Raggruppamento di risorse in un componente applicativo

Quando l'applicazione viene importata AWS Resilience Hub insieme alle relative risorse, AWS Resilience Hub fa del suo meglio per raggruppare le risorse correlate nella stessa AppComponent, ma potrebbe non essere sempre accurato al 100%. Inoltre, AWS Resilience Hub esegue le seguenti attività dopo che l'applicazione e le relative risorse sono state importate correttamente:

- Esamina le risorse per verificare se possono essere raggruppate in nuove risorse AppComponents per migliorare l'accuratezza della valutazione.
- Se AWS Resilience Hub identifica risorse che possono essere raggruppate in nuove risorse AppComponents, visualizza la stessa voce dei consigli e consente di accettarle, modificarle (aggiungere o rimuovere) o rifiutarle. In AWS Resilience Hub, il livello di confidenza assegnato a una raccomandazione di raggruppamento indica il grado di certezza con cui le risorse devono essere raggruppate in base ai rispettivi attributi e metadati. Un livello di confidenza elevato indica che AWS Resilience Hub ha un livello di confidenza pari o superiore al 90% che le risorse di quel gruppo sono correlate e devono essere raggruppate. Un livello di confidenza medio indica che

AWS Resilience Hub ha un livello di confidenza compreso tra il 70% e il 90% che le risorse di quel gruppo sono correlate e devono essere raggruppate.

> **Note**
>
> AWS Resilience Hub richiede il raggruppamento corretto in modo da poter calcolare il carico di lavoro stimato RTO e il carico di lavoro RPO stimato per generare raccomandazioni.

Di seguito sono riportati alcuni esempi di raggruppamenti corretti:

- Raggruppa database e repliche primari in un unico database. AppComponent
- Raggruppa un bucket Amazon S3 e la relativa replica di destinazione in un unico bucket. AppComponent
- Raggruppa EC2 le istanze Amazon che eseguono la stessa applicazione in un'unica AppComponent istanza.
- Raggruppa una SQS coda Amazon e la relativa coda di lettere non scritte in un'unica coda. AppComponent
- Raggruppa ECS i servizi Amazon in una regione ed esegui il failover ECS dei servizi Amazon in un'altra regione in un'unica AppComponent regione.

Per ulteriori informazioni sulla revisione e sull'inclusione dei consigli per il raggruppamento delle risorse per AWS Resilience Hub, consulta i seguenti argomenti:

- AWS Resilience Hub consigli per il raggruppamento delle risorse
- Raggruppamento manuale delle risorse in un AppComponent

AWS Resilience Hub consigli per il raggruppamento delle risorse

Questa sezione spiega come generare e rivedere i consigli per il raggruppamento delle risorse in. AWS Resilience Hub

> **Note**
>
> È possibile concedere le IAM autorizzazioni necessarie per lavorare utilizzando la politica AWS Resilience Hub `AWSResilienceHubAsssessmentExecutionPolicy`

AWS gestita. Per ulteriori informazioni sulla politica AWS gestita, vedereAWSResilienceHubAsssessmentExecutionPolicy.

Per visualizzare i consigli sul raggruppamento delle risorse

1. Nel riquadro di navigazione, scegliere Applications (Applicazioni).
2. Scegli la pagina Aggiungi applicazione, scegli il nome dell'applicazione per cui desideri esaminare i consigli sul raggruppamento delle risorse.
3. Scegli la scheda Struttura dell'applicazione.
4. Se AWS Resilience Hub visualizza un avviso informativo, scegli Rivedi consigli per visualizzare tutti i consigli sul raggruppamento delle risorse. Altrimenti completa i seguenti passaggi per generare manualmente consigli per il raggruppamento delle risorse:

   a. Scegliere Resources (Risorse).

   b. Scegli Ottieni consigli di raggruppamento dal menu Azioni.

      AWS Resilience Hub analizza le tue risorse per verificare come possono essere raggruppate nel miglior modo possibile in pertinenti AppComponents per migliorare l'accuratezza delle valutazioni. Se AWS Resilience Hub apprende che le risorse possono essere raggruppate, visualizza un avviso informativo in merito alle stesse.

   c. Se viene visualizzato l'avviso informativo, scegli Rivedi consigli per visualizzare tutti i consigli sul raggruppamento delle risorse.

   È possibile identificarli AppComponents nella sezione Rivedi i consigli per il raggruppamento delle risorse utilizzando quanto segue:

   - AppComponent name: nome del gruppo AppComponent in cui verranno raggruppate le risorse.
   - Livello di confidenza: indica il livello di confidenza di AWS Resilience Hub nella raccomandazione di raggruppamento.
   - Numero di risorse: indica il numero di risorse che verranno raggruppate in. AppComponent
   - AppComponent tipo: indica il tipo di. AppComponent

Per visualizzare le risorse che verranno raggruppate in AppComponents

1. Completare i passaggi indicati nella Per visualizzare i consigli sul raggruppamento delle risorseprocedura, quindi tornare a questa procedura.
2. Nella sezione Rivedi i consigli per il raggruppamento delle risorse, seleziona la casella di controllo (adiacente al AppComponent nome) per visualizzare tutte le risorse che verranno raggruppate all'interno di quelle selezionate. AppComponent Se selezioni più caselle di controllo, AWS Resilience Hub visualizza una sezione selezionata dei consigli generata dinamicamente che raggruppa le selezionate AppComponents in base al rispettivo tipo. AppComponent Scegliete il numero sotto ogni AppComponent tipo per visualizzare tutte le risorse che verranno raggruppate all'interno di quelle selezionate. AppComponent

   È possibile identificare le risorse che verranno raggruppate tra quelle selezionate AppComponent nella sezione Risorse utilizzando quanto segue:

   - ID logico: indica l'ID logico della risorsa. Un ID logico è un nome utilizzato per identificare le risorse nello AWS CloudFormation stack, nel file di stato Terraform, nell'applicazione aggiunta manualmente, nell' AppRegistry applicazione o. AWS Resource Groups
   - ID fisico: l'identificatore effettivo assegnato alla risorsa, ad esempio un ID di EC2 istanza Amazon o il nome di un bucket Amazon S3.
   - Tipo: indica il tipo di risorsa.
   - Regione: AWS regione in cui si trova la risorsa.

Per accettare i consigli sul raggruppamento delle risorse

1. Completare i passaggi indicati nella Per visualizzare i consigli sul raggruppamento delle risorseprocedura, quindi tornare a questa procedura.
2. Nella sezione Rivedi i consigli per il raggruppamento delle risorse, seleziona tutte le caselle di controllo adiacenti al AppComponentnome. Per trovare un nome specifico AppComponent, inserisci il AppComponent nome nella AppComponents casella Trova.

   > **Note**
   >
   > Per impostazione predefinita, AWS Resilience Hub visualizza tutti i consigli per il raggruppamento delle risorse. Per filtrare la tabella con i consigli di raggruppamento delle

risorse precedentemente rifiutati, scegli Precedentemente rifiutato dal menu a discesa adiacente alla casella Trova. AppComponents

3. Scegliere Accept (Accetta).
4. Scegli Accetta nella finestra di dialogo Accetta i consigli per il raggruppamento di risorse.

   AWS Resilience Hub visualizza un avviso informativo se il raggruppamento delle risorse ha esito positivo. Se hai accettato solo un sottoinsieme di consigli per il raggruppamento delle risorse, la sezione Rivedi i consigli per il raggruppamento delle risorse mostra tutti i consigli per il raggruppamento delle risorse che non hai accettato.

Per rifiutare i consigli sul raggruppamento delle risorse

1. Completare i passaggi indicati nella Per visualizzare i consigli sul raggruppamento delle risorseprocedura, quindi tornare a questa procedura.
2. Nella sezione Rivedi i consigli per il raggruppamento delle risorse, seleziona tutte le caselle di controllo adiacenti al AppComponentnome. Per trovare un nome specifico AppComponent, inserisci il AppComponent nome nella AppComponents casella Trova.

   > **Note**
   >
   > Per impostazione predefinita, AWS Resilience Hub visualizza tutti i consigli per il raggruppamento delle risorse. Per filtrare la tabella con i consigli di raggruppamento delle risorse precedentemente rifiutati, seleziona Precedentemente rifiutato dal menu a discesa adiacente alla casella Trova. AppComponents

3. Scegli Rifiuta.
4. Seleziona uno dei motivi per cui hai rifiutato il consiglio di raggruppamento di risorse, quindi scegli Rifiuta nella finestra di dialogo Rifiuta il consiglio di raggruppamento di risorse.

   AWS Resilience Hub visualizza un avviso informativo che conferma lo stesso. Se hai rifiutato solo un sottoinsieme di consigli per il raggruppamento di risorse, la sezione Rivedi i suggerimenti per il raggruppamento delle risorse mostra tutti i consigli per il raggruppamento di risorse che non hai accettato.

Raggruppamento manuale delle risorse in un AppComponent

Questa sezione spiega come raggruppare manualmente le risorse in una risorsa AppComponent e assegnarne di diverse AppComponent a una risorsa in. AWS Resilience Hub

Per raggruppare le risorse

1. Nel riquadro di navigazione, scegliere Applications (Applicazioni).
2. Nella pagina Applicazioni, scegli il nome dell'applicazione che contiene le risorse che desideri raggruppare.
3. Scegli la scheda Struttura dell'applicazione.
4. Nella scheda Versione, selezionate la versione dell'applicazione con lo stato Bozza.
5. Scegliere la scheda Resources (Risorse).
6. Seleziona le caselle di controllo adiacenti a Logical ID per selezionare tutte le risorse che desideri raggruppare.

   > **Note**
   >
   > Non è possibile scegliere risorse aggiunte manualmente.

7. Scegli Azioni, quindi scegli Raggruppa risorse.
8. Scegli una risorsa AppComponent dall'elenco a AppComponent discesa Scegli in cui vuoi raggruppare la risorsa.
9. Seleziona Salva.
10. Selezionare Publish new version (Pubblica nuova versione).
11. Scegli la scheda Struttura dell'applicazione.
12. Per visualizzare la versione pubblicata della tua applicazione, completa i seguenti passaggi:
    a. Nella scheda Versione, selezionate la versione dell'applicazione con lo stato di rilascio corrente.
    b. Scegliere la scheda Resources (Risorse).

Per assegnare risorse a un AppComponent

1. Nel riquadro di navigazione, scegliere Applications (Applicazioni).

2. Nella pagina Applicazioni, scegli il nome dell'applicazione che contiene la risorsa che desideri raggruppare.
3. Scegli la scheda Struttura dell'applicazione.
4. In Versione, selezionate la versione dell'applicazione con lo stato Bozza.
5. Scegliere la scheda Resources (Risorse).
6. Seleziona la casella di controllo adiacente a Logical ID per selezionare la risorsa.
7. Scegli Modifica AppComponent dal menu Azioni.
8. Per eliminare la corrente AppComponent dalla AppComponentsezione, scegli X nell'angolo in alto a destra dell'etichetta che mostra il tuo nome attuale. AppComponent
9. Per raggruppare la risorsa in modo diverso AppComponent, scegline una diversa AppComponent dall'elenco a discesa Scegli AppComponent.
10. Scegli Aggiungi.
11. Elimina eventuali spazi vuoti AppComponents dalla AppComponentsscheda.
12. Selezionare Publish new version (Pubblica nuova versione).
13. Scegli la scheda Struttura dell'applicazione.
14. Per visualizzare la versione pubblicata della tua applicazione, completa i seguenti passaggi:

    a. Nella scheda Versione, selezionate la versione dell'applicazione con lo stato di rilascio corrente.
    b. Scegliere la scheda Resources (Risorse).

Pubblicazione di una nuova versione AWS Resilience Hub dell'applicazione

Dopo aver apportato modifiche alle risorse AWS Resilience Hub dell'applicazione come descritto in[Modifica delle risorse delle AWS Resilience Hub applicazioni](), è necessario pubblicare una nuova versione dell'applicazione per eseguire una valutazione accurata della resilienza. Inoltre, potrebbe essere necessario pubblicare una nuova versione dell'applicazione se sono stati aggiunti nuovi allarmi e test consigliati all'applicazione. SOPs

Per pubblicare una nuova versione dell'applicazione

1. Nel riquadro di navigazione, scegliere Applications (Applicazioni).
2. Nella pagina Applicazioni, scegli il nome dell'applicazione.
3. Scegli la scheda Struttura dell'applicazione.

4. Selezionare Publish new version (Pubblica nuova versione).
5. Nella finestra di dialogo Pubblica versione, nella casella Nome, inserisci un nome per la versione dell'applicazione oppure puoi utilizzare il nome predefinito suggerito da AWS Resilience Hub.
6. Seleziona Publish (Pubblica).

   Quando pubblicate una nuova versione dell'applicazione, questa diventa la versione che viene valutata quando eseguite le valutazioni di resilienza. Inoltre, la versione bozza sarà identica alla versione rilasciata fino a quando non apporterete modifiche.

Dopo aver pubblicato una nuova versione dell'applicazione, ti consigliamo di eseguire un nuovo rapporto di valutazione della resilienza per confermare che l'applicazione soddisfa ancora la tua politica di resilienza. Per informazioni sull'esecuzione di una valutazione, consulta. Esecuzione e gestione delle valutazioni AWS Resilience Hub della resilienza

Visualizzazione di tutte le versioni AWS Resilience Hub dell'applicazione

Per tenere traccia delle modifiche all'applicazione, AWS Resilience Hub visualizza le versioni precedenti dell'applicazione dal momento della sua creazione in poi AWS Resilience Hub.

Per visualizzare tutte le versioni dell'applicazione

1. Nel riquadro di navigazione, scegliere Applications (Applicazioni).
2. Nella pagina Applicazioni, scegli il nome dell'applicazione.
3. Scegli la scheda Struttura dell'applicazione.
4. Per visualizzare tutte le versioni precedenti dell'applicazione, scegli il segno più (+) prima di Visualizza tutte le versioni. AWS Resilience Hub indica la versione bozza e la versione rilasciata di recente dell'applicazione utilizzando rispettivamente gli stati Bozza e Versione corrente. È possibile scegliere qualsiasi versione dell'applicazione per visualizzarne le risorse AppComponent, le fonti di input e altre informazioni associate.

   Inoltre, puoi anche filtrare l'elenco utilizzando una delle seguenti opzioni:

   - Filtra per nome della versione: inserisci un nome per filtrare i risultati in base al nome della versione dell'applicazione.
   - Filtra per intervallo di data e ora: per applicare questo filtro, scegli l'icona del calendario e seleziona una delle seguenti opzioni per filtrare in base ai risultati che corrispondono all'intervallo di tempo:

- Intervallo relativo: seleziona una delle opzioni disponibili e scegli Applica.

  Se scegli l'opzione Intervallo personalizzato, inserisci una durata nella casella Inserisci durata e seleziona l'unità di tempo appropriata dall'elenco a discesa Unità di tempo, quindi scegli Applica.

- Intervallo relativo: per specificare l'intervallo di data e ora, fornisci l'ora di inizio e l'ora di fine, quindi scegli Applica.

Visualizzazione delle risorse dell' AWS Resilience Hub applicazione

Per visualizzare le risorse dell'applicazione

1. Nel riquadro di navigazione, scegliere Applications (Applicazioni).
2. Nella pagina Applicazioni, seleziona l'applicazione per la quale desideri aggiornare le autorizzazioni di sicurezza.
3. Da Azioni, scegli Visualizza risorse.

   Nella scheda Risorse, puoi identificare le risorse nella tabella Risorse in base a quanto segue:

   - ID logico: un ID logico è un nome utilizzato per identificare le risorse nello AWS CloudFormation stack, nel file di stato Terraform, nell'applicazione aggiunta manualmente, nell' AppRegistry applicazione o. AWS Resource Groups

     > **Note**
     >
     > - Terraform ti consente di utilizzare lo stesso nome per diversi tipi di risorse. Pertanto, viene visualizzato "- tipo di risorsa" alla fine dell'ID logico per le risorse che condividono lo stesso nome.
     > - Per visualizzare le istanze di tutte le risorse dell'applicazione, scegliete il segno più (+) prima dell'ID logico. Per visualizzare tutte le istanze di una risorsa dell'applicazione, scegliete il segno più (+) prima dell'ID logico di ciascuna risorsa.
     >
     >   Per ulteriori informazioni sulle risorse supportate, vederethe section called “ AWS Resilience Hub risorse supportate”.

   - Stato: indica se AWS Resilience Hub valuteranno la resilienza della risorsa.

- Tipo di risorsa: il tipo di risorsa identifica la risorsa componente per l'applicazione. Ad esempio, `AWS::EC2::Instance` dichiara un'EC2istanza Amazon. Per ulteriori informazioni sul raggruppamento AppComponent delle risorse, consulta. Raggruppamento di risorse in un componente applicativo
- Nome sorgente: il nome della sorgente di input. Scegliete il nome della sorgente per visualizzarne i dettagli nella rispettiva applicazione. Per le sorgenti di input aggiunte manualmente, il collegamento non sarà disponibile. Ad esempio, se scegli il nome della fonte che viene importato da uno AWS CloudFormation stack, verrai reindirizzato alla pagina dei dettagli dello stack sul. AWS CloudFormation
- Tipo di sorgente: il tipo di sorgente di input.
- AppComponent tipo: il tipo di sorgente di input. Le fonti di input includono AWS CloudFormation pile, AppRegistry applicazioni AWS Resource Groups, file di stato Terraform e risorse aggiunte manualmente.

  > **Note**
  >
  > Per modificare i tuoi EKS cluster Amazon, completa i passaggi in Per modificare le fonti di input della procedura di AWS Resilience Hub applicazione.

- ID fisico: l'identificatore effettivo assegnato a quella risorsa, ad esempio un ID di EC2 istanza Amazon o il nome di un bucket S3.
- Incluso: indica se queste risorse sono AWS Resilience Hub incluse nell'applicazione.
- AppComponents— Il AWS Resilience Hub componente assegnato a questa risorsa quando è stata scoperta la relativa struttura applicativa.
- Nome: nome della risorsa dell'applicazione.
- Account: l' AWS account proprietario della risorsa fisica.

4. Scegli Salva e aggiorna.

Eliminazione di un'applicazione AWS Resilience Hub

Dopo aver raggiunto il limite massimo di dieci applicazioni, è necessario eliminare una o più applicazioni prima di poterne aggiungere altre.

Eliminazione di un'applicazione

1. Nel riquadro di navigazione, scegliere Applications (Applicazioni).

2. Nella pagina Applicazioni, seleziona l'applicazione che desideri eliminare.
3. Scegliere Actions (Operazioni), quindi Delete application (Elimina applicazione).
4. Per confermare l'eliminazione, inserisci Elimina nella casella Elimina e scegli Elimina.

Parametri di configurazione dell'applicazione

AWS Resilience Hub fornisce un meccanismo di input per raccogliere informazioni aggiuntive sulle risorse associate alle applicazioni. Con queste informazioni, AWS Resilience Hub acquisirete una comprensione più approfondita delle vostre risorse e fornirete migliori consigli sulla resilienza.

La sezione Parametri di configurazione dell'applicazione elenca tutti i parametri di configurazione del supporto di failover interregionale per. AWS Elastic Disaster RecoveryÈ possibile identificare i parametri di configurazione nel modo seguente:

- Argomento: indica l'area dell'applicazione configurata. Ad esempio, la configurazione del failover.
- Scopo: indica il motivo per cui sono state AWS Resilience Hub richieste le informazioni.
- Parametro: indica i dettagli specifici dell'area di applicazione, che AWS Resilience Hub verranno utilizzati per fornire consigli per l'applicazione. Attualmente, questo parametro utilizza un valore-chiave di una sola regione di failover e di un account associato.

Aggiornamento dei parametri di configurazione dell'applicazione

Questa sezione consente di aggiornare i parametri di configurazione dell'applicazione AWS Elastic Disaster Recovery e di pubblicare l'applicazione per includere i parametri aggiornati per le valutazioni della resilienza.

Per aggiornare i parametri di configurazione dell'applicazione

1. Nel riquadro di navigazione, scegliere Applications (Applicazioni).
2. Nella pagina Applicazioni, scegli il nome dell'applicazione che desideri modificare.
3. Scegli la scheda Parametri di configurazione dell'applicazione.
4. Scegli Aggiorna.
5. Inserisci l'ID dell'account di failover nella casella Account ID.
6. Seleziona una regione di failover dall'elenco a discesa Regione.

> **Note**
>
> Se desideri disabilitare questa funzionalità, seleziona "—" dall'elenco a discesa.

7. Scegli Aggiorna e pubblica.

Gestione delle politiche di resilienza

Questa sezione descrive come creare politiche di resilienza per le applicazioni. L'impostazione corretta delle politiche di resilienza consente di comprendere lo stato di resilienza dell'applicazione. Una policy di resilienza contiene informazioni e obiettivi da utilizzare per valutare se è previsto il ripristino dell'applicazione in seguito a un tipo di interruzione, ad esempio software, hardware, zona di disponibilità o regione. AWS Queste politiche non modificano né influiscono su un'applicazione effettiva. Più applicazioni possono avere la stessa politica di resilienza.

Quando si crea una politica di resilienza, si definiscono gli obiettivi target: Recovery Time Objective (RTO) e Recovery Point Objective (RPO). Gli obiettivi determinano se l'applicazione soddisfa la politica di resilienza. Allega la policy alla tua applicazione ed esegui una valutazione della resilienza. Puoi creare politiche diverse per i diversi tipi di applicazioni del tuo portafoglio. Ad esempio, un'applicazione di trading in tempo reale avrebbe una politica di resilienza diversa rispetto a un'applicazione di rendicontazione mensile.

> **Note**
>
> AWS Resilience Hub consente di inserire un valore zero nei campi RTO e RPO della politica di resilienza. Tuttavia, durante la valutazione della domanda, il risultato di valutazione più basso possibile è vicino allo zero. Pertanto, se inserisci un valore zero nei campi RTO e RPO, il risultato dell'RTO del carico di lavoro stimato e dell'RPO del carico di lavoro stimato saranno vicini allo zero e lo stato di conformità dell'applicazione verrà impostato su Policy violata.

La valutazione valuta la configurazione dell'applicazione rispetto alla politica di resilienza allegata. Al termine del processo, AWS Resilience Hub fornisce una valutazione del modo in cui l'applicazione si colloca rispetto agli obiettivi di ripristino indicati nella politica di resilienza.

È possibile creare politiche di resilienza nelle applicazioni e anche nelle politiche di resilienza. Puoi accedere ai dettagli pertinenti sulle tue politiche e anche modificarle ed eliminarle.

AWS Resilience Hub utilizza gli obiettivi RTO e RPO per misurare la resilienza a questi potenziali tipi di interruzioni:

- Applicazione: perdita di un servizio o di un processo software richiesto.
- Infrastruttura cloud: perdita di hardware, come le istanze EC2.
- Zona di disponibilità dell'infrastruttura cloud (AZ): una o più zone di disponibilità non sono disponibili.
- Regione dell'infrastruttura cloud: una o più regioni non sono disponibili.

AWS Resilience Hub ti consente di creare politiche di resilienza personalizzate o utilizzare le nostre politiche di resilienza a standard aperti consigliate. Quando crei policy personalizzate, assegna un nome e descrivi la tua policy e scegli il livello o il livello appropriato che definisce la tua policy. Questi livelli includono: servizi IT di base, Mission critical, Critical, Important e Non critical.

Scegliete il livello più adatto alla vostra classe di applicazione. Ad esempio, potresti classificare un sistema di trading in tempo reale come critico, mentre potresti classificare un'applicazione di rendicontazione mensile come non critica. Quando utilizzi le nostre politiche standard, puoi scegliere una politica di resilienza con un livello e valori preconfigurati per gli obiettivi RTO e RPO suddivisi per tipo di interruzione. Se necessario, puoi modificare il livello e gli obiettivi RTO e RPO.

È possibile creare politiche di resilienza in Politiche di resilienza o quando si descrive una nuova applicazione.

Creazione di politiche di resilienza

Nel AWS Resilience Hub, puoi creare una politica di resilienza. Una policy di resilienza contiene informazioni e obiettivi da utilizzare per valutare se l'applicazione è in grado di eseguire il ripristino dopo un tipo di interruzione, ad esempio software, hardware, zona di disponibilità o regione. AWS Queste politiche non modificano o influiscono su un'applicazione effettiva. Più applicazioni possono avere la stessa politica di resilienza.

Quando si crea una politica di resilienza, si definiscono gli obiettivi RTO (Recovery Time Objective) e RPO (Recovery Point Objective). Quando si esegue una valutazione, AWS Resilience Hub determina se si stima che l'applicazione soddisfi gli obiettivi definiti nella politica di resilienza.

La valutazione valuta la configurazione dell'applicazione rispetto alla politica di resilienza allegata. Al termine del processo, AWS Resilience Hub fornisce una valutazione del modo in cui l'applicazione si colloca rispetto agli obiettivi della politica di resilienza.

> **Note**
>
> AWS Resilience Hub consente di inserire un valore zero nei campi RTO e RPO della politica di resilienza. Tuttavia, durante la valutazione della domanda, il risultato di valutazione più basso possibile è vicino allo zero. Pertanto, se inserisci un valore zero nei campi RTO e RPO, il risultato dell'RTO del carico di lavoro stimato e dell'RPO del carico di lavoro stimato saranno vicini allo zero e lo stato di conformità dell'applicazione verrà impostato su Policy violata.

È possibile creare politiche di resilienza nelle applicazioni e anche nelle politiche di resilienza. Puoi accedere ai dettagli pertinenti sulle tue politiche e anche modificarle ed eliminarle.

Per creare politiche di resilienza nelle applicazioni

1. Nel menu di navigazione a sinistra, scegli Applicazioni.
2. Completa le procedure dall'inizio the section called “Passaggio 1: Inizia aggiungendo un'applicazione” alla finethe section called “Fase 8: Aggiungere tag all'applicazione ”.
3. Nella sezione Politiche di resilienza, scegli Crea politica di resilienza.

   Viene visualizzata la pagina Crea politica di resilienza.
4. Nella sezione Scegli un metodo di creazione, seleziona Crea una politica.
5. Inserisci un nome per la policy.
6. (Facoltativo) Immettere una descrizione per la policy.
7. Scegli una delle seguenti opzioni dall'elenco a discesa Tier:

   - Servizi IT di base
   - Mission critical
   - Critico
   - Importante
   - Non critico
8. Per entrambi gli obiettivi RTO e RPO, in Customer Application RTO e RPO, inserisci un valore numerico nella casella, quindi scegli l'unità di tempo rappresentata dal valore.

   Ripeti queste voci in Infrastructure RTO e RPO for Infrastructure and Availability Zone.
9. (Facoltativo) Se si dispone di un'applicazione multiregionale, è possibile definire gli obiettivi RTO e RPO di una regione.

Attiva la regione. Per entrambi gli obiettivi Region RTO e RPO, in Customer Application RTO e RPO, inserisci un valore numerico nella casella, quindi scegli l'unità di tempo rappresentata dal valore.

10. (Facoltativo) Se desideri aggiungere tag, puoi farlo in un secondo momento man mano che continui a creare la tua politica. Per ulteriori informazioni sui tag, consulta Etichettatura delle risorse nella Guida AWS generale.
11. Per creare la politica, scegli Crea.

Per creare politiche di resilienza in Politiche di resilienza

1. Nel menu di navigazione a sinistra, scegli Politiche.
2. Nella sezione Politiche di resilienza, scegli Crea politica di resilienza.

   Viene visualizzata la pagina Crea politica di resilienza.
3. Inserisci un nome per la policy.
4. (Facoltativo) Immettere una descrizione per la policy.
5. Scegli una delle seguenti opzioni da Tier:

   - Servizi IT di base
   - Mission critical
   - Critico
   - Importante
   - Non critico
6. Per entrambi gli obiettivi RTO e RPO, in Customer Application RTO e RPO, inserisci un valore numerico nella casella, quindi scegli l'unità di tempo rappresentata dal valore.

   Ripeti queste voci in Infrastructure RTO e RPO for Infrastructure and Availability Zone.
7. (Facoltativo) Se si dispone di un'applicazione multiregionale, è possibile definire gli obiettivi RTO e RPO di una regione.

   Attiva la regione. Per entrambi gli obiettivi RTO e RPO, in Customer Application RTO and RPO, inserisci un valore numerico nella casella, quindi scegli l'unità di tempo rappresentata dal valore.
8. (Facoltativo) Se desideri aggiungere tag, puoi farlo in un secondo momento, man mano che continui a creare la tua politica. Per ulteriori informazioni sui tag, consulta Etichettatura delle risorse nella Guida AWS generale.

9. Per creare la politica, scegli Crea.

Per creare politiche di resilienza basate su una politica suggerita

1. Nel menu di navigazione a sinistra, scegli Politiche.
2. Nella sezione Scegli un metodo di creazione, seleziona Seleziona una politica basata su una politica suggerita.
3. Nella sezione Politiche di resilienza, scegli Crea politica di resilienza.

   Viene visualizzata la pagina Crea politica di resilienza.
4. Immettere un nome per la politica di resilienza.
5. (Facoltativo) Immettere una descrizione per la policy.
6. Nella sezione Politiche di resilienza consigliate, visualizza e scegli uno dei seguenti livelli di policy di resilienza predeterminati:

   - Applicazione non critica
   - Applicazione importante
   - Applicazione critica
   - Applicazione critica globale
   - Applicazione mission critical
   - Applicazione mission critical a livello globale
   - Servizio di base
7. Per creare la politica di resilienza, scegli Crea politica.

Accesso ai dettagli della politica di resilienza

Quando si apre una politica di resilienza, vengono visualizzati dettagli importanti sulla politica. Puoi anche modificare o eliminare la resilienza.

I dettagli della politica di resilienza consistono in due visualizzazioni principali: riepilogo e tag.

Riepilogo

Informazioni di base

Fornisce le seguenti informazioni sulla politica di resilienza: nome, descrizione, livello, livello di costo e data di creazione.

RTO del carico di lavoro stimato e RPO del carico di lavoro stimato

Mostra l'RTO stimato del carico di lavoro e il tipo di interruzione dell'RPO stimato del carico di lavoro associati a questa politica di resilienza.

Tag

Utilizzate questa visualizzazione per gestire, aggiungere ed eliminare i tag interni a questa applicazione.

Per modificare le politiche di resilienza in Dettagli delle politiche di resilienza

1. Nel menu di navigazione a sinistra, scegli Politiche.
2. In Politiche di resilienza, apri una politica di resilienza.
3. Scegli Modifica. Inserisci le modifiche appropriate nei campi Informazioni di base e RTO e RPO. Selezionare quindi Save changes (Salva modifiche).

Per modificare le politiche di resilienza in Politica di resilienza

1. Nel menu di navigazione a sinistra, scegli Politiche.
2. In Politiche di resilienza, scegli una politica di resilienza.
3. Scegli Azioni, quindi seleziona Modifica.
4. Inserisci le modifiche appropriate nei campi Informazioni di base e RTO e RPO. Selezionare quindi Save changes (Salva modifiche).

Per eliminare le politiche di resilienza in Dettagli delle politiche di resilienza

1. Nel menu di navigazione a sinistra, scegli Politiche.
2. In Politiche di resilienza, apri una politica di resilienza.
3. Scegli Elimina. Conferma l'eliminazione, quindi scegli Elimina.

Per eliminare le politiche di resilienza nella politica di resilienza

1. Nel menu di navigazione a sinistra, scegli Politiche.

2. In Politiche di resilienza, scegli una politica di resilienza.
3. Scegli Azioni, quindi seleziona Elimina.
4. Conferma l'eliminazione, quindi scegli Elimina.

Esecuzione e gestione delle valutazioni AWS Resilience Hub della resilienza

Quando l'applicazione cambia, è necessario eseguire una valutazione della resilienza. La valutazione confronta la configurazione di ogni componente dell'applicazione con la policy e fornisce raccomandazioni in materia di allarmi e test. SOP Questi consigli di configurazione possono migliorare la velocità delle procedure di ripristino.

I consigli sugli allarmi consentono di impostare allarmi che rilevano interruzioni. SOPle raccomandazioni forniscono script che gestiscono i processi di ripristino comuni, come il ripristino da un backup. I consigli per i test offrono suggerimenti per verificare il corretto funzionamento delle configurazioni. Ad esempio, è possibile verificare se un'applicazione viene ripristinata durante i processi di ripristino automatici, come il ridimensionamento automatico o il bilanciamento del carico, a causa di problemi di rete. È possibile verificare se gli allarmi delle applicazioni vengono attivati quando le risorse raggiungono i limiti. Puoi anche verificare l'efficienza del tuo SOPs funzionamento nelle condizioni da te indicate.

Esecuzione di valutazioni della resilienza

È possibile eseguire un rapporto di valutazione della resilienza da più sedi in. AWS Resilience Hub Per ulteriori informazioni sulla tua applicazione, consultathe section called “Gestione delle applicazioni”.

Per eseguire una valutazione della resilienza dal menu Azioni

1. Nel menu di navigazione a sinistra, scegli Applicazioni.
2. Scegli un'applicazione dalla tabella Applicazioni.
3. Scegli Valuta la resilienza dal menu Azioni.
4. Nella finestra di dialogo Esegui la valutazione della resilienza, puoi inserire un nome univoco o utilizzare il nome generato per la valutazione.
5. Seleziona Esegui.

Per esaminare il rapporto di valutazione, scegli Valutazioni nella tua applicazione. Per ulteriori informazioni, consulta the section called “Revisione dei rapporti di valutazione”.

Per eseguire una valutazione della resilienza dalla scheda Valutazioni

È possibile eseguire una nuova valutazione della resilienza quando l'applicazione o la politica di resilienza cambiano.

1. Nel menu di navigazione a sinistra, scegli Applicazioni.
2. Scegli un'applicazione dalla tabella Applicazioni.
3. Scegli la scheda Valutazioni.
4. Scegli Esegui una valutazione della resilienza.
5. Nella finestra di dialogo Esegui la valutazione della resilienza, puoi inserire un nome univoco o utilizzare il nome generato per la valutazione.
6. Seleziona Esegui.

   Per esaminare il rapporto di valutazione, scegli Valutazioni nella tua applicazione. Per ulteriori informazioni, consulta the section called “Revisione dei rapporti di valutazione”.

Revisione dei rapporti di valutazione

I report di valutazione sono disponibili nella visualizzazione Valutazioni dell'applicazione.

Per trovare un rapporto di valutazione

1. Nel menu di navigazione a sinistra, scegli Applicazioni.
2. In Applicazioni, apri un'applicazione.
3. Nella scheda Valutazioni, scegli un rapporto di valutazione dalla tabella Valutazioni della resilienza.

Quando apri il rapporto, vedi quanto segue:

- Una panoramica generale del rapporto di valutazione
- Raccomandazioni per migliorare la resilienza.
- Consigli per impostare allarmi e SOPs test

- Come creare e gestire tag per cercare e filtrare le risorse AWS

Verificare

Questa sezione fornisce una panoramica del rapporto di valutazione. AWS Resilience Hub elenca ogni tipo di interruzione e il componente applicativo associato. Elenca inoltre le politiche effettive RTO e RPO le politiche e determina se il componente applicativo è in grado di raggiungere gli obiettivi della politica.

Panoramica

Mostra il nome dell'applicazione, il nome della politica di resilienza e la data di creazione del rapporto.

Derive di risorse rilevate

Questa sezione elenca tutte le risorse che sono state aggiunte o rimosse dopo essere state incluse nell'ultima versione dell'applicazione pubblicata. Scegliete Reimporta le sorgenti di input per reimportare tutte le fonti di input (che contengono risorse alla deriva) nella scheda Fonti di input. Scegli Pubblica e valuta per includere le risorse aggiornate nell'applicazione e ricevere una valutazione accurata della resilienza.

È possibile identificare le sorgenti di input deviate utilizzando quanto segue:

- ID logico: indica l'ID logico della risorsa. Un ID logico è un nome utilizzato per identificare le risorse nello AWS CloudFormation stack, nel file di stato Terraform, nell'applicazione aggiunta manualmente, nell' AppRegistry applicazione o. AWS Resource Groups
- Modifica: indica se una risorsa di input è stata aggiunta o rimossa.
- Nome sorgente: indica il nome della risorsa. Scegliete il nome di una fonte per visualizzarne i dettagli nella rispettiva applicazione. Per le sorgenti di input aggiunte manualmente, il collegamento non sarà disponibile. Ad esempio, se scegli il nome della fonte che viene importato da uno AWS CloudFormation stack, verrai reindirizzato alla pagina dei dettagli dello stack sul. AWS CloudFormation
- Tipo di risorsa: indica il tipo di risorsa.
- Account: indica l' AWS account proprietario della risorsa fisica.
- Regione: indica la AWS regione in cui si trova la risorsa.

RTO

Mostra una rappresentazione grafica che indica se si stima che l'applicazione soddisfi gli obiettivi della politica di resilienza. Si basa sul periodo di tempo in cui un'applicazione può rimanere inattiva senza causare danni significativi all'organizzazione. La valutazione fornisce un carico di lavoro RTO stimato.

RPO

Mostra una rappresentazione grafica che indica se si stima che l'applicazione soddisfi gli obiettivi della politica di resilienza. Ciò si basa sul periodo di tempo in cui i dati possono essere persi prima che si verifichi un danno significativo all'azienda. La valutazione fornisce un carico di lavoro RPO stimato.

Dettagli

Fornisce descrizioni dettagliate di ogni tipo di interruzione utilizzando le schede Tutti i risultati e Application compliance drifts. La scheda Tutti i risultati mostra tutte le interruzioni, comprese le derive relative alla conformità, mentre la scheda Dati sulla conformità delle applicazioni mostra solo le variazioni di conformità. Il tipo di interruzione include l'applicazione, l'infrastruttura cloud (infrastruttura e zona di disponibilità) e la regione e fornisce le seguenti informazioni al riguardo:

- AppComponent

  Le risorse che compongono l'applicazione. Ad esempio, l'applicazione potrebbe avere un database o un componente di calcolo.

- Stimato RTO

  Indica se la configurazione della politica è in linea con i requisiti della politica. Forniamo due valori, il nostro Stimato RTO e il Vostro Targeted RTO. Ad esempio, se vedi un valore di 2 ore in Targeted RTO e 40 m in quello di Stimated Workload RTO, significa che forniamo un carico RTO di lavoro stimato di 40 minuti, mentre la durata attuale dell'applicazione è RTO di due ore. Basiamo il RTO calcolo del carico di lavoro stimato sulla configurazione, non sulla politica. Di conseguenza, un database con più zone di disponibilità avrà lo stesso carico di lavoro stimato in caso RTO di errore della zona di disponibilità, indipendentemente dalla politica selezionata.
- RTOderiva

  Indica la durata entro la quale l'applicazione si è allontanata dal carico di lavoro stimato RTO della precedente valutazione positiva. Forniamo due valori, i nostri valori RTOstimati e quelli relativi alla deriva. RTO Ad esempio, se vedi il valore di 2 ore in Stimato RTO e 40 m in quello di

RTOderiva, significa che l'applicazione si discosta di 40 minuti dal carico RTO di lavoro stimato della precedente valutazione positiva.

- Stimato RPO

  Mostra la RPO politica di carico di lavoro stimata effettiva stimata, in base alla RPO politica di Targeted impostata per ogni componente dell'applicazione. AWS Resilience Hub Ad esempio, potreste aver impostato l'RPOobiettivo della vostra politica di resilienza per i guasti nella zona di disponibilità su un'ora. Il risultato stimato potrebbe essere calcolato vicino allo zero. Ciò presuppone che Amazon Aurora, dove effettuiamo ogni transazione, abbia successo in quattro nodi su sei, su più zone di disponibilità. Potrebbero essere necessari cinque minuti per il ripristino. point-in-time

  L'unico RTO RPO obiettivo che puoi scegliere di non fornire è la regione. Per alcune applicazioni, è utile pianificare il ripristino quando esiste una dipendenza cruciale da un AWS servizio, che potrebbe non essere disponibile nell'intera regione.

  Se scegli questa opzione, ad esempio l'impostazione RTO o RPO gli obiettivi per la regione, riceverai un tempo di ripristino stimato e consigli operativi per tali errori.

- RPOderiva

  Indica la durata entro la quale l'applicazione si è allontanata dal carico di lavoro stimato RPO della precedente valutazione positiva. Forniamo due valori, i nostri valori RPOstimati e quelli relativi alla deriva. RPO Ad esempio, se vedi il valore di 2 ore in Stimato RPO e 40 m in quello di RPOderiva, significa che l'applicazione si discosta di 40 minuti dal carico RPO di lavoro stimato della precedente valutazione positiva.

Revisione delle raccomandazioni sulla resilienza

I consigli sulla resilienza valutano i componenti dell'applicazione e consigliano come ottimizzarli in base al carico di lavoro stimato RTO e al carico di lavoro stimatoRPO, ai costi e alle modifiche minime.

Con AWS Resilience Hub, puoi ottimizzare la resilienza utilizzando una delle seguenti opzioni consigliate in Perché scegliere questa opzione:

Note

- AWS Resilience Hub offre fino a tre opzioni AWS Resilience Hub consigliate.
- Se si impostano Regionali RTO e RPO obiettivi, AWS Resilience Hub visualizza Optimize for RegionRTO/RPOnelle opzioni consigliate. Se non sono RPO impostati obiettivi RTO e regionali, RPO viene visualizzato Optimize for Availability Zone (AZ)RTO/. Per ulteriori informazioni sull'impostazione RPO degli obiettivi RTO regionali/durante la creazione di politiche di resilienza, consultaCreazione di politiche di resilienza .
- Il carico di lavoro stimato RTO e RPO i valori stimati del carico di lavoro per le applicazioni e le relative configurazioni sono determinati considerando la quantità di dati e gli individui. AppComponents Tuttavia, questi valori sono solo stime. È necessario utilizzare test propri (come Amazon Fault Injection Service) per verificare i tempi di ripristino effettivi dell'applicazione.

Ottimizzazione per la zona di disponibilitàRTO/RPO

I tempi di ripristino del carico di lavoro stimati più bassi possibili (RTO/RPO) durante un'interruzione della zona di disponibilità (AZ). Se la configurazione non può essere modificata in modo sufficiente per soddisfare gli RPO obiettivi RTO AND, verrai informato sui tempi di ripristino AZ del carico di lavoro stimati più bassi per avvicinare la tua configurazione alla possibilità di soddisfare la policy.

Ottimizza per regione/RTORPO

I tempi di ripristino del carico di lavoro stimati più bassi possibili (RTO/RPO) durante un'interruzione regionale. Se la configurazione non può essere modificata sufficientemente per soddisfare gli RPO obiettivi RTO e, per avvicinare la configurazione alla policy, verrai informato sui tempi di ripristino della regione con il carico di lavoro più bassi stimati.

Ottimizza i costi

Il costo più basso che puoi sostenere pur rispettando la tua politica di resilienza. Se la configurazione non può essere modificata sufficientemente per soddisfare gli obiettivi di ottimizzazione, siete informati sul costo più basso che potete sostenere per avvicinare la vostra configurazione alla possibilità di soddisfare la policy.

Ottimizza per modifiche minime

Le modifiche minime necessarie per raggiungere gli obiettivi politici. Se la configurazione non può essere modificata sufficientemente per soddisfare gli obiettivi di ottimizzazione, verrai informato sulle modifiche consigliate che possono avvicinare la tua configurazione alla possibilità di soddisfare la policy.

I seguenti elementi sono inclusi nelle suddivisioni per categoria di ottimizzazione:

- Descrizione

  Descrive le configurazioni suggerite da. AWS Resilience Hub

- Modifiche

  Un elenco di modifiche al testo che descrivono le attività necessarie per passare alla configurazione suggerita.

- Costo base

  Il costo stimato associato alle modifiche consigliate.

  > **Note**
  >
  > Il costo base può variare in base all'utilizzo e non include sconti o offerte dell'Enterprise Discount Program (EDP).

- Carico di lavoro RTO stimato e RPO

  Carico di lavoro stimato RTO e carico di lavoro RPO stimato dopo le modifiche.

AWSResilience Hub valuta se un componente applicativo (AppComponent) è conforme a una politica di resilienza. Se AppComponent non è conforme a una politica di resilienza e AWS Resilience Hub non è in grado di formulare raccomandazioni per facilitare la conformità, è possibile che il tempo di ripristino per il selezionato AppComponent non possa essere rispettato entro i limiti del. AppComponent Esempi di AppComponent vincoli includono il tipo di risorsa, la dimensione di archiviazione o la configurazione delle risorse.

Per facilitare la AppComponent conformità della politica di resilienza, modifica il tipo di risorsa AppComponent o aggiorna la politica di resilienza per allinearla a ciò che la risorsa può offrire.

Revisione delle raccomandazioni operative

Le raccomandazioni operative contengono raccomandazioni per impostare allarmi ed AWS FIS esperimenti tramite AWS CloudFormation modelli. SOPs

AWS Resilience Hub fornisce file AWS CloudFormation modello che consentono di scaricare e gestire l'infrastruttura dell'applicazione sotto forma di codice. Di conseguenza, forniamo consigli in AWS CloudFormation modo da poterli aggiungere al codice dell'applicazione. Se la dimensione del file AWS CloudFormation modello è superiore a un MB e contiene più di 500 risorse, AWS Resilience Hub genera più di un file AWS CloudFormation modello in cui la dimensione di ogni file non è superiore a un MB e contiene fino a 500 risorse. Se il file AWS CloudFormation modello è suddiviso in più file, ai nomi dei file AWS CloudFormation modello verrà aggiuntopartXofY, dove X indica il numero di file nella sequenza e Y indica il numero totale di file in cui è suddiviso il file AWS CloudFormation modello. Ad esempio, se il file modello `big-app-template5-Alarm-104849185070-us-west-2.yaml` è diviso in quattro file, i nomi dei file sarebbero i seguenti:

- `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`

Tuttavia, in caso di AWS CloudFormation modelli di grandi dimensioni, ti viene richiesto di fornire Amazon Simple Storage Service URI anziché utilizzareCLI/APIcon file locale come input.

In AWS Resilience Hub, puoi eseguire le seguenti azioni:

- È possibile fornire gli allarmi selezionati e SOPs gli AWS FIS esperimenti. Per fornire allarmi ed AWS FIS esperimentiSOPs, seleziona il consiglio appropriato e inserisci un nome univoco. AWS Resilience Hub crea un modello basato sui consigli selezionati. In Templates, puoi accedere ai modelli creati tramite Amazon Simple Storage Service (Amazon S3). URL
- Puoi includere o escludere allarmi selezionati ed AWS FIS esperimenti consigliati per la tua applicazione in qualsiasi momento. SOPs Per ulteriori informazioni, consultare the section called “Inclusione o esclusione di raccomandazioni operative”.
- Potete anche cercare, creare, aggiungere, rimuovere e gestire i tag di un'applicazione e visualizzare tutti i tag ad essa associati.

Inclusione o esclusione di raccomandazioni operative

AWS Resilience Hub offre la possibilità di includere o escludere gli allarmi e SOPs gli AWS FIS esperimenti (test) consigliati per migliorare il punteggio di resilienza dell'applicazione in qualsiasi momento. L'inclusione o l'esclusione dei consigli operativi avrà un impatto sul punteggio di resilienza dell'applicazione solo dopo l'esecuzione di una nuova valutazione. Pertanto, ti consigliamo di eseguire una valutazione per ottenere il punteggio di resilienza aggiornato e comprenderne l'impatto sulla tua applicazione.

Per ulteriori informazioni sulla limitazione delle autorizzazioni per includere o escludere consigli per applicazione, consulta. the section called “Limitazione delle autorizzazioni per includere o escludere consigli AWS Resilience Hub ”

Per includere o escludere i consigli operativi dalle applicazioni

1. Nel menu di navigazione a sinistra, scegli Applicazioni.
2. In Applicazioni, apri un'applicazione.
3. Scegli Valutazioni e seleziona una valutazione dalla tabella Valutazioni della resilienza. Se non disponi di una valutazione, completa la procedura riportata in the section called “Esecuzione di valutazioni della resilienza” e poi torna a questo passaggio.
4. Seleziona la scheda Raccomandazioni operative.
5. Per includere o escludere i consigli operativi dalla tua applicazione, completa le seguenti procedure:

Per includere o escludere gli allarmi consigliati dall'applicazione

1. Per escludere gli allarmi, completa i seguenti passaggi:

    a. Nella scheda Allarmi, dalla tabella Allarmi, seleziona tutti gli allarmi (con lo stato Non implementato) che desideri escludere. Puoi identificare lo stato di implementazione corrente di un allarme dalla colonna Stato.

    b. In Azioni, scegli Escludi selezionati.

    c. Dalla finestra di dialogo Escludi consigli, seleziona uno dei seguenti motivi (opzionale) e scegli Escludi selezionati per escludere gli allarmi selezionati dall'applicazione.

        - Già implementato: scegli questa opzione se hai già implementato questi allarmi in un AWS servizio come Amazon CloudWatch o qualsiasi altro fornitore di servizi di terze parti.

- Non pertinente: scegli questa opzione se gli allarmi non soddisfano i tuoi requisiti aziendali.
- Troppo complicato da implementare: scegli questa opzione se ritieni che questi allarmi siano troppo complicati da implementare.
- Altro: scegli questa opzione per specificare qualsiasi altro motivo per escludere la raccomandazione.

2. Per includere gli allarmi, completa i seguenti passaggi:

   a. Nella scheda Allarmi, dalla tabella Allarmi, seleziona tutti gli allarmi (con stato Escluso) che desideri includere. È possibile identificare lo stato di implementazione corrente dell'allarme dalla colonna Stato.

   b. Da Azioni, scegli Includi selezionati.

   c. Dalla finestra di dialogo Includi consigli, scegli Includi selezionati per includere tutti gli allarmi selezionati nell'applicazione.

Per includere o escludere le procedure operative standard consigliate (SOPs) dall'applicazione

1. Per escludere le opzioni consigliateSOPs, completa la procedura seguente:

   a. Nella scheda Procedure operative standard, dalla SOPstabella, seleziona tutte le SOPs (con lo stato Implementato o Non implementato) che desideri escludere. È possibile identificare lo stato di implementazione corrente di an SOP dalla colonna Stato.

   b. In Azioni, scegli Escludi selezionati per escludere i selezionati SOPs dalla tua applicazione.

   c. Dalla finestra di dialogo Escludi consigli, seleziona uno dei seguenti motivi (opzionale) e scegli Escludi selezionati per escludere il selezionato SOPs dall'applicazione.

      - Già implementato: scegli questa opzione se li hai già implementati SOPs in un AWS servizio o in qualsiasi altro fornitore di servizi di terze parti.
      - Non pertinente: scegli questa opzione se SOPs non soddisfa i tuoi requisiti aziendali.
      - Troppo complicate da implementare: scegliete questa opzione se ritenete che SOPs siano troppo complicate da implementare.
      - Nessuno: scegli questa opzione se non desideri specificare il motivo.

2. Per includereSOPs, completa i seguenti passaggi:

a. Nella scheda Procedure operative standard, dalla SOPstabella, seleziona tutti gli allarmi (con lo stato Escluso) che desideri includere. È possibile identificare lo stato di implementazione corrente dell'allarme dalla colonna Stato.

b. Da Azioni, scegli Includi selezionati.

c. Dalla finestra di dialogo Includi consigli, scegli Includi selezionati per includere tutti i selezionati SOPs nell'applicazione.

Per includere o escludere i test consigliati dall'applicazione

1. Per escludere i test consigliati, completa i seguenti passaggi:

   a. Nella scheda Modelli di esperimenti di iniezione di errori, dalla tabella Modelli di esperimenti di iniezione di errori, seleziona tutti i test (con lo stato Implementato o Non implementato) che desideri escludere. È possibile identificare lo stato di implementazione corrente di un test dalla colonna Stato.

   b. In Azioni, scegli Escludi selezionati.

   c. Dalla finestra di dialogo Escludi consigli, selezionate uno dei seguenti motivi (opzionale) e scegliete Escludi selezionati per escludere gli AWS FIS esperimenti selezionati dall'applicazione.

      - Già implementato: scegli questa opzione se hai già implementato questi test in un AWS servizio o in qualsiasi altro fornitore di servizi di terze parti.
      - Non pertinente: scegli questa opzione se i test non soddisfano i tuoi requisiti aziendali.
      - Troppo complicati da implementare: scegli questa opzione se ritieni che questi test siano troppo complicati da implementare.
      - Nessuno: scegli questa opzione se non desideri specificare il motivo.

2. Per includere i test consigliati, completa i seguenti passaggi:

   a. Nella scheda Modelli di esperimenti di iniezione di errore, dalla tabella Modelli di esperimenti di iniezione di errori, seleziona tutti i test (con lo stato Escluso) che desideri includere. È possibile identificare lo stato di implementazione corrente del test dalla colonna Stato.

   b. Da Azioni, scegli Includi selezionati.

   c. Nella finestra di dialogo Includi consigli, scegli Includi selezionati per includere tutti i test selezionati nella tua applicazione.

Eliminazione delle valutazioni di resilienza

Puoi eliminare le valutazioni della resilienza nella vista Valutazioni dell'applicazione.

Per eliminare una valutazione della resilienza

1. Nel menu di navigazione a sinistra, scegli Applicazioni.
2. In Applicazioni, apri un'applicazione.
3. In Valutazioni, scegli un rapporto di valutazione nella tabella Valutazioni della resilienza.
4. Per confermare l'eliminazione, scegliere Delete (Elimina).

   Il rapporto non appare più nella tabella delle valutazioni della resilienza.

Gestione degli allarmi

Quando esegui una valutazione della resilienza, come parte delle raccomandazioni operative, AWS Resilience Hub ti consigliamo di configurare gli CloudWatch allarmi Amazon per monitorare la resilienza delle tue applicazioni. Consigliamo questi allarmi in base alle risorse e ai componenti della configurazione corrente dell'applicazione. Se le risorse e i componenti dell'applicazione cambiano, è necessario eseguire una valutazione della resilienza per assicurarsi di disporre degli allarmi corretti per l'applicazione aggiornata.

AWS Resilience Hub fornisce un file modello (`README.md`) che consente di creare allarmi consigliati dall' AWS Resilience Hub interno AWS (come Amazon CloudWatch) o dall'esterno AWS. I valori predefiniti forniti negli allarmi si basano sulle migliori pratiche utilizzate per creare questi allarmi.

Argomenti

- Creazione di allarmi in base alle raccomandazioni operative
- Visualizzazione degli allarmi

Creazione di allarmi in base alle raccomandazioni operative

AWS Resilience Hub crea un AWS CloudFormation modello che contiene i dettagli per creare gli allarmi selezionati in Amazon CloudWatch. Dopo aver generato il modello, puoi accedervi tramite Amazon S3URL, scaricarlo e inserirlo nella pipeline di codice o creare uno stack tramite la console. AWS CloudFormation

Per creare un allarme basato sui AWS Resilience Hub consigli, devi creare un AWS CloudFormation modello per gli allarmi consigliati e includerli nella tua base di codice.

Per creare allarmi nei consigli operativi

1. Nel menu di navigazione a sinistra, scegli Applicazioni.
2. In Applicazioni, scegli la tua applicazione.
3. Scegli la scheda Valutazioni.

   Nella tabella delle valutazioni della resilienza, puoi identificare le tue valutazioni utilizzando le seguenti informazioni:

   - Nome: nome della valutazione che avevi fornito al momento della creazione.
   - Stato: indica lo stato di esecuzione della valutazione.
   - Stato di conformità: indica se la valutazione è conforme alla politica di resilienza.
   - Stato di variazione della resilienza: indica se la domanda si è allontanata o meno dalla precedente valutazione positiva.
   - Versione dell'app: versione dell'applicazione.
   - Invoker: indica il ruolo che ha richiamato la valutazione.
   - Ora di inizio: indica l'ora di inizio della valutazione.
   - Ora di fine: indica l'ora di fine della valutazione.
   - ARN— L'Amazon Resource Name (ARN) della valutazione.
4. Seleziona una valutazione dalla tabella delle valutazioni della resilienza. Se non disponi di una valutazione, completa la procedura riportata in the section called “Esecuzione di valutazioni della resilienza” e poi torna a questo passaggio.
5. Scegli Raccomandazioni operative.
6. Se non è selezionata per impostazione predefinita, scegli la scheda Allarmi.

   Nella tabella Allarmi, puoi identificare gli allarmi consigliati utilizzando quanto segue:

   - Nome: nome dell'allarme che hai impostato per l'applicazione.
   - Descrizione: descrive l'obiettivo dell'allarme.
   - Stato: indica lo stato attuale di implementazione degli CloudWatch allarmi Amazon.

     Questa colonna mostra uno dei seguenti valori:

- Implementato: indica che gli allarmi consigliati da AWS Resilience Hub sono implementati nell'applicazione. Scegliendo il numero seguente, la tabella Allarmi verrà filtrata per visualizzare tutti gli allarmi consigliati implementati nell'applicazione.
- Non implementato: indica che gli allarmi consigliati da AWS Resilience Hub sono inclusi ma non implementati nell'applicazione. Scegliendo il numero seguente, la tabella Allarmi verrà filtrata per visualizzare tutti gli allarmi consigliati che non sono implementati nell'applicazione.
- Escluso: indica che gli allarmi consigliati da AWS Resilience Hub sono esclusi dall'applicazione. Scegliendo il numero seguente, la tabella Allarmi verrà filtrata per visualizzare tutti gli allarmi consigliati esclusi dall'applicazione. Per ulteriori informazioni sull'inclusione e l'esclusione degli allarmi consigliati, consulta Inclusione o esclusione dei consigli operativi.
- Inattivo: indica che gli allarmi sono distribuiti su Amazon CloudWatch, ma lo stato è impostato su _ INSUFFICIENTin DATA Amazon. CloudWatch Scegliendo il numero seguente, la tabella Allarmi verrà filtrata per visualizzare tutti gli allarmi implementati e non attivi.

- Configurazione: indica se ci sono dipendenze di configurazione in sospeso che devono essere risolte.
- Tipo: indica il tipo di allarme.
- AppComponent— Indica i componenti dell'applicazione (AppComponents) associati a questo allarme.
- ID di riferimento: indica l'identificatore logico dell'evento AWS CloudFormation stack in. AWS CloudFormation
- ID di raccomandazione: indica l'identificatore logico della risorsa dello AWS CloudFormation stack in. AWS CloudFormation

7. Nella scheda Allarmi, per filtrare i consigli sugli allarmi nella tabella Allarmi in base a uno stato specifico, seleziona un numero al di sotto dello stesso.
8. Seleziona gli allarmi consigliati che desideri configurare per la tua applicazione e scegli Crea modello. CloudFormation
9. Nella finestra di dialogo Crea CloudFormation modello, puoi utilizzare il nome generato automaticamente oppure puoi inserire un nome per il AWS CloudFormation modello nella casella del nome del CloudFormation modello.
10. Scegli Create (Crea) . Questa operazione può richiedere fino a qualche minuto per creare il AWS CloudFormation modello.

Completate la procedura seguente per includere i consigli nella vostra base di codice.

Per includere i AWS Resilience Hub consigli nella tua base di codice

1. Scegli la scheda Modelli per visualizzare il modello appena creato. Puoi identificare i tuoi modelli utilizzando quanto segue:
   - Nome: nome della valutazione che avevi fornito al momento della creazione.
   - Stato: indica lo stato di esecuzione della valutazione.
   - Tipo: indica il tipo di raccomandazione operativa.
   - Formato: indica il formato (JSON/testo) in cui viene creato il modello.
   - Ora di inizio: indica l'ora di inizio della valutazione.
   - Ora di fine: indica l'ora di fine della valutazione.
   - ARN— Il ARN modello
2. In Dettagli modello, scegli il link sotto Templates S3 Path per aprire l'oggetto modello nella console Amazon S3.
3. Nella console Amazon S3, dalla tabella Oggetti, scegli il collegamento alla SOP cartella.
4. Per copiare il percorso Amazon S3, seleziona la casella di controllo davanti al JSON file e scegli Copia. URL
5. Crea uno AWS CloudFormation stack dalla AWS CloudFormation console. Per ulteriori informazioni sulla creazione di uno AWS CloudFormation stack, consulta. https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-console-create-stack.html

   Durante la creazione AWS CloudFormation dello stack, devi fornire il percorso Amazon S3 che hai copiato dal passaggio precedente.

Visualizzazione degli allarmi

Puoi visualizzare tutti gli allarmi attivi che hai configurato per monitorare la resilienza delle tue applicazioni. AWS Resilience Hub utilizza AWS CloudFormation un modello per memorizzare i dettagli degli allarmi che viene a sua volta utilizzato per creare gli allarmi in Amazon. CloudWatch Puoi accedere al AWS CloudFormation modello utilizzando Amazon S3URL, scaricarlo e inserirlo nella tua pipeline di codice o creare uno stack tramite la console. AWS CloudFormation

Per visualizzare gli allarmi dalla dashboard, scegli Dashboard dal menu di navigazione a sinistra. Nella tabella Allarmi implementati, puoi identificare gli allarmi implementati utilizzando le seguenti informazioni:

- Applicazione interessata: nome delle applicazioni che hanno implementato questo allarme.
- Allarmi attivi: indica il numero di allarmi attivi attivati dalle applicazioni.
- FISin corso: indica l' AWS FIS esperimento attualmente in esecuzione per l'applicazione.

Per visualizzare gli allarmi implementati nell'applicazione

1. Nel menu di navigazione a sinistra, scegli Applicazioni.
2. Seleziona un'applicazione dalla tabella Applicazioni.
3. Nella pagina di riepilogo dell'applicazione, la tabella Allarmi implementati mostra tutti gli allarmi consigliati implementati nell'applicazione.

   Per trovare un allarme specifico nella tabella Allarmi implementati, nella casella Trova allarmi per testo, proprietà o valore, seleziona uno dei seguenti campi, scegli un'operazione e quindi digita un valore.

   - Nome dell'allarme: nome dell'allarme che hai impostato per l'applicazione.
   - Descrizione: descrive l'obiettivo dell'allarme.
   - Stato: indica lo stato di implementazione corrente dell' CloudWatch allarme Amazon.

     Questa colonna mostra uno dei seguenti valori:

     - Implementato: indica che gli allarmi consigliati da AWS Resilience Hub sono implementati nell'applicazione. Scegli il numero seguente per visualizzare tutti gli allarmi consigliati e implementati nella scheda Raccomandazioni operative.
     - Non implementato: indica che gli allarmi consigliati da AWS Resilience Hub sono inclusi ma non implementati nell'applicazione. Scegli il numero seguente per visualizzare tutti gli allarmi consigliati e non implementati nella scheda Raccomandazioni operative.
     - Escluso: indica che gli allarmi consigliati da AWS Resilience Hub sono esclusi dall'applicazione. Scegli il numero seguente per visualizzare tutti gli allarmi consigliati ed esclusi nella scheda Raccomandazioni operative. Per ulteriori informazioni sull'inclusione e l'esclusione degli allarmi consigliati, consulta Inclusione o esclusione dei consigli operativi.

    - Inattivo: indica che gli allarmi sono distribuiti su Amazon CloudWatch, ma lo stato è impostato su _ INSUFFICIENTin DATA Amazon. CloudWatch Scegli il numero seguente per visualizzare tutti gli allarmi implementati e inattivi nella scheda Raccomandazioni operative.
  - Modello di origine: fornisce l'Amazon Resource Name (ARN) dello AWS CloudFormation stack che contiene i dettagli dell'allarme.
  - Risorsa: mostra le risorse a cui questo allarme è collegato e per cui è stato implementato.
  - Metrica: visualizza la CloudWatch metrica Amazon assegnata all'allarme. Per ulteriori informazioni sui parametri di Amazon, consulta Amazon CloudWatch CloudWatch Metrics.
  - Ultima modifica: mostra la data e l'ora dell'ultima modifica di un allarme.

Per visualizzare gli allarmi consigliati dalle valutazioni

1. Nel menu di navigazione a sinistra, scegli Applicazioni.
2. Seleziona un'applicazione dalla tabella Applicazioni.

   Per trovare un'applicazione, immettete il nome dell'applicazione nella casella Trova applicazioni.
3. Scegli la scheda Valutazioni.

   Nella tabella delle valutazioni della resilienza, puoi identificare le tue valutazioni utilizzando le seguenti informazioni:

   - Nome: nome della valutazione che avevi fornito al momento della creazione.
   - Stato: indica lo stato di esecuzione della valutazione.
   - Stato di conformità: indica se la valutazione è conforme alla politica di resilienza.
   - Stato di variazione della resilienza: indica se la domanda si è allontanata o meno dalla precedente valutazione positiva.
   - Versione dell'app: versione dell'applicazione.
   - Invoker: indica il ruolo che ha richiamato la valutazione.
   - Ora di inizio: indica l'ora di inizio della valutazione.
   - Ora di fine: indica l'ora di fine della valutazione.
   - ARN— L'Amazon Resource Name (ARN) della valutazione.
4. Seleziona una valutazione dalla tabella delle valutazioni della resilienza.
5. Scegli la scheda Raccomandazioni operative.
6. Se non è selezionata per impostazione predefinita, scegli la scheda Allarmi.

Nella tabella Allarmi, puoi identificare gli allarmi consigliati utilizzando quanto segue:

- Nome: nome dell'allarme che hai impostato per l'applicazione.
- Descrizione: descrive l'obiettivo dell'allarme.
- Stato: indica lo stato attuale di implementazione degli CloudWatch allarmi Amazon.

  Questa colonna mostra uno dei seguenti valori:

  - Implementato: indica che l'allarme è implementato nell'applicazione. Scegliendo il numero seguente, la tabella Allarmi verrà filtrata per visualizzare tutti gli allarmi consigliati implementati nell'applicazione.
  - Non implementato: indica che l'allarme non è implementato o incluso nell'applicazione. Scegliendo il numero seguente, la tabella Allarmi verrà filtrata per visualizzare tutti gli allarmi consigliati che non sono implementati nell'applicazione.
  - Escluso: indica che l'allarme è escluso dall'applicazione. Scegliendo il numero seguente, la tabella Allarmi verrà filtrata per visualizzare tutti gli allarmi consigliati esclusi dall'applicazione. Per ulteriori informazioni sull'inclusione e l'esclusione degli allarmi consigliati, consulta. the section called “Inclusione o esclusione di raccomandazioni operative”
  - Inattivo: indica che gli allarmi sono distribuiti su Amazon CloudWatch, ma lo stato è impostato su _ INSUFFICIENTin DATA Amazon. CloudWatch Scegliendo il numero seguente, la tabella Allarmi verrà filtrata per visualizzare tutti gli allarmi implementati e non attivi.
- Configurazione: indica se ci sono dipendenze di configurazione in sospeso che devono essere risolte.
- Tipo: indica il tipo di allarme.
- AppComponent— Indica i componenti dell'applicazione (AppComponents) associati a questo allarme.
- ID di riferimento: indica l'identificatore logico dell'evento AWS CloudFormation stack in. AWS CloudFormation
- ID di raccomandazione: indica l'identificatore logico della risorsa dello AWS CloudFormation stack in. AWS CloudFormation

Gestione delle procedure operative standard

Una procedura operativa standard (SOP) è una serie di passaggi prescrittivi progettati per ripristinare in modo efficiente l'applicazione in caso di interruzione o allarme. Preparate, testate e misurate le SOP in anticipo per garantire un ripristino tempestivo in caso di interruzione operativa.

In base ai componenti dell'applicazione, AWS Resilience Hub consiglia le SOP da preparare. AWS Resilience Hub collabora con Systems Manager per automatizzare i passaggi delle SOP fornendo una serie di documenti SSM che è possibile utilizzare come base per tali SOP.

Ad esempio, AWS Resilience Hub può consigliare una SOP per aggiungere spazio su disco sulla base di un documento di automazione SSM esistente. Per eseguire questo documento SSM, è necessario un ruolo IAM specifico con le autorizzazioni corrette. AWS Resilience Hub crea metadati nell'applicazione che indicano quale documento di automazione SSM eseguire in caso di carenza di dischi e quale ruolo IAM è necessario per eseguire quel documento SSM. Questi metadati vengono quindi salvati in un parametro SSM.

Oltre a configurare l'automazione SSM, è consigliabile testarla con un esperimento. AWS FIS Pertanto, fornisce AWS Resilience Hub anche un AWS FIS esperimento che richiama il documento di automazione SSM: in questo modo, puoi testare in modo proattivo l'applicazione per assicurarti che il SOP che hai creato esegua il lavoro previsto.

AWS Resilience Hub fornisce i consigli sotto forma di un AWS CloudFormation modello che è possibile aggiungere alla base di codice dell'applicazione. Questo modello fornisce:

- Il ruolo IAM con le autorizzazioni necessarie per eseguire la SOP.
- Un AWS FIS esperimento che puoi usare per testare la SOP.
- Un parametro SSM che contiene i metadati dell'applicazione che indicano quale documento SSM e quale ruolo IAM deve essere eseguito come SOP e su quale risorsa. Ad esempio: `$(DocumentName) for SOP $(HandleCrisisA) on $(ResourceA)`.

La creazione di un SOP può richiedere alcuni tentativi ed errori. L'esecuzione di una valutazione della resilienza rispetto all'applicazione e la generazione di un AWS CloudFormation modello in base ai AWS Resilience Hub consigli sono un buon inizio. Utilizzate il AWS CloudFormation modello per generare uno AWS CloudFormation stack, quindi utilizzate i parametri SSM e i relativi valori predefiniti nella SOP. Esegui il SOP e scopri quali perfezionamenti devi apportare.

Poiché tutte le applicazioni hanno requisiti diversi, l'elenco predefinito di documenti SSM AWS Resilience Hub fornito non sarà sufficiente per tutte le esigenze. Tuttavia, puoi copiare i documenti SSM predefiniti e utilizzarli come base per creare documenti personalizzati su misura per la tua applicazione. Puoi anche creare i tuoi documenti SSM completamente nuovi. Se crei i tuoi documenti SSM invece di modificare i valori predefiniti, devi associarli ai parametri SSM, in modo che il documento SSM corretto venga chiamato quando viene eseguito il SOP.

Dopo aver finalizzato la SOP creando i documenti SSM necessari e aggiornando le associazioni di parametri e documenti secondo necessità, aggiungi i documenti SSM direttamente alla tua base di codice e apporta eventuali modifiche o personalizzazioni successive. In questo modo, ogni volta che distribuisci la tua applicazione, implementerai anche la maggior parte delle SOP. up-to-date

Argomenti

Creazione di una SOP basata sui consigli AWS Resilience Hub

Per creare una SOP basata sui AWS Resilience Hub consigli, è necessaria un' AWS Resilience Hub applicazione a cui è associata una politica di resilienza e deve aver eseguito una valutazione della resilienza rispetto a tale applicazione. La valutazione della resilienza genera i consigli per la SOP.

Per creare una SOP basata sui AWS Resilience Hub consigli, è necessario creare un AWS CloudFormation modello per le SOP consigliate e includerle nella base di codice.

Crea un AWS CloudFormation modello per i consigli SOP

1. Apri la AWS Resilience Hub console.
2. Nel riquadro di navigazione, scegliere Applications (Applicazioni).
3. Dall'elenco delle applicazioni, scegli l'applicazione per cui desideri creare una SOP.
4. Scegli la scheda Valutazioni.

5. Seleziona una valutazione dalla tabella delle valutazioni della resilienza. Se non disponi di una valutazione, completa la procedura riportata in the section called “Esecuzione di valutazioni della resilienza” e poi torna a questo passaggio.
6. In Raccomandazioni operative, scegli Procedure operative standard.
7. Seleziona tutti i consigli SOP che desideri includere.
8. Scegli Crea CloudFormation modello. Questa operazione può richiedere fino a qualche minuto per creare il AWS CloudFormation modello.

   Completate la procedura seguente per includere i consigli SOP nella vostra base di codice.

Per includere i AWS Resilience Hub consigli nella tua base di codice

1. In Raccomandazioni operative, scegli Modelli.
2. Nell'elenco dei modelli, scegli il nome del modello SOP che hai appena creato.

   È possibile identificare le SOP implementate nell'applicazione utilizzando le seguenti informazioni:

   - Nome SOP: nome del SOP definito per l'applicazione.
   - Descrizione: descrive l'obiettivo della SOP.
   - Documento SSM: URL Amazon S3 del documento SSM che contiene la definizione SOP.
   - Esecuzione del test: URL Amazon S3 del documento che contiene i risultati del test più recente.
   - Modello di origine: fornisce l'Amazon Resource Name (ARN) dello AWS CloudFormation stack che contiene i dettagli SOP.
3. In Dettagli modello, scegli il link in Templates S3 Path per aprire l'oggetto modello nella console Amazon S3.
4. Nella console Amazon S3, dalla tabella Oggetti, scegli il collegamento alla cartella SOP.
5. Per copiare il percorso Amazon S3, seleziona la casella di controllo davanti al file JSON e scegli Copia URL.
6. Crea uno AWS CloudFormation stack dalla console. AWS CloudFormation Per ulteriori informazioni sulla creazione di uno AWS CloudFormation stack, consulta. https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-console-create-stack.html

Durante la creazione AWS CloudFormation dello stack, devi fornire il percorso Amazon S3 che hai copiato dal passaggio precedente.

Creazione di un documento SSM personalizzato

Per automatizzare completamente il ripristino dell'applicazione, potrebbe essere necessario creare un documento SSM personalizzato per la SOP nella console Systems Manager. È possibile modificare un documento SSM esistente come base oppure creare un nuovo documento SSM.

Per informazioni dettagliate sull'utilizzo di Systems Manager per creare un documento SSM, vedere Procedura dettagliata: utilizzo di Document Builder per creare un runbook personalizzato.

Per informazioni sulla sintassi dei documenti SSM, vedere Sintassi del documento SSM.

Per informazioni sull'automazione delle azioni dei documenti SSM, vedere il riferimento alle azioni di automazione di Systems Manager.

Utilizzo di un documento SSM personalizzato anziché quello predefinito

Per sostituire il documento SSM AWS Resilience Hub suggerito per il tuo SOP con un documento personalizzato che hai creato, lavora direttamente nella tua base di codice. Oltre ad aggiungere il tuo nuovo documento di automazione SSM personalizzato, potrai anche:

1. Aggiungi le autorizzazioni IAM necessarie per eseguire l'automazione.
2. Aggiungi un AWS FIS esperimento per testare il tuo documento SSM.
3. Aggiungi un parametro SSM che punti al documento di automazione che desideri utilizzare come SOP.

In genere, è più efficiente utilizzare i valori predefiniti suggeriti AWS Resilience Hub e personalizzarli secondo necessità. Ad esempio, aggiungi o rimuovi le autorizzazioni necessarie per il ruolo IAM, modifica la configurazione dell' AWS FIS esperimento in modo che punti al nuovo documento SSM o modifica il parametro SSM in modo che punti al tuo nuovo documento SSM.

Test delle SOP

Come accennato in precedenza, è consigliabile aggiungere AWS FIS esperimenti alle pipeline CI/CD per testare regolarmente le SOP, in modo da garantire che siano pronte all'uso in caso di interruzione.

Verifica sia le SOP fornite che quelle personalizzate AWS Resilience Hub.

Visualizzazione delle procedure operative standard

Per visualizzare le SOP implementate dalle applicazioni

1. Nel menu di navigazione a sinistra, scegli Applicazioni.
2. In Applicazioni, apri un'applicazione.
3. Scegli la scheda Procedure operative standard.

   Nella sezione di riepilogo delle procedure operative standard, la tabella Procedure operative standard implementate mostra l'elenco delle SOP generate dai consigli SOP.

   È possibile identificare le SOP in base a quanto segue:

   - Nome SOP: nome del SOP definito per l'applicazione.
   - Documento SSM: URL S3 del documento Amazon EC2 Systems Manager che contiene la definizione SOP.
   - Descrizione: descrive l'obiettivo della SOP.
   - Esecuzione del test: URL S3 del documento che contiene i risultati del test più recente.
   - ID di riferimento: identificatore della raccomandazione SOP a cui si fa riferimento.
   - ID risorsa: identificatore della risorsa per la quale è implementata la raccomandazione SOP.

Per visualizzare le SOP consigliate dalle valutazioni

1. Nel menu di navigazione a sinistra, scegli Applicazioni.
2. Seleziona un'applicazione dalla tabella Applicazioni.

   Per trovare un'applicazione, immettete il nome dell'applicazione nella casella Trova applicazioni.
3. Scegli la scheda Valutazioni.

   Nella tabella delle valutazioni della resilienza, puoi identificare le tue valutazioni utilizzando le seguenti informazioni:

   - Nome: nome della valutazione che avevi fornito al momento della creazione.
   - Stato: indica lo stato di esecuzione della valutazione.
   - Stato di conformità: indica se la valutazione è conforme alla politica di resilienza.

- Stato di variazione della resilienza: indica se la domanda si è allontanata o meno dalla precedente valutazione positiva.
- Versione dell'app: versione dell'applicazione.
- Invoker: indica il ruolo che ha richiamato la valutazione.
- Ora di inizio: indica l'ora di inizio della valutazione.
- Ora di fine: indica l'ora di fine della valutazione.
- ARN: Amazon Resource Name (ARN) della valutazione.

4. Seleziona una valutazione dalla tabella delle valutazioni della resilienza.
5. Scegli la scheda Raccomandazioni operative.
6. Scegli la scheda Procedure operative standard.

   Nella tabella Procedure operative standard, è possibile ottenere ulteriori informazioni sulle SOP consigliate utilizzando le seguenti informazioni:

   - Nome: nome della SOP consigliata.
   - Descrizione: descrive l'obiettivo della SOP.
   - Stato: indica lo stato di implementazione corrente della SOP. Ovvero, implementato, non implementato ed escluso.
   - Configurazione: indica se ci sono dipendenze di configurazione in sospeso che devono essere risolte.
   - Tipo: indica il tipo di SOP.
   - AppComponent— Indica i componenti dell'applicazione (AppComponents) associati a questa SOP. Per ulteriori informazioni sulle risorse supportate AppComponents, vedere Raggruppamento delle risorse in un. AppComponent
   - ID di riferimento: indica l'identificatore logico dell'evento AWS CloudFormation stack in. AWS CloudFormation
   - ID di raccomandazione: indica l'identificatore logico della risorsa dello AWS CloudFormation stack in. AWS CloudFormation

Gestione degli esperimenti di Amazon Fault Injection Service

Questa sezione descrive come creare ed eseguire esperimenti su Amazon Fault Injection Service (AWS FIS) in AWS Resilience Hub. Esegui AWS FIS esperimenti per misurare la resilienza delle tue

AWS risorse e la quantità di tempo necessaria per il ripristino da applicazioni, infrastrutture, zone di disponibilità e Regione AWS incidenti.

Per misurare la resilienza, questi AWS FIS esperimenti simulano interruzioni delle risorse. AWS Esempi di interruzioni includono errori di rete non disponibili, failover, processi interrotti su Amazon EC2 o AWS ASG, ripristino all'avvio in Amazon RDS e problemi con la zona di disponibilità. Al termine dell' AWS FIS esperimento, puoi stimare se un'applicazione è in grado di ripristinare i tipi di interruzione definiti nell'obiettivo RTO della politica di resilienza.

Tutti gli esperimenti AWS Resilience Hub sono costruiti utilizzando AWS FIS ed eseguono azioni. AWS FIS La maggior parte degli AWS FIS esperimenti richiama azioni di automazione di Systems Manager per eseguire interruzioni e monitorare gli allarmi, mentre altri AWS FIS esperimenti utilizzano solo azioni di AWS FIS automazione personalizzate per AWS servizi specifici (come l'azione di Amazon EKS). Per ulteriori informazioni sulle AWS FIS azioni, consulta il riferimento alle azioni.AWS FIS

Puoi utilizzare gli AWS FIS esperimenti nel loro stato predefinito o personalizzarli in base alle tue esigenze. AWS FIS è possibile accedere agli esperimenti da AWS Resilience Hub (the section called “Visualizzazione degli esperimenti di iniezione dei guasti”) o AWS FIS console (AWS FIS).

Argomenti

- Creazione di AWS FIS esperimenti sulla base delle raccomandazioni operative
- Esecuzione di un esperimento da AWS FISAWS Resilience Hub
- Visualizzazione degli esperimenti di iniezione dei guasti
- Errori/controllo dello stato dell'esperimento Amazon Fault Injection Service

Creazione di AWS FIS esperimenti sulla base delle raccomandazioni operative

AWS Resilience Hub consiglia di testare l'applicazione dopo aver eseguito un rapporto di valutazione. È possibile accedere ed eseguire questi esperimenti dal rapporto di valutazione dell'applicazione.

AWS Resilience Hub fornisce un elenco di AWS FIS esperimenti, che sono documenti di Systems Manager con parametri di test. Quando selezionate un AWS FIS esperimento dall'elenco, AWS Resilience Hub crea un AWS CloudFormation modello con i parametri definiti nel documento Systems Manager. Dopo la creazione dello AWS CloudFormation stack, è possibile visualizzare gli AWS FIS esperimenti predisposti per l'applicazione.

Il AWS CloudFormation modello è costituito da un ruolo IAM per ogni documento Systems Manager, con le autorizzazioni minime richieste per l'esecuzione.

Per creare un AWS FIS esperimento basato sui AWS Resilience Hub consigli, devi creare un AWS CloudFormation modello per i test consigliati e includerli nella tua base di codice.

Per creare un AWS CloudFormation modello per l' AWS FIS esperimento

1. Apri la AWS Resilience Hub console.
2. Nel riquadro di navigazione, scegliere Applications (Applicazioni).
3. Dall'elenco delle applicazioni, scegli l'applicazione per cui desideri creare un test.
4. Scegli la scheda Valutazioni.
5. Seleziona una valutazione dalla tabella delle valutazioni della resilienza. Se non disponi di una valutazione, completa la procedura riportata in the section called “Esecuzione di valutazioni della resilienza” e poi torna a questo passaggio.
6. In Raccomandazioni operative, scegli Esperimenti di iniezione in caso di guasto.
7. Seleziona tutti i test che desideri includere.
8. Scegli Crea CloudFormation modello. Questa operazione può richiedere alcuni minuti per creare il AWS CloudFormation modello.
9. Scegliere Templates (Modelli).

   È possibile visualizzare il AWS CloudFormation modello appena creato nella tabella Modelli.

   Completate la procedura seguente per includere i consigli nella vostra base di codice.

Per includere i AWS Resilience Hub consigli nella tua base di codice

1. In Consigli operativi, scegli Modelli.
2. Nell'elenco dei modelli, scegli il nome del modello di AWS FIS esperimento che hai appena creato.

   È possibile identificare i test implementati nell'applicazione utilizzando le seguenti informazioni:

   - Nome del test: nome del test che avete creato per l'applicazione.
   - Descrizione: descrive l'obiettivo del test.
   - Stato: indica lo stato di implementazione corrente del test.

Questa colonna mostra uno dei seguenti valori:

- Implementato: indica che il test è implementato nell'applicazione.
- Non implementato: indica che il test non è implementato o incluso nell'applicazione.
- Escluso: indica che il test è escluso dall'applicazione.
- Inattivo: indica che il test è stato distribuito AWS FIS, ma non è stato eseguito negli ultimi 30 giorni.

- Esecuzione del test: URL Amazon S3 del documento che contiene i risultati del test più recente.
- Modello di origine: fornisce l'Amazon Resource Name (ARN) dello AWS CloudFormation stack che contiene i dettagli dell'esperimento.

3. In Dettagli modello, scegli il link in Templates S3 Path per aprire l'oggetto modello nella console Amazon S3.
4. Nella console Amazon S3, dalla tabella Oggetti, scegli il collegamento alla cartella di test.
5. Per copiare il percorso Amazon S3, seleziona la casella di controllo davanti al file JSON e scegli Copia URL.
6. Crea uno AWS CloudFormation stack dalla console. AWS CloudFormation Per ulteriori informazioni sulla creazione di uno AWS CloudFormation stack, consulta. https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-console-create-stack.html

   Durante la creazione AWS CloudFormation dello stack, devi fornire il percorso Amazon S3 che hai copiato dal passaggio precedente.

Esecuzione di un esperimento da AWS FISAWS Resilience Hub

Nella tua applicazione, devi prima creare un modello di AWS FIS esperimento in base ai consigli operativi prima di AWS Resilience Hub poter eseguire l' AWS FIS esperimento.

Per iniziare un AWS FIS esperimento

1. Nel menu di navigazione a sinistra, scegli Applicazioni.
2. Dalla tabella Applicazioni, apri un'applicazione.
3. Scegli la scheda Esperimenti di Fault injection.

4. Seleziona il pulsante di opzione prima del modello di esperimento utilizzato per creare l'esperimento che desideri eseguire dalla tabella Modelli di esperimento, quindi scegli Avvia esperimento.

Per interrompere un AWS FIS esperimento

1. Nel menu di navigazione a sinistra, scegli Applicazioni.
2. Dalla tabella Applicazioni, apri un'applicazione.
3. Scegli la scheda Esperimenti di Fault injection.
4. Seleziona il pulsante di opzione prima dell'esperimento dalla tabella Esperimento, quindi scegli Interrompi esperimento.

Visualizzazione degli esperimenti di iniezione dei guasti

In AWS Resilience Hub, visualizza gli AWS FIS esperimenti che hai impostato per misurare la resilienza delle tue AWS risorse e la quantità di tempo necessaria per il ripristino dall'applicazione, dall'infrastruttura, dalla zona di disponibilità e dagli incidenti. Regione AWS

Per visualizzare AWS FIS gli esperimenti dalla dashboard, scegli Dashboard dal menu di navigazione a sinistra. Nella tabella Esperimenti, puoi identificare gli AWS FIS esperimenti implementati utilizzando le seguenti informazioni:

- ID esperimento: identificatore dell' AWS FIS esperimento.
- ID del modello di esperimento: identificatore del modello di AWS FIS esperimento utilizzato per creare l' AWS FIS esperimento.
- Modello di origine: fornisce l'Amazon Resource Name (ARN) dello AWS CloudFormation stack che contiene i dettagli dell'esperimento. AWS FIS
- Stato: indica se l' AWS FIS esperimento è stato completato con successo o meno.

Per visualizzare gli AWS FIS esperimenti implementati dalle applicazioni

1. Nel menu di navigazione a sinistra, scegli Applicazioni.
2. Dalla tabella Applicazioni, apri un'applicazione.
3. Scegliete Esperimenti di iniezione di errori.
4. Scegli la scheda Esperimento.

Nella scheda Esperimento, puoi vedere un elenco di AWS FIS esperimenti attivi nella tabella Esperimento.

Nella tabella Esperimenti, puoi identificare l' AWS FIS esperimento implementato utilizzando le seguenti informazioni:

- Nome del test: nome del test consigliato da AWS Resilience Hub utilizzato per creare l' AWS FIS esperimento.
- ID dell'esperimento: identificatore dell' AWS FIS esperimento.
- Descrizione: descrive l'obiettivo dell' AWS FIS esperimento.
- Ora di creazione: data e ora in cui è stato creato l' AWS FIS esperimento.
- Ora dell'ultimo aggiornamento: data e ora dell'ultimo aggiornamento dell' AWS FIS esperimento.
- Modello di origine: fornisce l'Amazon Resource Name (ARN) dello AWS CloudFormation stack che contiene i dettagli dell'esperimento. AWS FIS

Per visualizzare gli esperimenti consigliati dalle valutazioni

1. Nel menu di navigazione a sinistra, scegli Applicazioni.
2. Seleziona un'applicazione dalla tabella Applicazioni.

   Per trovare un'applicazione, immettete il nome dell'applicazione nella casella Trova applicazioni.
3. Scegli la scheda Valutazioni.

   Nella tabella delle valutazioni della resilienza, puoi identificare le tue valutazioni utilizzando le seguenti informazioni:

   - Nome: nome della valutazione che avevi fornito al momento della creazione.
   - Stato: indica lo stato di esecuzione della valutazione.
   - Stato di conformità: indica se la valutazione è conforme alla politica di resilienza.
   - Stato di variazione della resilienza: indica se la domanda si è allontanata o meno dalla precedente valutazione positiva.
   - Versione dell'app: versione dell'applicazione.
   - Invoker: indica il ruolo che ha richiamato la valutazione.
   - Ora di inizio: indica l'ora di inizio della valutazione.

- Ora di fine: indica l'ora di fine della valutazione.
- ARN: Amazon Resource Name (ARN) della valutazione.

4. Seleziona una valutazione dalla tabella delle valutazioni della resilienza.
5. Scegli la scheda Raccomandazioni operative.
6. Scegli la scheda Esperimenti di iniezione di guasto.

   Nella tabella dei modelli di sperimentazione di Fault injection, puoi comprendere meglio i test consigliati utilizzando le seguenti informazioni:

   - Nome: nome del test consigliato.
   - Descrizione: descrive l'obiettivo del test.
   - Stato: indica lo stato di implementazione corrente del test.

     Questa colonna mostra uno dei seguenti valori:

     - Implementato: indica che il test è implementato nell'applicazione.
     - Non implementato: indica che il test non è implementato o incluso nell'applicazione.
     - Escluso: indica che il test è escluso dall'applicazione.
     - Inattivo: indica che il test è stato distribuito AWS FIS, ma non è stato eseguito negli ultimi 30 giorni.
   - Configurazione: indica se ci sono dipendenze di configurazione in sospeso che devono essere risolte.
   - Tipo: indica il tipo di test.
   - AppComponent— Indica i componenti dell'applicazione (AppComponents) associati a questo test. Per ulteriori informazioni sulle risorse supportate AppComponents, vedere Raggruppamento delle risorse in un AppComponent.
   - Rischio: indica il livello di rischio del fallimento del test. I livelli di rischio sono indicati utilizzando Alto, Medio e Basso per indicare rispettivamente i livelli di rischio alto, moderato e basso.
   - ID di riferimento: indica l'identificatore logico dell'evento AWS CloudFormation stack in. AWS CloudFormation
   - ID di raccomandazione: indica l'identificatore logico della risorsa dello AWS CloudFormation stack in. AWS CloudFormation

Errori/controllo dello stato dell'esperimento Amazon Fault Injection Service

AWS Resilience Hub ti consente di tenere traccia dello stato dell'esperimento che hai iniziato. Per ulteriori informazioni, consulta la procedura Per visualizzare gli esperimenti consigliati tratti dalle valutazioni inthe section called “Visualizzazione degli esperimenti di iniezione dei guasti”.

Argomenti

- Analisi dell'esecuzione degli AWS FIS esperimenti con AWS Systems Manager
- AWS FIS sperimenta errori durante il test dei pod Kubernetes in esecuzione nei cluster Amazon Elastic Kubernetes Service

Analisi dell'esecuzione degli AWS FIS esperimenti con AWS Systems Manager

Dopo aver eseguito un AWS FIS esperimento, è possibile visualizzare i dettagli dell'esecuzione in AWS Systems Manager.

1. Vai a CloudTrail> Cronologia eventi.
2. Filtra gli eventi in base al nome utente utilizzando l'ID dell'esperimento.
3. Visualizza la StartAutomationExecution voce. L'ID della richiesta è l'ID di automazione SSM.
4. Accedere a AWS Systems Manager > Automation.
5. Filtra per ID di esecuzione utilizzando l'ID di automazione SSM e visualizza i dettagli dell'automazione.

   È possibile analizzare l'esecuzione con qualsiasi automazione di Systems Manager. Per ulteriori informazioni, consulta la guida per l'utente di AWS Systems Manager Automation. I parametri di input di esecuzione vengono visualizzati nella sezione Parametri di input di Execution Detail e includono parametri opzionali non presenti nell' AWS FIS esperimento.

   È possibile trovare informazioni sullo stato dei passaggi e altri dettagli dei passaggi approfondendo i passaggi specifici all'interno dei passaggi di esecuzione.

Errori comuni

Di seguito sono riportati gli errori più comuni riscontrati durante l'esecuzione di un rapporto di valutazione:

- Il modello di allarme non è stato distribuito prima dell'esecuzione dell'esperimento test/SOP. Ciò causa un messaggio di errore durante la fase di automazione.
  - Messaggio di errore: `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.`
  - Correzione: assicurati di attivare l'allarme pertinente e di implementare il modello risultante prima di eseguire nuovamente l'esperimento di iniezione dei guasti.
- Autorizzazioni mancanti nel ruolo di esecuzione. Questo messaggio di errore si verifica se al ruolo di esecuzione fornito manca un'autorizzazione e viene visualizzato nei dettagli del passaggio.
  - Messaggio di errore:`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`.
  - Correzione: verifica di aver fornito il ruolo di esecuzione corretto. In tal caso, aggiungi l'autorizzazione richiesta ed esegui nuovamente la valutazione.
- L'esecuzione è riuscita ma non ha prodotto il risultato previsto. Questo è il risultato di parametri errati o di un problema interno di automazione.
  - Messaggio di errore: l'esecuzione è riuscita, quindi non viene visualizzato alcun messaggio di errore.
  - Correzione: controllate i parametri di input e osservate i passaggi eseguiti come spiegato nell'esecuzione dell' AWS FIS esperimento Analyze prima di esaminare i singoli passaggi per individuare gli input e gli output previsti.

AWS FIS sperimenta errori durante il test dei pod Kubernetes in esecuzione nei cluster Amazon Elastic Kubernetes Service

Di seguito sono riportati gli errori più comuni di Amazon Elastic Kubernetes Service (Amazon EKS) riscontrati durante il test dei pod Kubernetes in esecuzione nei cluster Amazon EKS:

- Configurazione errata dei ruoli IAM per gli esperimenti o l'account di servizio Kubernetes. AWS FIS
  - Messaggi di errore:
    - `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.`
  - Correzione: verificare quanto segue.
    - Assicurati di aver seguito le istruzioni riportate in Utilizzare le AWS FIS`aws:eks:pod` azioni.
    - Assicurati di aver creato e configurato un account di servizio Kubernetes con le autorizzazioni RBAC necessarie e lo spazio dei nomi corretto.
    - Assicurati di aver mappato il ruolo IAM fornito (vedi l'output dello AWS CloudFormation stack del test) all'utente Kubernetes.
- Impossibile avviare AWS FIS Pod: è stato raggiunto il numero massimo di contenitori sidecar guasti. Questo di solito accade quando la memoria non è sufficiente per far funzionare il contenitore del AWS FIS sidecar.
  - Messaggio di errore:`Unable to heartbeat FIS Pod: Max failed sidecar containers reached.`
  - Correzione: un'opzione per evitare questo errore consiste nel ridurre la percentuale di carico di destinazione da allineare alla memoria o alla CPU disponibili.
- L'asserzione dell'allarme non è riuscita all'inizio dell'esperimento. Questo errore si verifica perché l'allarme correlato non ha un datapoint.
  - Messaggio di errore:. `Assertion failed for the following alarms` Elenca tutti gli allarmi per i quali l'asserzione ha avuto esito negativo.
  - Correzione: assicurati che Container Insights sia installato correttamente per gli allarmi e che l'allarme non sia acceso (in stato). `ALARM`

Comprendere i punteggi di resilienza

Questa sezione descrive come AWS Resilience Hub quantifica la prontezza delle applicazioni in base a diversi scenari di interruzione.

AWS Resilience Hub fornisce un punteggio di resilienza che rappresenta lo stato di resilienza dell'applicazione. Questo punteggio riflette la precisione con cui l'applicazione segue i nostri consigli per soddisfare la politica di resilienza, gli allarmi, le procedure operative standard () SOPs e i test dell'applicazione. In base al tipo di risorse utilizzate dall'applicazione, AWS Resilience Hub consiglia allarmi e una serie di test per ogni tipo di interruzione. SOPs

Il punteggio massimo di resilienza è di 100 punti. Per ottenere il miglior punteggio possibile o il punteggio massimo, è necessario implementare tutti gli allarmi e i SOPs test consigliati nell'applicazione. Ad esempio, AWS Resilience Hub consiglia un test con un allarme e unoSOP. Il test viene eseguito, attiva l'allarme e avvia quello associato. SOP Se funzionano correttamente e se l'applicazione soddisfa i criteri di resilienza, riceve un punteggio di resilienza vicino o uguale a 100 punti.

Dopo aver eseguito la prima valutazione, AWS Resilience Hub offre la possibilità di escludere i consigli operativi dall'applicazione. Per comprendere l'impatto dei consigli esclusi sul punteggio di resilienza, è necessario eseguire una nuova valutazione. Tuttavia, puoi sempre includere i consigli esclusi nella tua applicazione ed eseguire una nuova valutazione. Per ulteriori informazioni sull'inclusione e l'esclusione degli allarmi e sui consigli sui test, consultathe section called “Inclusione o esclusione di raccomandazioni operative”. SOP

Accesso al punteggio di resilienza delle applicazioni

È possibile visualizzare il punteggio di resilienza dell'applicazione scegliendo Dashboard o Applicazioni dal menu di navigazione.

Accesso al punteggio di resilienza da Dashboard

1. Nel menu di navigazione a sinistra, scegli Dashboard.
2. Nel punteggio di resilienza delle applicazioni nel tempo, scegli una o più applicazioni nell'elenco a discesa Scegli fino a 4 applicazioni.
3. Il grafico del punteggio di resilienza mostra il punteggio di resilienza per tutte le applicazioni scelte.

Accesso al punteggio di resilienza da Applications

1. Nel menu di navigazione a sinistra, scegli Applicazioni.
2. In Applicazioni, apri un'applicazione.
3. Scegli Riepilogo.

   Il grafico del punteggio di resilienza mostra l'andamento del punteggio di resilienza dell'applicazione per un massimo di un anno. AWS Resilience Hub mostra le azioni da intraprendere, le violazioni delle politiche di resilienza e le raccomandazioni operative che devono essere affrontate per migliorare e raggiungere il massimo punteggio di resilienza possibile utilizzando quanto segue:

- Per visualizzare le azioni che devono essere completate per migliorare e raggiungere il punteggio di resilienza massimo possibile, scegli la scheda Elementi d'azione. Se selezionata, AWS Resilience Hub visualizza quanto segue:
  - RTO/RPO— Indica il numero di tempi di ripristino (RTO/RPOs) che devono essere corretti per risolvere le violazioni della politica di resilienza dell'applicazione. Scegliete il valore per visualizzare iRTO/RPOdettagli nel rapporto di valutazione della vostra applicazione.
  - Allarmi: indica il numero di CloudWatch allarmi Amazon consigliati che devono essere implementati nella tua applicazione. Scegli il valore per visualizzare gli CloudWatch allarmi Amazon che devono essere corretti nel rapporto di valutazione della tua applicazione.
  - SOPs— Indica il numero di consigliati SOPs che devono essere implementati nella tua applicazione. Scegliete il valore da visualizzare SOPs che deve essere corretto nel rapporto di valutazione della vostra applicazione.
  - FIS— Indica il numero di test consigliati che devono essere implementati nell'applicazione. Scegliete il valore per visualizzare i test che devono essere corretti nel rapporto di valutazione della vostra applicazione.
- Per visualizzare il punteggio di ogni componente che influisce sul tuo punteggio di resilienza, scegli Score breakdown. Se selezionato, AWS Resilience Hub visualizza quanto segue:
  - RTO/RPOconformità: indica la conformità dei componenti delle applicazioni (AppComponents) ai tempi di ripristino stimati del carico di lavoro e ai tempi di ripristino target definiti nella politica di resilienza dell'applicazione. Scegliete il valore per visualizzare leRTO/RPOstime nel rapporto di valutazione della vostra applicazione.
  - Allarmi implementati: indica il contributo effettivo degli CloudWatch allarmi Amazon implementati rispetto al massimo contributo possibile al punteggio di resilienza dell'applicazione. Scegli il valore per visualizzare gli CloudWatch allarmi Amazon implementati nel rapporto di valutazione della tua applicazione.
  - SOPsimplementato: indica il contributo effettivo dell'implementazione SOPs rispetto al suo massimo contributo possibile al punteggio di resilienza dell'applicazione. Scegliete il valore per visualizzare l'implementazione SOPs nel rapporto di valutazione della vostra applicazione.
  - FISesperimenti implementati: indica il contributo effettivo dei test implementati rispetto al massimo contributo possibile al punteggio di resilienza dell'applicazione. Scegliete il valore per visualizzare i test implementati nel rapporto di valutazione della vostra applicazione.

- Per visualizzare le violazioni delle politiche di resilienza e le raccomandazioni operative, scegli la freccia destra per espandere la sezione Analisi delle violazioni delle politiche e delle raccomandazioni operative. Una volta espanso, visualizza quanto segue: AWS Resilience Hub
  - Violazioni delle politiche di resilienza: indica il numero di componenti dell'applicazione che violano la politica di resilienza dell'applicazione. Scegli il valore accanto RPO a RTO/per visualizzare i dettagli nella scheda Raccomandazioni sulla resilienza del rapporto di valutazione dell'applicazione.
  - Consigli operativi: indica i consigli operativi che non sono stati implementati o eseguiti per migliorare la resilienza dell'applicazione utilizzando le schede Eccezionale ed Escluso. Le raccomandazioni operative includono tutte le raccomandazioni che sono inattive e quelle che non sono state implementate.

    Per visualizzare i consigli operativi che devono essere implementati, scegli la scheda Eccezionale. Se selezionata, AWS Resilience Hub visualizza quanto segue:
    - Allarmi: indica il numero di CloudWatch allarmi Amazon consigliati che devono essere implementati.
    - SOPs— Indica il numero di consigliati SOPs che devono essere implementati.
    - FIS— Indica il numero di test consigliati che devono essere implementati.

    Per visualizzare i consigli operativi esclusi dall'applicazione, selezionare la scheda Esclusi. Se selezionata, AWS Resilience Hub visualizza quanto segue:
    - Allarmi: indica il numero di CloudWatch allarmi Amazon consigliati esclusi dall'applicazione.
    - SOPs— Indica il numero di avvisati SOPs che sono esclusi dalla tua applicazione.
    - FIS— Indica il numero di test consigliati esclusi dall'applicazione.

Calcolo dei punteggi di resilienza

Le tabelle di questa sezione spiegano le formule utilizzate da AWS Resilience Hub per determinare i componenti di punteggio di ciascun tipo di raccomandazione e il punteggio di resilienza dell'applicazione. Tutti i valori risultanti, determinati dai componenti di punteggio AWS Resilience Hub di ciascun tipo di raccomandazione e dal punteggio di resilienza dell'applicazione, vengono arrotondati al punto più vicino. Ad esempio, se fossero implementati due allarmi su tre, il punteggio sarebbe di 13,33 (2/3) * 20) punti. Questo valore verrà arrotondato a 13 punti. Per ulteriori

informazioni sui pesi utilizzati nelle formule all'interno delle tabelle, vedere the section called “Pesi e tipi di AppComponents interruzioni” la sezione.

Alcuni dei componenti del punteggio possono essere ottenuti solo tramite. `ScoringComponentResiliencyScore` API Per ulteriori informazioni su questo argomentoAPI, vedere ScoringComponentResiliencyScore.

Tabelle

- Formule per calcolare la componente di punteggio di ogni tipo di raccomandazione
- Formula per calcolare il punteggio di resilienza
- Formule per calcolare il punteggio di resilienza e i tipi di interruzione AppComponents

La tabella seguente spiega le formule utilizzate da per calcolare il componente AWS Resilience Hub di punteggio di ciascun tipo di raccomandazione.

Formule per calcolare la componente di punteggio di ogni tipo di raccomandazione

Componente di punteggio	Descrizione	Formula	Esempio
Copertura del test () `T`	Un punteggio normalizzato (0-100 punti) basato sul numero di test implementati ed esclusi con successo, rispetto al numero totale di test AWS Resilience Hub consigliati. **Note** Per calcolare il punteggio di resilienza, i test consigliati devono essere stati eseguiti con successo	`T = ((Total number of tests implemented) + (Total number of tests excluded) ) / (Total number of tests recommended)` Le parti della formula sono le seguenti: • Numero totale di test configurati: indica il numero totale di test configurati al momento della creazione e del caricamento del AWS CloudFormation modello	Se hai implementato 10 test ed escluso 5 test su 20 test AWS Resilience Hub consigliati, la copertura dei test viene calcolata come segue: `T = (10 + 5) / 20` Cioè, `T = .75 or 75 points`

Componente di punteggio	Descrizione	Formula	Esempio
	negli ultimi 30 giorni perché sia considerato AWS Resilience Hub implementato.	nella AWS CloudFormation console. • Numero totale di test consigliati: indica i test consigliati da AWS Resilience Hub in base alle risorse dell'applicazione. • Numero totale di test esclusi: indica il numero di test consigliati che sono stati esclusi dall'applicazione.	

Componente di punteggio	Descrizione	Formula	Esempio
Copertura degli allarmi () `A`	Un punteggio normalizzato (0-100 punti) basato sul numero di CloudWatch allarmi Amazon implementati ed esclusi con successo, rispetto al numero totale di allarmi AWS Resilience Hub Amazon consigliati. CloudWatch **Note** Per calcolare il punteggio di resilienza, gli allarmi consigliati devono essere in stato Pronto per AWS Resilience Hub essere considerati implementati.	`A = ((Total number of alarms implemented) + (Total number of alarms excluded)) / (Total number of alarms recommended)` Le parti della formula sono le seguenti: • Numero totale di allarmi configurati: indica il numero totale di CloudWatch allarmi Amazon configurati al momento della creazione e del caricamento del AWS CloudFormation modello nella AWS CloudFormation console. • Numero totale di allarmi consigliato: indica gli CloudWatch allarmi Amazon consigliati da in AWS Resilience Hub base alle risorse dell'applicazione. • Numero totale di allarmi esclusi: indica il numero di CloudWatch allarmi Amazon consigliati che	Se hai implementato 10 allarmi Amazon ed escluso 5 su 20 CloudWatch allarmi Amazon AWS Resilience Hub consigliati, la copertura degli CloudWatch allarmi Amazon CloudWatch viene calcolata come segue: `A = (10 + 5) / 20` Cioè, `A = .75 or 75 points`

Componente di punteggio	Descrizione	Formula	Esempio
		hai escluso dall'appl icazione.	

Componente di punteggio	Descrizione	Formula	Esempio
SOPcopertura (S)	Un punteggio normalizzato (0-100 punti) basato sul numero di SOPs quelli implementati ed esclusi con successo, rispetto al numero totale di punteggi consigliati. AWS Resilience Hub SOPs	`S = ((Total number of SOPs implemented) + (Total number of SOPs excluded)) / (Total number of SOPs recommended)` Le parti della formula sono le seguenti: • Numero totale di SOPs configurati: indica il numero totale di SOPs configurati al momento della creazione e del caricamento del AWS CloudFormation modello nella AWS CloudFormation console. • Numero totale di SOPs consigliati: indica il numero SOPs consigliato AWS Resilience Hub in base alle risorse dell'applicazione. • Numero totale di SOPs esclusi: indica il numero di opzioni SOPs consigliate che sono state escluse dall'applicazione.	Se ne hai implementati 10 e ne hai SOPs esclusi 5 su 20 AWS Resilience Hub consigliatiSOPs, la SOP copertura viene calcolata come segue: `S = (10 + 5) / 20` Cioè, `S = .75 or 75 points`

Componente di punteggio	Descrizione	Formula	Esempio

RTO/RPOconformità (P)	Un punteggio normalizzato (0-100 punti) basato sul rispetto della politica di resilienza dell'applicazione.	`P = Total weights of disruption types meeting the application's resiliency policy / Total weights of all disruption types .`	Se la policy di resilienza dell'applicazione soddisfa solo i tipi di Availability Zone (AZ) e di interruzione dell'infrastruttura, il punteggio della policy di resilienza (P) viene calcolato come segue:
			• Se sono stati impostati RPO obiettivi RTO e regionali, `P` viene calcolato come segue:
			`P = (20 + 30)/ 100`
			Cioè, `P = .5 or 50 points`
			• Se non sono stati impostati RPO obiettivi RTO e obiettivi regionali, `P` viene calcolato come segue:
			`P = (22.22 + 33.33)/ 99.9`

Componente di punteggio	Descrizione	Formula	Esempio
			Cioè, `P = .55 or 55 points`

La tabella seguente spiega la formula utilizzata da AWS Resilience Hub per calcolare il punteggio di resilienza per l'intera applicazione.

Formula per calcolare il punteggio di resilienza

Componente di punteggio	Descrizione	Formula	Esempio
Punteggio di resilienza per l'applicazione () `RS`	Un punteggio di resilienza normalizzato (0-100 punti) basato sul rispetto della politica di resilienza dell'applicazione. Il punteggio di resilienza per applicazione è la media ponderata di tutti i tipi di raccomandazioni. Ovvero: `RS = Weighted Average (T, A, S, P)`	Il punteggio di resilienza per applicazione viene calcolato utilizzando la seguente formula: `RS = (T * Weight(T) + A * Weight(A) + S * Weight(S) + P * Weight(P)) / (Weight(T) + Weight(A) + Weight(S) + Weight(P))`	Le formule per calcolare la copertura di ogni tabella dei tipi di raccomandazione sono le seguenti: • `Test coverage (T) = .75` • `Alarms (A) = .75` • `SOPs (S) = .75` • `Meeting resiliency policy (P) = .5` Il punteggio di resilienza per applicazione viene

Componente di punteggio	Descrizione	Formula	Esempio
			calcolato come segue: `RS = ((.75 * .2) + (.75 * .2) + (.75 * .2) + (.5 * .4)) /(.2 + .2 + .2 + .4)` Cioè, `RS = .65 or 65 points`

La tabella seguente spiega le formule utilizzate da AWS Resilience Hub per calcolare il punteggio di resilienza per i componenti dell'applicazione (AppComponents) e i tipi di interruzione. Tuttavia, è possibile ottenere il punteggio di resilienza AppComponents e i tipi di interruzione solo tramite il seguente Resilience Hub: AWS APIs

- DescribeAppAssessmentottenere `RSo`
- ListAppComponentCompliancesottenere `RSao` e `RSA`

Formule per calcolare il punteggio di resilienza AppComponents e i tipi di interruzione

Componente di punteggio	Descrizione	Formula	Esempio

Punteggio di resilienza per AppComponent e per tipo di interruzione () `RSao`	Un punteggio normalizzato (0-100 punti) basato sul rispetto della politica di resilienza	Il punteggio di resilienza per AppComponent e per tipo di interruzione viene calcolato utilizzando la seguente formula:
		
		`RSao = (T * Weight(T) +`
		
		`A * Weight(A) +`
			`RSao`le ipotesi per tutti i tipi di raccomandazione sono le seguenti:
			
			• `Test coverage (T) = .75`

Componente di punteggio	Descrizione	Formula	Esempio

	AppComponent per tipo di interruzione. Il punteggio di resilienza per AppComponent e per tipo di interruzione è la media ponderata di tutti i tipi di raccomandazione.
	
	Ovvero: `RSao = Weighted Average (T, A, S, P)`
	
	I valori di `T, A, S, P` vengono calcolati per tutti i test, gli allarmi e il rispetto SOPs della politica di resilienza consigliati AppComponent e del tipo di interruzione.
		`S * Weight(S) +`
		
		`P * Weight(P)) /`
		
		`(Weight(T) + Weight(A) + Weight(S) + Weight(P))`
			• `Alarms (A) = .75`
			• `SOPs (S) = .75`
			• `Meeting resiliency policy (P) = .5`
			
			Il punteggio di resilienza per tipo AppComponent di interruzione è calcolato come segue:
			
			`RSao = ((.75 * .2) + (.75 * .2) + (.75 * .2) + (.5 * .4)) / (.2 + .2 + .2 + .4)`
			
			Cioè, `RSao = .65 or 65 points`

Componente di punteggio	Descrizione	Formula	Esempio
Punteggio di resilienza per AppComponent () RSa	Un punteggio normalizzato (0-100 punti) basato sul rispetto della politica di resilienza. Il punteggio di resilienza per AppComponent è la media ponderata di tutti i tipi di raccomandazione. Ovvero: RSa = Weighted Average (T, A, S, P) I valori di T, A, S, P vengono calcolati per tutti i test e gli allarmi consigliati e per soddisfare la politica di resilienza di. SOPs AppComponent	Il punteggio di resilienza per AppComponent viene calcolato utilizzando la seguente formula: RSa = (T * Weight(T) + A * Weight(A) + S * Weight(S) + P * Weight(P)) / (Weight(T) + Weight(A) + Weight(S) + Weight(P))	RSale ipotesi per tutti i tipi di raccomandazione sono le seguenti: • Test coverage (T) = .75 • Alarms (A) = .75 • SOPs (S) = .75 • Meeting resiliency policy (P) = .5 Il punteggio di resilienza per AppComponent viene calcolato come segue: RSa = ((.75 * .2) + (.75 * .2) + (.75 * .2) + (.5 * .4)) / (.2 + .2 + .2 + .4) Cioè, RSa = .65 or 65 points

Componente di punteggio	Descrizione	Formula	Esempio
Punteggio di resilienza per tipo di interruzione () RSo	Un punteggio normalizzato (0-100 punti) basato sul rispetto della politica di resilienza. Il punteggio di resilienza per tipo di interruzione è la media ponderata di tutti i tipi di raccomandazione. Ovvero: RSo = Weighted Average (T, A, S, P) I valori di T, A, S, P vengono calcolati per tutti i test e gli allarmi consigliati e per soddisfare la politica di resilienza del tipo di interruzione. SOPs	Il punteggio di resilienza per tipo di interruzione viene calcolato utilizzando la seguente formula: RSo = (T * Weight(T) + A * Weight(A) + S * Weight(S) + P * Weight(P)) / (Weight(T) + Weight(A) + Weight(S) + Weight(P))	RSole ipotesi per tutti i tipi di raccomandazione sono le seguenti: • Test coverage (T) = .75 • Alarms (A) = .75 • SOPs (S) = .75 • Meeting resiliency policy (P) = .5 Il punteggio di resilienza per tipo di interruzione viene calcolato come segue: RSo = ((.75 * .2) + (.75 * .2) + (.75 * .2) + (.5 *.4)) / (.2 + .2 + .2 + .4) Cioè, RSo = .65 or 65 points

Pesi

AWS Resilience Hub assegna un peso a ciascun tipo di raccomandazione per il punteggio di resilienza totale.

Le tabelle seguenti mostrano il peso degli allarmi, dei testSOPs, della conformità alle politiche di resilienza e dei tipi di interruzione. I tipi di interruzioni includono applicazione, infrastruttura, AZ e regione.

> **Note**
>
> Se scegli di non definire obiettivi regionali RTO o RPO obiettivi per la tua politica, i pesi per gli altri tipi di interruzione vengono aumentati di conseguenza, come mostrato nella colonna Peso quando la regione non è definita.

Pesi relativi agli allarmi, ai test e agli obiettivi delle SOPs politiche

Tipo di raccomandazione	Weight
Allarmi	20 punti
SOPs	20 punti
Tests	20 punti
Rispettare la politica di resilienza	40 punti

Pesi relativi al tipo di interruzione

Tipo di interruzione	Peso quando la regione è definita	Peso quando la regione non è definita
Applicazione	40 punti	44.44 punti
Infrastruttura	30 punti	33,33 punti
Zona di disponibilità	20 punti	22.22 punti
Regione	10 punti	N/D

Integrazione dei consigli operativi nella tua applicazione con AWS CloudFormation

Dopo aver scelto Crea CloudFormation modello nella pagina Consigli operativi, AWS Resilience Hub crea un AWS CloudFormation modello che descrive l'allarme specifico, la procedura operativa standard (SOP) o l' AWS FIS esperimento per l'applicazione. Il AWS CloudFormation modello è archiviato in un bucket Amazon S3 e puoi controllare il percorso S3 verso il modello nella scheda Dettagli del modello nella pagina Consigli operativi.

Ad esempio, l'elenco seguente mostra un AWS CloudFormation modello in JSON formato -format che descrive una raccomandazione di allarme resa da. AWS Resilience HubÈ un allarme di limitazione della lettura per una tabella DynamoDB chiamata. `Employees`

La `Resources` sezione del modello descrive l'`AWS::CloudWatch::Alarm`allarme che si attiva quando il numero di eventi di accelerazione della lettura per la tabella DynamoDB supera 1. Inoltre, le due `AWS::SSM::Parameter` risorse definiscono i metadati che consentono di identificare le risorse installate senza dover AWS Resilience Hub scansionare l'applicazione effettiva.

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

Modificare il modello AWS CloudFormation

Il modo più semplice per integrare un allarme o una AWS FIS risorsa nell'applicazione principale consiste semplicemente nell'aggiungerlo come altra risorsa nel modello che descrive il modello dell'applicazione. SOP Il file JSON -formatted fornito di seguito fornisce una descrizione di base di come una tabella DynamoDB viene descritta in un modello. AWS CloudFormation È probabile che un'applicazione reale includa molte altre risorse, come tabelle aggiuntive.

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

Per consentire l'implementazione della risorsa di allarme con l'applicazione, ora è necessario sostituire le risorse codificate con un riferimento dinamico negli stack delle applicazioni.

Quindi, nella definizione della `AWS::CloudWatch::Alarm` risorsa, modifica quanto segue:

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

al seguente:

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

E nella definizione della `AWS::SSM::Parameter` risorsa, modifica quanto segue:

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

a quanto segue:

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

Quando modificate AWS CloudFormation modelli SOPs ed AWS FIS esperimenti, seguirete lo stesso approccio, sostituendo i riferimenti codificati IDs con riferimenti dinamici che continuano a funzionare anche dopo le modifiche all'hardware.

Utilizzando un riferimento alla tabella DynamoDB, è possibile eseguire le seguenti AWS CloudFormation operazioni:

- Create prima la tabella del database.
- Utilizza sempre l'ID effettivo della risorsa generata nell'allarme e aggiorna l'allarme dinamicamente se è AWS CloudFormation necessario sostituire la risorsa.

> **Note**
>
> È possibile scegliere metodi più avanzati per gestire le risorse dell'applicazione, ad AWS CloudFormation esempio annidando gli stack o facendo riferimento agli output delle risorse in uno stack separato. AWS CloudFormation (Ma se vuoi mantenere lo stack di consigli separato dallo stack principale, devi configurare un modo per passare le informazioni tra i due stack.)
> Inoltre, è possibile utilizzare strumenti di terze parti, come Terraform by HashiCorp, per fornire Infrastructure as Code (IaC).

Utilizzo AWS Resilience Hub APIs per descrivere e gestire l'applicazione

In alternativa alla descrizione e alla gestione delle applicazioni tramite AWS Resilience Hub console, AWS Resilience Hub consente di descrivere e gestire le applicazioni utilizzando AWS Resilience Hub APIs. Questo capitolo spiega come creare un'applicazione utilizzando AWS Resilience Hub APIs. Definisce anche la sequenza in cui è necessario eseguire APIs e i valori dei parametri da fornire con esempi appropriati. Per ulteriori informazioni, consulta i seguenti argomenti:

- the section called “Preparazione della domanda”
- the section called “Esecuzione e analisi dell'applicazione”
- the section called “Modifica la tua applicazione”

Fase 1: Preparazione dell'applicazione

Per preparare un'applicazione, è necessario innanzitutto creare un'applicazione, assegnare una politica di resilienza e quindi importare le risorse dell'applicazione dalle fonti di input. Per ulteriori informazioni sulle modalità AWS Resilience Hub APIs utilizzate per preparare un'applicazione, consultate i seguenti argomenti:

- the section called “Creazione di un'applicazione”
- the section called “Crea una politica di resilienza”
- the section called “Importa le risorse dell'applicazione e monitora lo stato delle importazioni”
- the section called “Pubblica la tua applicazione e assegna una politica di resilienza”

Creazione di un'applicazione

Per creare una nuova applicazione in AWS Resilience Hub, è necessario chiamare `CreateApp` API e fornire un nome di applicazione univoco. Per ulteriori informazioni su questo argomentoAPI, vederehttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_CreateApp.html.

L'esempio seguente mostra come creare una nuova applicazione `newApp` in AWS Resilience Hub uso `CreateApp`API.

Richiesta

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

Risposta

```
{
    "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"
    }
}
```

Creazione di una politica di resilienza

Dopo aver creato l'applicazione, è necessario creare una politica di resilienza che consenta di comprendere lo stato di resilienza dell'applicazione utilizzando. `CreateResiliencyPolicy` API Per ulteriori informazioni su questo API argomento, vedere. https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_CreateResiliencyPolicy.html

L'esempio seguente mostra come creare `newPolicy` per l'applicazione in AWS Resilience Hub uso `CreateResiliencyPolicy`API.

Richiesta

```
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}}'
```

Risposta

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

Importazione di risorse da una fonte di input e monitoraggio dello stato dell'importazione

AWS Resilience Hub fornisce quanto segue APIs per importare risorse nell'applicazione:

- `ImportResourcesToDraftAppVersion`— Ciò API consente di importare risorse nella versione bozza dell'applicazione da diverse fonti di input. Per ulteriori informazioni su questo argomentoAPI, vederehttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_ImportResourcesToDraftAppVersion.html.
- `PublishAppVersion`— Viene API pubblicata una nuova versione dell'applicazione insieme a quella aggiornata AppComponents. Per ulteriori informazioni su questo argomentoAPI, vederehttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_PublishAppVersion.html.
- `DescribeDraftAppVersionResourcesImportStatus`— Ciò API consente di monitorare lo stato di importazione delle risorse in una versione dell'applicazione. Per ulteriori informazioni su

questo argomentoAPI, vederehttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_DescribeDraftAppVersionResourcesImportStatus.html.

L'esempio seguente mostra come importare risorse nell'applicazione in AWS Resilience Hub uso `ImportResourcesToDraftAppVersion`API.

Richiesta

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

Risposta

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

L'esempio seguente mostra come aggiungere manualmente risorse all'applicazione in AWS Resilience Hub uso `CreateAppVersionResource`API.

Richiesta

```
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"]'
```

Risposta

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

L'esempio seguente mostra come monitorare lo stato di importazione delle risorse in AWS Resilience Hub uso `DescribeDraftAppVersionResourcesImportStatus`API.

Richiesta

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

Risposta

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

Pubblicazione della versione bozza dell'applicazione e assegnazione di una politica di resilienza

Prima di eseguire una valutazione, è necessario innanzitutto pubblicare la versione bozza dell'applicazione e assegnare una politica di resilienza alla versione rilasciata dell'applicazione.

Per pubblicare la versione bozza dell'applicazione e assegnare una politica di resilienza

1. Per pubblicare la bozza della tua applicazione, usa. `PublishAppVersion` API Per ulteriori informazioni su questo argomentoAPI, vederehttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_PublishAppVersion.html.

   L'esempio seguente mostra come pubblicare la bozza dell'applicazione in AWS Resilience Hub uso `PublishAppVersion`API.

   Richiesta

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

   Risposta

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

2. Applica una politica di resilienza alla versione rilasciata dell'applicazione utilizzando `UpdateApp`API. Per ulteriori informazioni su questo argomentoAPI, vederehttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_UpdateApp.html.

   L'esempio seguente mostra come applicare una politica di resilienza alla versione rilasciata di un'applicazione in AWS Resilience Hub uso `UpdateApp`API.

   Richiesta

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

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

Risposta

```
{
    "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"
    }
}
```

Fase 2: Esecuzione e gestione delle valutazioni della AWS Resilience Hub resilienza

Dopo aver pubblicato una nuova versione dell'applicazione, è necessario eseguire una nuova valutazione della resilienza e analizzare i risultati per garantire che l'applicazione soddisfi il carico di lavoro stimato RTO e stimato RPO definito nella politica di resilienza. La valutazione confronta la configurazione di ogni componente dell'applicazione con la policy e fornisce raccomandazioni in materia di allarmi e test. SOP

Per ulteriori informazioni, consulta i seguenti argomenti:

- the section called “Esegui e monitora una valutazione della resilienza”
- the section called “Crea una politica di resilienza”

Esecuzione e monitoraggio delle valutazioni della AWS Resilience Hub resilienza

Per eseguire valutazioni della resilienza AWS Resilience Hub e monitorarne lo stato, è necessario utilizzare quanto segue: APIs

- `StartAppAssessment`— Questo API crea una nuova valutazione per un'applicazione. Per ulteriori informazioni su questo argomentoAPI, vederehttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_StartAppAssessment.html.
- `DescribeAppAssessment`— API Descrive una valutazione per la domanda e fornisce lo stato di completamento della valutazione. Per ulteriori informazioni a riguardoAPI, vederehttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_DescribeAppAssessment.html.

L'esempio seguente mostra come iniziare a eseguire una nuova valutazione in AWS Resilience Hub uso `StartAppAssessment`API.

Richiesta

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

Risposta

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

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

L'esempio seguente mostra come monitorare lo stato della valutazione in fase di AWS Resilience Hub utilizzo `DescribeAppAssessment`API. È possibile estrarre lo stato della valutazione dalla `assessmentStatus` variabile.

Richiesta

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

Risposta

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

Esame dei risultati della valutazione

Una volta completata con successo la valutazione, è possibile esaminare i risultati della valutazione utilizzando quanto segueAPIs.

- `DescribeAppAssessment`— Ciò API consente di tenere traccia dello stato attuale della domanda rispetto alla politica di resilienza. Inoltre, è possibile estrarre dalla struttura lo stato di conformità da `complianceStatus` una variabile e il punteggio di resilienza per ogni tipo di interruzione. `resiliencyScore` Per ulteriori informazioni su questo argomentoAPI, vedere. https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_DescribeAppAssessment.html
- `ListAlarmRecommendations`— Ciò API consente di ottenere i consigli sugli allarmi utilizzando l'Amazon Resource Name (ARN) della valutazione. Per ulteriori informazioni a riguardoAPI, consultahttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_ListAlarmRecommendations.html.

> **Note**
>
> Per ottenere SOP e FIS testare i consigli, utilizzare `ListSopRecommendations` e `ListTestRecommendations`APIs.

L'esempio seguente mostra come ottenere i consigli sugli allarmi utilizzando l'Amazon Resource Name (ARN) della valutazione utilizzata `ListAlarmRecommendations`API.

> **Note**
>
> Per ottenere SOP e FIS testare i consigli, sostituiscili con `ListSopRecommendations` o`ListTestRecommendations`.

Richiesta

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

Risposta


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

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

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

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

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

```
    ]
}
```

L'esempio seguente mostra come ottenere i consigli di configurazione (consigli su come migliorare la resilienza attuale) utilizzando `ListAppComponentRecommendations`API.

Richiesta

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

Risposta

```
{
    "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"
                }
```

```
            ]
        }
    ]
}
```

Fase 3: Modifica dell'applicazione

AWS Resilience Hub consente di modificare le risorse dell'applicazione modificando una bozza dell'applicazione e pubblicando le modifiche in una nuova versione (pubblicata). AWS Resilience Hub utilizza la versione pubblicata dell'applicazione, che include le risorse aggiornate, per eseguire le valutazioni della resilienza.

Per ulteriori informazioni, consulta i seguenti argomenti:

- the section called “Aggiungere manualmente le risorse”
- the section called “Raggruppamento delle risorse in un unico componente dell'applicazione”
- the section called “Escludere una risorsa da un AppComponent”

Aggiungere manualmente risorse all'applicazione

Se la risorsa non viene distribuita come parte di una sorgente di input, AWS Resilience Hub consente di aggiungere manualmente la risorsa all'applicazione utilizzando `CreateAppVersionResource`API. Per ulteriori informazioni su questo argomentoAPI, vederehttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_CreateAppVersionResource.html.

A tale scopo è necessario fornire i seguenti parametriAPI:

- Amazon Resource Name (ARN) dell'applicazione
- ID logico della risorsa
- ID fisico della risorsa
- AWS CloudFormation tipo

L'esempio seguente mostra come aggiungere manualmente risorse all'applicazione in AWS Resilience Hub uso `CreateAppVersionResource`API.

Richiesta

```
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"]'
```

Risposta

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

Raggruppamento delle risorse in un unico componente dell'applicazione

Un componente applicativo (AppComponent) è un gruppo di AWS risorse correlate che funzionano e falliscono come una singola unità. Ad esempio, quando sono presenti carichi di lavoro interregionali utilizzati come distribuzioni in standby. AWS Resilience Hub dispone di regole che stabiliscono quali

AWS risorse possono appartenere a quale tipo di. AppComponent AWS Resilience Hub consente di raggruppare le risorse in un'unica AppComponent utilizzando la seguente gestione delle risorseAPIs.

- `UpdateAppVersionResource`— Questo API aggiorna i dettagli delle risorse di un'applicazione. Per ulteriori informazioni su questo argomentoAPI, vedere UpdateAppVersionResource.
- `DeleteAppVersionAppComponent`— Questo API elimina il file AppComponent dall'applicazione. Per ulteriori informazioni su questo argomentoAPI, vedere DeleteAppVersionAppComponent.

L'esempio seguente mostra come aggiornare i dettagli delle risorse dell'applicazione in AWS Resilience Hub uso `DeleteAppVersionAppComponent`API.

Richiesta

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

Risposta

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

L'esempio seguente mostra come eliminare AppComponent lo spazio vuoto creato negli esempi precedenti di AWS Resilience Hub utilizzo `UpdateAppVersionResource`API.

Richiesta

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

Risposta

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

Escludere una risorsa da un AppComponent

AWS Resilience Hub consente di escludere risorse dalle valutazioni utilizzando `UpdateAppVersionResource`API. Queste risorse non verranno prese in considerazione durante il calcolo della resilienza dell'applicazione. Per ulteriori informazioni su questo argomentoAPI, vederehttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_UpdateAppVersionResource.html.

> **Note**
>
> È possibile escludere solo le risorse che sono state importate da una fonte di input.

L'esempio seguente mostra come escludere una risorsa dell'applicazione durante l' AWS Resilience Hub utilizzo `UpdateAppVersionResource`API.

Richiesta

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

Risposta

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

Sicurezza in AWS Resilience Hub

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di data center e architetture di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra te e te. AWS Il modello di responsabilità condivisa descrive questo aspetto come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi nel AWS cloud. AWS ti fornisce anche servizi che puoi utilizzare in modo sicuro. I revisori esterni testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei AWS Programmi di AWS conformità dei Programmi di conformità dei di . Per maggiori informazioni sui programmi di conformità applicabili AWS Resilience Hub, consulta la sezione AWS Servizi rientranti nell'ambito del programma di conformitàAWS .
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della tua azienda e le leggi e normative vigenti.

Questa documentazione ti aiuta a capire come applicare il modello di responsabilità condivisa durante l'utilizzo AWS Resilience Hub. I seguenti argomenti mostrano come eseguire la configurazione AWS Resilience Hub per soddisfare gli obiettivi di sicurezza e conformità. Imparerai anche a utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere AWS Resilience Hub le tue risorse.

Indice

Protezione dei dati in AWS Resilience Hub

Il modello di responsabilità AWS condivisa di si applica alla protezione dei dati in AWS Resilience Hub. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati

su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i AWS servizi utilizzati. Per ulteriori informazioni sulla privacy dei dati, consulta la sezione Privacy dei dati FAQ. Per informazioni sulla protezione dei dati in Europa, consulta il Modello di responsabilitàAWS condivisa e GDPR il post sul blog sulla AWS sicurezza.

Ai fini della protezione dei dati, ti consigliamo di proteggere Account AWS le credenziali e di configurare i singoli utenti con AWS IAM Identity Center o AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- UsaSSL/TLSper comunicare con AWS le risorse. Richiediamo TLS 1.2 e consigliamo TLS 1.3.
- Configurazione API e registrazione delle attività degli utenti con AWS CloudTrail.
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno AWS servizi.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di FIPS 140-3 moduli crittografici convalidati per accedere AWS tramite un'interfaccia a riga di comando o unAPI, usa un endpoint. FIPS Per ulteriori informazioni sugli FIPS endpoint disponibili, vedere Federal Information Processing Standard () 140-3. FIPS

Ti consigliamo vivamente di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori con Resilience Hub o altro AWS servizi utilizzando la console,API, AWS CLI o. AWS SDKs I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Se fornisci un URL a un server esterno, ti consigliamo vivamente di non includere le informazioni sulle credenziali URL per convalidare la tua richiesta a quel server.

Crittografia a riposo

AWS Resilience Hub crittografa i tuoi dati quando sono inattivi. I dati in ingresso AWS Resilience Hub vengono crittografati quando sono inattivi utilizzando una crittografia trasparente lato server. Questo consente di ridurre gli oneri operativi e la complessità associati alla protezione dei dati sensibili. La crittografia dei dati inattivi consente di creare applicazioni sicure che rispettano rigorosi requisiti normativi e di conformità per la crittografia.

Crittografia in transito

AWS Resilience Hub crittografa i dati in transito tra il servizio e altri servizi integrati. AWS Tutti i dati che passano tra AWS Resilience Hub e i servizi integrati vengono crittografati utilizzando Transport Layer Security (TLS). AWS Resilience Hub fornisce azioni preconfigurate per tipi specifici di obiettivi tra AWS i servizi e supporta azioni per le risorse di destinazione.

Identity and Access Management per AWS Resilience Hub

AWS Identity and Access Management (IAM) è uno strumento AWS servizio che aiuta un amministratore a controllare in modo sicuro l'accesso alle risorse. AWS IAMgli amministratori controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare AWS le risorse di Resilience Hub. IAMè un software AWS servizio che puoi utilizzare senza costi aggiuntivi.

Argomenti

Destinatari

Il modo in cui usi AWS Identity and Access Management (IAM) varia a seconda del lavoro svolto in AWS Resilience Hub.

Utente del servizio: se utilizzi il servizio AWS Resilience Hub per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più funzionalità di AWS Resilience Hub per svolgere il tuo lavoro, potresti aver bisogno di autorizzazioni aggiuntive. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità di AWS Resilience Hub, consulta. Risoluzione dei problemi relativi all'identità e all'accesso a AWS Resilience Hub

Amministratore del servizio: se sei responsabile delle risorse di AWS Resilience Hub presso la tua azienda, probabilmente hai pieno accesso a AWS Resilience Hub. È tuo compito determinare a quali funzionalità e risorse di AWS Resilience Hub devono accedere gli utenti del servizio. È quindi necessario inviare richieste all'IAMamministratore per modificare le autorizzazioni degli utenti del servizio. Consulta le informazioni contenute in questa pagina per comprendere i concetti di base diIAM. Per ulteriori informazioni su come la tua azienda può utilizzare IAM AWS Resilience Hub, consultaCome funziona AWS Resilience Hub con IAM.

IAMamministratore: se sei un IAM amministratore, potresti voler conoscere i dettagli su come scrivere politiche per gestire l'accesso a AWS Resilience Hub. Per visualizzare esempi di policy basate sull'identità di AWS Resilience Hub che puoi utilizzare in, consulta. IAM Esempi di policy basate sull'identità per Resilience Hub AWS

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. È necessario autenticarsi (accedere a AWS) come Utente root dell'account AWS, come IAM utente o assumendo un ruolo. IAM

È possibile accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAMIdentity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Quando accedi come identità federata, l'amministratore aveva precedentemente configurato la federazione delle identità utilizzando i ruoli. IAM Quando si accede AWS utilizzando la federazione, si assume indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al AWS Management Console o al portale di AWS accesso. Per ulteriori informazioni sull'accesso a AWS, vedi Come accedere al tuo Account AWS nella Guida per l'Accedi ad AWS utente.

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando () per firmare crittograficamente le tue richieste utilizzando le tue credenziali. CLI Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sull'utilizzo del metodo consigliato per firmare autonomamente le richieste, consulta Firmare AWS API le richieste nella Guida per l'IAMutente.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. Ad esempio, ti AWS consiglia di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del tuo account. Per ulteriori informazioni, consulta Autenticazione a più fattori nella Guida per l'AWS IAM Identity Center utente e Utilizzo dell'autenticazione a più fattori (MFA) AWS nella Guida per l'IAMutente.

Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte AWS servizi le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzale per eseguire le operazioni che solo l'utente root può eseguire. Per l'elenco completo delle attività che richiedono l'accesso come utente root, consulta Attività che richiedono le credenziali dell'utente root nella Guida per l'IAMutente.

Identità federata

Come procedura consigliata, richiedi agli utenti umani, compresi gli utenti che richiedono l'accesso come amministratore, di utilizzare la federazione con un provider di identità per accedere AWS servizi utilizzando credenziali temporanee.

Un'identità federata è un utente dell'elenco utenti aziendale, di un provider di identità Web AWS Directory Service, della directory Identity Center o di qualsiasi utente che accede utilizzando le AWS servizi credenziali fornite tramite un'origine di identità. Quando le identità federate accedono Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. Puoi creare utenti e gruppi in IAM Identity Center oppure puoi connetterti e sincronizzarti con un set di utenti e gruppi nella tua fonte di identità per utilizzarli su tutte le tue applicazioni. Account AWS Per

informazioni su IAM Identity Center, vedi Cos'è IAM Identity Center? nella Guida AWS IAM Identity Center per l'utente.

IAM users and groups

Un IAMutente è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Laddove possibile, consigliamo di fare affidamento su credenziali temporanee anziché creare IAM utenti con credenziali a lungo termine come password e chiavi di accesso. Tuttavia, se hai casi d'uso specifici che richiedono credenziali a lungo termine con IAM gli utenti, ti consigliamo di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta Ruotare regolarmente le chiavi di accesso per i casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente. IAM

Un IAMgruppo è un'identità che specifica un insieme di utenti. IAM Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, potresti avere un gruppo denominato IAMAdminse concedere a quel gruppo le autorizzazioni per IAM amministrare le risorse.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta Quando creare un IAM utente (anziché un ruolo) nella Guida per l'IAMutente.

IAMruoli

Un IAMruolo è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un IAM utente, ma non è associato a una persona specifica. È possibile assumere temporaneamente un IAM ruolo in AWS Management Console cambiando ruolo. È possibile assumere un ruolo chiamando un' AWS APIoperazione AWS CLI or o utilizzando un'operazione personalizzataURL. Per ulteriori informazioni sui metodi di utilizzo dei ruoli, vedere Utilizzo IAM dei ruoli nella Guida per l'IAMutente.

IAMi ruoli con credenziali temporanee sono utili nelle seguenti situazioni:

- Accesso utente federato: per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per informazioni

sui ruoli per la federazione, vedere Creazione di un ruolo per un provider di identità di terze parti nella Guida per l'IAMutente. Se utilizzi IAM Identity Center, configuri un set di autorizzazioni. Per controllare a cosa possono accedere le identità dopo l'autenticazione, IAM Identity Center correla il set di autorizzazioni a un ruolo in. IAM Per informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .

- Autorizzazioni IAM utente temporanee: un IAM utente o un ruolo può assumere il IAM ruolo di assumere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso su più account: puoi utilizzare un IAM ruolo per consentire a qualcuno (un responsabile fidato) di un altro account di accedere alle risorse del tuo account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni AWS servizi, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per conoscere la differenza tra ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta la sezione Accesso alle risorse su più account IAM nella Guida per l'utente. IAM
- Accesso tra servizi: alcuni AWS servizi utilizzano funzionalità in altri. AWS servizi Ad esempio, quando effettui una chiamata in un servizio, è normale che quel servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
  - Sessioni di accesso diretto (FAS): quando utilizzi un IAM utente o un ruolo per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FASutilizza le autorizzazioni del principale che chiama an AWS servizio, in combinazione con la richiesta di effettuare richieste AWS servizio ai servizi downstream. FASle richieste vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri AWS servizi o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli FAS delle politiche relative alle richieste, consulta Forward access sessions.
  - Ruolo di servizio: un ruolo di servizio è un IAMruolo che un servizio assume per eseguire azioni per conto dell'utente. Un IAM amministratore può creare, modificare ed eliminare un ruolo di servizio dall'internoIAM. Per ulteriori informazioni, vedere Creazione di un ruolo per delegare le autorizzazioni a un utente AWS servizio nella Guida per l'IAMutente.
  - Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. AWS servizio Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un IAM amministratore può visualizzare, ma non modificare le autorizzazioni per i ruoli collegati al servizio.

- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un IAM ruolo per gestire le credenziali temporanee per le applicazioni in esecuzione su un'EC2istanza e che effettuano AWS CLI o effettuano AWS API richieste. È preferibile alla memorizzazione delle chiavi di accesso all'interno dell'EC2istanza. Per assegnare un AWS ruolo a un'EC2istanza e renderlo disponibile per tutte le sue applicazioni, create un profilo di istanza collegato all'istanza. Un profilo di istanza contiene il ruolo e consente ai programmi in esecuzione sull'EC2istanza di ottenere credenziali temporanee. Per ulteriori informazioni, consulta Usare un IAM ruolo per concedere le autorizzazioni alle applicazioni in esecuzione su EC2 istanze Amazon nella Guida per l'IAMutente.

Per sapere se utilizzare IAM ruoli o IAM utenti, consulta Quando creare un IAM ruolo (anziché un utente) nella Guida per l'IAMutente.

Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e associandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata AWS come JSON documenti. Per ulteriori informazioni sulla struttura e il contenuto dei documenti relativi alle JSON politiche, vedere Panoramica delle JSON politiche nella Guida per l'IAMutente.

Gli amministratori possono utilizzare AWS JSON le policy per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un IAM amministratore può creare IAM politiche. L'amministratore può quindi aggiungere le IAM politiche ai ruoli e gli utenti possono assumerli.

IAMle politiche definiscono le autorizzazioni per un'azione indipendentemente dal metodo utilizzato per eseguire l'operazione. Ad esempio, supponiamo di disporre di una policy che consente l'operazione `iam:GetRole`. Un utente con tale criterio può ottenere informazioni sul ruolo da AWS Management Console, da o da. AWS CLI AWS API

Policy basate su identità

I criteri basati sull'identità sono documenti relativi alle politiche di JSON autorizzazione che è possibile allegare a un'identità, ad esempio un IAM utente, un gruppo di utenti o un ruolo. Tali policy

definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una politica basata sull'identità, consulta Creazione di politiche nella Guida per l'utente. IAM IAM

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono integrate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli all'interno del tuo. Account AWS Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una politica gestita o una politica in linea, consulta Scelta tra politiche gestite e politiche in linea nella Guida per l'IAMutente.

Policy basate su risorse

Le politiche basate sulle risorse sono documenti di JSON policy allegati a una risorsa. Esempi di politiche basate sulle risorse sono le policy di trust dei IAM ruoli e le policy dei bucket di Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. AWS servizi

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non è possibile utilizzare le policy AWS gestite contenute IAM in una policy basata sulle risorse.

Elenchi di controllo degli accessi () ACLs

Le liste di controllo degli accessi (ACLs) controllano quali principali (membri dell'account, utenti o ruoli) dispongono delle autorizzazioni per accedere a una risorsa. ACLssono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy. JSON

Amazon S3 e Amazon VPC sono esempi di servizi che supportano. AWS WAF ACLs Per ulteriori informazioniACLs, consulta la panoramica di Access control list (ACL) nella Amazon Simple Storage Service Developer Guide.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi e meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- Limiti delle autorizzazioni: un limite di autorizzazioni è una funzionalità avanzata in cui si impostano le autorizzazioni massime che una politica basata sull'identità può concedere a un'entità

(utente o ruolo). IAM IAM È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal`sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità nella Guida per l'utente. IAM IAM

- Politiche di controllo del servizio (SCPs): SCPs sono JSON politiche che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in. AWS Organizations AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più Account AWS di proprietà dell'azienda. Se abiliti tutte le funzionalità di un'organizzazione, puoi applicare le politiche di controllo del servizio (SCPs) a uno o tutti i tuoi account. SCPLimita le autorizzazioni per le entità negli account dei membri, inclusa ciascuna Utente root dell'account AWS. Per ulteriori informazioni su Organizations andSCPs, consulta le politiche di controllo dei servizi nella Guida AWS Organizations per l'utente.
- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta le politiche di sessione nella Guida IAM per l'utente.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per informazioni su come AWS determinare se consentire una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle politiche nella Guida per l'IAMutente.

Come funziona AWS Resilience Hub con IAM

Prima di utilizzare IAM per gestire l'accesso a AWS Resilience Hub, scopri quali IAM funzionalità sono disponibili per l'uso con AWS Resilience Hub.

IAMfunzionalità che puoi usare con AWS Resilience Hub

IAMcaratteristica	AWS supporto Resilience Hub
Policy basate su identità	Sì
Policy basate su risorse	No
Azioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione della policy (specifica del servizio)	Sì
ACLs	No
ABAC(tag nelle politiche)	Parziale
Credenziali temporanee	Sì
Sessioni di accesso diretto (FAS)	Sì
Ruoli di servizio	Sì

Per avere una panoramica generale del funzionamento di AWS Resilience Hub e altri AWS servizi con la maggior parte delle IAM funzionalità, consulta AWS i servizi che funzionano con IAM nella Guida per l'IAMutente.

Politiche basate sull'identità per Resilience Hub AWS

Supporta le policy basate su identità: sì

Le politiche basate sull'identità sono documenti relativi alle politiche di JSON autorizzazione che è possibile allegare a un'identità, ad esempio un IAM utente, un gruppo di utenti o un ruolo. Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una politica basata sull'identità, consulta Creazione di politiche nella Guida per l'utente. IAM IAM

Con le politiche IAM basate sull'identità, puoi specificare azioni e risorse consentite o negate, nonché le condizioni in base alle quali le azioni sono consentite o negate. Non è possibile specificare l'entità

principale in una policy basata sull'identità perché si applica all'utente o al ruolo a cui è associato. Per ulteriori informazioni su tutti gli elementi che è possibile utilizzare in una JSON politica, vedere il riferimento agli elementi IAM JSON della politica nella Guida per l'IAMutente.

Esempi di policy basate sull'identità per Resilience Hub AWS

Per visualizzare esempi di politiche basate sull'identità di AWS Resilience Hub, vedere. Esempi di policy basate sull'identità per Resilience Hub AWS

Politiche basate sulle risorse all'interno di Resilience Hub AWS

Supporta le policy basate su risorse: no

Le politiche basate sulle risorse sono documenti di policy allegati a JSON una risorsa. Esempi di politiche basate sulle risorse sono le policy di trust dei IAM ruoli e le policy dei bucket di Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. AWS servizi

Per abilitare l'accesso tra più account, puoi specificare un intero account o IAM entità in un altro account come principale in una politica basata sulle risorse. L'aggiunta di un principale multi-account a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando il principale e la risorsa sono diversi Account AWS, un IAM amministratore dell'account fidato deve inoltre concedere all'entità principale (utente o ruolo) l'autorizzazione ad accedere alla risorsa. L'autorizzazione viene concessa collegando all'entità una policy basata sull'identità. Tuttavia, se una policy basata su risorse concede l'accesso a un principale nello stesso account, non sono richieste ulteriori policy basate su identità. Per ulteriori informazioni, consulta la sezione Cross Account Resource Access IAM nella Guida IAM per l'utente.

Azioni politiche per AWS Resilience Hub

Supporta le operazioni di policy: si

Gli amministratori possono utilizzare AWS JSON le policy per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'`Action`elemento di una JSON policy descrive le azioni che è possibile utilizzare per consentire o negare l'accesso a una policy. Le azioni politiche in genere hanno lo stesso nome dell' AWS

APIoperazione associata. Esistono alcune eccezioni, come le azioni basate solo sulle autorizzazioni che non hanno un'operazione corrispondente. API Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per visualizzare un elenco delle azioni di AWS Resilience Hub, consulta Azioni definite da AWS Resilience Hub nel Service Authorization Reference.

Le azioni politiche in AWS Resilience Hub utilizzano il seguente prefisso prima dell'azione:

```
resiliencehub
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

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

Per visualizzare esempi di politiche basate sull'identità di AWS Resilience Hub, vedere. Esempi di policy basate sull'identità per Resilience Hub AWS

Risorse politiche per Resilience Hub AWS

Supporta le risorse di policy: sì

Gli amministratori possono utilizzare AWS JSON le policy per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento `Resource` JSON policy specifica l'oggetto o gli oggetti a cui si applica l'azione. Le istruzioni devono includere un elemento `Resource`o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il relativo Amazon Resource Name (ARN). Puoi eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

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

Per visualizzare un elenco dei tipi di risorse di AWS Resilience Hub e relativiARNs, consulta Resources defined by AWS Resilience Hub nel Service Authorization Reference. Per sapere con quali azioni è possibile specificare il tipo ARN di ciascuna risorsa, consulta Azioni definite da AWS Resilience Hub.

Per visualizzare esempi di politiche basate sull'identità di AWS Resilience Hub, vedere. Esempi di policy basate sull'identità per Resilience Hub AWS

Chiavi delle condizioni politiche per Resilience Hub AWS

Supporta le chiavi di condizione delle policy specifiche del servizio: sì

Gli amministratori possono utilizzare AWS JSON le policy per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Condition`(o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition`è facoltativo. Puoi compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

Se specifichi più elementi `Condition`in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione `AND`logica. Se si specificano più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione logica`OR`. Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, è possibile concedere a un IAM utente l'autorizzazione ad accedere a una risorsa solo se è contrassegnata con il suo nome IAM utente. Per ulteriori informazioni, consulta gli elementi IAM della politica: variabili e tag nella Guida IAM per l'utente.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche del servizio. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'IAMutente.

Per visualizzare un elenco delle chiavi di condizione di AWS Resilience Hub, consulta Chiavi di condizione per AWS Resilience Hub nel Service Authorization Reference Reference. Per sapere con

quali azioni e risorse è possibile utilizzare una chiave di condizione, consulta Azioni definite da AWS Resilience Hub.

Per visualizzare esempi di politiche basate sull'identità di AWS Resilience Hub, vedere. Esempi di policy basate sull'identità per Resilience Hub AWS

ACLs AWS in Resilience Hub

SupportiACLs: no

Le liste di controllo degli accessi (ACLs) controllano quali principali (membri dell'account, utenti o ruoli) dispongono delle autorizzazioni per accedere a una risorsa. ACLssono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy. JSON

ABACcon Resilience Hub AWS

Supporti ABAC (tag nelle politiche): Parziale

Il controllo degli accessi basato sugli attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, questi attributi sono chiamati tag. È possibile allegare tag a IAM entità (utenti o ruoli) e a molte AWS risorse. L'etichettatura di entità e risorse è il primo passo diABAC. Quindi si progettano ABAC politiche per consentire le operazioni quando il tag del principale corrisponde al tag sulla risorsa a cui sta tentando di accedere.

ABACè utile in ambienti in rapida crescita e aiuta in situazioni in cui la gestione delle politiche diventa complicata.

Per controllare l'accesso basato su tag, fornisci informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Yes (Sì). Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per ulteriori informazioni suABAC, vedere Cos'è? ABAC nella Guida IAM per l'utente. Per visualizzare un tutorial con i passaggi per la configurazioneABAC, consulta Utilizzare il controllo di accesso basato sugli attributi (ABAC) nella Guida per l'IAMutente.

Utilizzo di credenziali temporanee con Resilience Hub AWS

Supporta le credenziali temporanee: sì

Alcune AWS servizi non funzionano quando accedi utilizzando credenziali temporanee. Per ulteriori informazioni, incluse quelle che AWS servizi funzionano con credenziali temporanee, consulta la sezione AWS servizi relativa alla funzionalità IAM nella Guida per l'IAMutente.

Si utilizzano credenziali temporanee se si accede AWS Management Console utilizzando qualsiasi metodo tranne il nome utente e la password. Ad esempio, quando accedete AWS utilizzando il link Single Sign-on (SSO) della vostra azienda, tale processo crea automaticamente credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sul cambio di ruolo, consulta Passare a un ruolo (console) nella Guida per l'IAMutente.

È possibile creare manualmente credenziali temporanee utilizzando AWS CLI o AWS API. È quindi possibile utilizzare tali credenziali temporanee per accedere. AWS AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, vedere Credenziali di sicurezza temporanee in. IAM

Sessioni di accesso diretto per AWS Resilience Hub

Supporta sessioni di accesso diretto (FAS): Sì

Quando utilizzi un IAM utente o un ruolo per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FASutilizza le autorizzazioni del principale che chiama an AWS servizio, in combinazione con la richiesta AWS servizio per effettuare richieste ai servizi downstream. FASle richieste vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri AWS servizi o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli FAS delle politiche relative alle richieste, consulta Forward access sessions.

Ruoli di servizio per AWS Resilience Hub

Supporta i ruoli di servizio: sì

Un ruolo di servizio è un IAMruolo che un servizio assume per eseguire azioni per conto dell'utente. Un IAM amministratore può creare, modificare ed eliminare un ruolo di servizio dall'internoIAM. Per ulteriori informazioni, vedere Creazione di un ruolo per delegare le autorizzazioni a un utente AWS servizio nella Guida per l'IAMutente.

> **Warning**
>
> La modifica delle autorizzazioni per un ruolo di servizio potrebbe interrompere la funzionalità di AWS Resilience Hub. Modifica i ruoli di servizio solo quando AWS Resilience Hub fornisce indicazioni in tal senso.

Esempi di policy basate sull'identità per Resilience Hub AWS

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare AWS le risorse di Resilience Hub. Inoltre, non possono eseguire attività utilizzando AWS Management Console, AWS Command Line Interface (AWS CLI) o AWS API. Per concedere agli utenti il permesso di eseguire azioni sulle risorse di cui hanno bisogno, un IAM amministratore può creare IAM policy. L'amministratore può quindi aggiungere le IAM politiche ai ruoli e gli utenti possono assumerli.

Per informazioni su come creare una politica IAM basata sull'identità utilizzando questi documenti di esempioJSON, consulta Creazione di IAM politiche nella Guida per l'IAMutente.

Per i dettagli sulle azioni e sui tipi di risorse definiti da AWS Resilience Hub, incluso il formato di ARNs per ogni tipo di risorsa, consulta Azioni, risorse e chiavi di condizione per AWS Resilience Hub nel Service Authorization Reference Reference.

Argomenti

- Best practice per le policy
- Utilizzo della console AWS Resilience Hub
- Consentire agli utenti di visualizzare le loro autorizzazioni
- Elenco delle applicazioni disponibili AWS Resilience Hub
- Avvio di una valutazione dell'applicazione
- Eliminazione di una valutazione dell'applicazione
- Creazione di un modello di raccomandazione per un'applicazione specifica
- Eliminazione di un modello di raccomandazione per un'applicazione specifica
- Aggiornamento di un'applicazione con una politica di resilienza specifica

Best practice per le policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare le risorse di AWS Resilience Hub nel tuo account. Queste azioni possono comportare costi aggiuntivi per l' Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche gestite che concedono le autorizzazioni per molti casi d'uso comuni.AWS Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta le politiche AWS gestite o le politiche AWS gestite per le funzioni lavorative nella Guida per l'IAMutente.
- Applica le autorizzazioni con privilegi minimi: quando imposti le autorizzazioni con le IAM politiche, concedi solo le autorizzazioni necessarie per eseguire un'attività. Puoi farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo per applicare le autorizzazioni, consulta Politiche e autorizzazioni nella Guida IAM per l'utente. IAM IAM
- Utilizza le condizioni nelle IAM politiche per limitare ulteriormente l'accesso: puoi aggiungere una condizione alle tue politiche per limitare l'accesso ad azioni e risorse. Ad esempio, puoi scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzandoSSL. È inoltre possibile utilizzare condizioni per concedere l'accesso alle azioni di servizio se vengono utilizzate tramite uno specifico AWS servizio, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta Elementi IAM JSON della politica: Condizione nella Guida IAM per l'utente.
- Usa IAM Access Analyzer per convalidare IAM le tue policy e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio delle IAM policy () e alle best practice. JSON IAM IAMAccess Analyzer fornisce più di 100 controlli delle politiche e consigli pratici per aiutarti a creare policy sicure e funzionali. Per ulteriori informazioni, vedere Convalida delle policy di IAM Access Analyzer nella Guida per l'utente. IAM
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede l'utilizzo di IAM utenti o di un utente root Account AWS, attiva questa opzione MFA per una maggiore sicurezza. Per richiedere MFA quando vengono richiamate API le operazioni, aggiungi MFA delle condizioni alle tue politiche. Per ulteriori informazioni, vedere Configurazione dell'APIaccesso MFA protetto nella Guida per l'IAMutente.

Per ulteriori informazioni sulle procedure consigliate inIAM, consulta la sezione Procedure consigliate in materia di sicurezza IAM nella Guida per l'IAMutente.

Utilizzo della console AWS Resilience Hub

Per accedere alla console AWS Resilience Hub, è necessario disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle risorse di AWS Resilience Hub presenti nel tuo. Account AWS Se crei una policy basata sull'identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti o ruoli) associate a tale policy.

Non è necessario consentire autorizzazioni minime per la console per gli utenti che effettuano chiamate solo verso la o la AWS CLI . AWS API Consenti invece l'accesso solo alle azioni che corrispondono all'APIoperazione che stanno cercando di eseguire.

Per garantire che utenti e ruoli possano ancora utilizzare la console AWS Resilience Hub, collega anche il AWS Resilience Hub *ConsoleAccess* o la policy *ReadOnly* AWS gestita alle entità. Per ulteriori informazioni, consulta Aggiungere autorizzazioni a un utente nella Guida per l'utente. IAM

La seguente politica concede agli utenti l'autorizzazione a elencare e visualizzare tutte le risorse nella AWS Resilience Hub console, ma non a crearle, aggiornarle o eliminarle.

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

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra come è possibile creare una politica che consenta IAM agli utenti di visualizzare le politiche in linea e gestite allegate alla propria identità utente. Questa politica include le autorizzazioni per completare questa azione sulla console o utilizzando o a livello di codice. AWS CLI 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": "*"
        }
    ]
}
```

Elenco delle applicazioni disponibili AWS Resilience Hub

La seguente politica concede agli utenti il permesso di elencare AWS Resilience Hub le applicazioni disponibili.

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

```
      "Effect": "Allow",
      "Action": [
          "resiliencehub:ListApps"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Avvio di una valutazione dell'applicazione

La seguente politica concede agli utenti il permesso di avviare una valutazione per un' AWS Resilience Hub applicazione specifica.

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

Eliminazione di una valutazione dell'applicazione

La seguente politica concede agli utenti l'autorizzazione a eliminare una valutazione per un'applicazione specifica AWS Resilience Hub .

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

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

Creazione di un modello di raccomandazione per un'applicazione specifica

La seguente politica concede agli utenti l'autorizzazione a creare un modello di raccomandazione per un' AWS Resilience Hub applicazione specifica.

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

Eliminazione di un modello di raccomandazione per un'applicazione specifica

La seguente politica concede agli utenti l'autorizzazione a eliminare un modello di raccomandazione per un'applicazione specifica AWS Resilience Hub .

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

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

Aggiornamento di un'applicazione con una politica di resilienza specifica

La seguente politica concede agli utenti l'autorizzazione ad aggiornare un' AWS Resilience Hub applicazione con una politica di resilienza specifica.

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

Imposta IAM ruoli e autorizzazioni

AWS Resilience Hub consente di configurare i IAM ruoli che si desidera utilizzare durante l'esecuzione delle valutazioni per l'applicazione. Esistono diversi modi di configurazione per ottenere AWS Resilience Hub l'accesso in sola lettura alle risorse dell'applicazione. Tuttavia, AWS Resilience Hub consiglia le seguenti modalità:

- Accesso basato sul ruolo: questo ruolo viene definito e utilizzato nell'account corrente. AWS Resilience Hub assumerà questo ruolo per accedere alle risorse dell'applicazione.

  Per fornire un accesso basato sui ruoli, il ruolo deve includere quanto segue:

  - Autorizzazione di sola lettura per leggere le risorse (AWS Resilience Hub consiglia di utilizzare la `AWSResilienceHubAsssessmentExecutionPolicy` politica gestita).
  - Politica di fiducia per l'assunzione di questo ruolo, che consente a AWS Resilience Hub Service Principal di assumerlo. Se non hai un ruolo di questo tipo configurato nel tuo account, AWS Resilience Hub verranno visualizzate le istruzioni per creare quel ruolo. Per ulteriori informazioni, consulta the section called “Fase 6: Autorizzazioni di configurazione”.

  > **Note**
  >
  > Se fornisci solo il nome del ruolo dell'invoker e se le tue risorse si trovano in un altro account, AWS Resilience Hub utilizzerà questo nome di ruolo negli altri account per accedere alle risorse tra account. Facoltativamente, puoi configurare il ruolo ARNs per altri account, che verranno utilizzati al posto del nome del ruolo invoker.

- Accesso IAM utente corrente: AWS Resilience Hub utilizzerà l'IAMutente corrente per accedere alle risorse dell'applicazione. Quando le tue risorse si trovano in un account diverso, AWS Resilience Hub assumerà i seguenti IAM ruoli per accedere alle risorse:
  - `AwsResilienceHubAdminAccountRole`nell'account corrente
  - `AwsResilienceHubExecutorAccountRole`in altri conti

  Inoltre, quando configuri una valutazione pianificata, AWS Resilience Hub assumerà il `AwsResilienceHubPeriodicAssessmentRole` ruolo. Tuttavia, l'utilizzo non `AwsResilienceHubPeriodicAssessmentRole` è consigliato perché è necessario configurare manualmente ruoli e autorizzazioni e alcune funzionalità (come la notifica Drift) potrebbero non funzionare come previsto.

Risoluzione dei problemi relativi all'identità e all'accesso a AWS Resilience Hub

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi comuni che potresti riscontrare quando lavori con AWS Resilience Hub e. IAM

Argomenti

- Non sono autorizzato a eseguire un'azione in AWS Resilience Hub
- Non sono autorizzato a eseguire iam: PassRole
- Voglio consentire a persone esterne a me di accedere Account AWS alle risorse del mio AWS Resilience Hub

Non sono autorizzato a eseguire un'azione in AWS Resilience Hub

Se ricevi un errore che indica che non disponi dell'autorizzazione per eseguire un'operazione, le tue policy devono essere aggiornate in modo che ti sei consentito eseguire tale operazione.

L'errore di esempio seguente si verifica quando l'`mateojacksonIAM`utente tenta di utilizzare la console per visualizzare i dettagli su una *`my-example-widget`* risorsa fittizia ma non dispone delle autorizzazioni fittizie. `resiliencehub:`*`GetWidget`*

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

In questo caso, la policy per l'utente `mateojackson` deve essere aggiornata per consentire l'accesso alla risorsa *`my-example-widget`* utilizzando l'azione `resiliencehub:`*`GetWidget`*.

Se hai bisogno di assistenza, contatta l'amministratore. AWS L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Non sono autorizzato a eseguire iam: PassRole

Se ricevi un messaggio di errore indicante che non sei autorizzato a eseguire l'`iam:PassRole`azione, le tue politiche devono essere aggiornate per consentirti di trasferire un ruolo a AWS Resilience Hub.

Alcuni AWS servizi consentono di trasferire un ruolo esistente a quel servizio invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

L'errore di esempio seguente si verifica quando un IAM utente denominato `marymajor` tenta di utilizzare la console per eseguire un'azione in AWS Resilience Hub. Tuttavia, l'azione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per passare il ruolo al servizio.

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

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Voglio consentire a persone esterne a me di accedere Account AWS alle risorse del mio AWS Resilience Hub

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per i servizi che supportano politiche basate sulle risorse o liste di controllo degli accessi (ACLs), puoi utilizzare tali politiche per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se AWS Resilience Hub supporta queste funzionalità, consulta. Come funziona AWS Resilience Hub con IAM
- Per informazioni su Account AWS come fornire l'accesso alle risorse di tua proprietà, consulta Fornire l'accesso a un IAM utente di un altro Account AWS utente di tua proprietà nella Guida per l'IAMutente.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a persone Account AWS di proprietà di terzi nella Guida per l'IAMutente.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso agli utenti autenticati esternamente (federazione delle identità) nella Guida per l'IAMutente.
- Per conoscere la differenza tra l'utilizzo di ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta la sezione Accesso alle risorse tra account nella Guida per l'utente. IAM IAM

AWS Resilience Hub riferimento alle autorizzazioni di accesso

È possibile utilizzare AWS Identity and Access Management (IAM) per gestire l'accesso alle risorse dell'applicazione e creare IAM politiche applicabili a utenti, gruppi o ruoli.

Ogni AWS Resilience Hub applicazione può essere configurata per utilizzare the section called "Ruolo invoker" (un IAM ruolo) o utilizzare le autorizzazioni IAM utente correnti (insieme a una serie di ruoli predefiniti per la valutazione pianificata e tra più account). In questo ruolo, è possibile allegare una politica che definisce le autorizzazioni richieste AWS Resilience Hub per accedere ad altre AWS risorse o risorse dell'applicazione. Il ruolo invoker deve avere una politica di fiducia che viene aggiunta a AWS Resilience Hub Service Principal.

Per gestire le autorizzazioni per la tua applicazione, ti consigliamo di utilizzare. the section called "AWS politiche gestite" È possibile utilizzare queste politiche gestite senza alcuna modifica oppure utilizzarle come punto di partenza per scrivere politiche restrittive personalizzate. Le politiche possono limitare le autorizzazioni degli utenti a livello di risorsa per diverse azioni utilizzando condizioni opzionali aggiuntive.

Se le risorse dell'applicazione si trovano in account diversi (account secondari/di risorse), è necessario impostare un nuovo ruolo in ogni account che contiene le risorse dell'applicazione.

Argomenti

- the section called "Utilizzo del IAM ruolo"
- the section called "Utilizzo delle autorizzazioni IAM utente correnti"

Utilizzo del ruolo IAM

AWS Resilience Hub utilizzerà un IAM ruolo esistente predefinito per accedere alle risorse nell'account principale o nell'account secondario/delle risorse. Questa è l'opzione di autorizzazione consigliata per accedere alle tue risorse.

Argomenti

- the section called "Ruolo invoker"
- the section called "Ruoli in AWS account diversi per l'accesso su più account"

Ruolo invoker

Il ruolo AWS Resilience Hub invoker è un ruolo AWS Identity and Access Management (IAM) che AWS Resilience Hub presuppone l'accesso a servizi e risorse. AWS Ad esempio, potresti creare un ruolo invoker con l'autorizzazione ad accedere al tuo CFN modello e alla risorsa che crea. Questa pagina fornisce informazioni su come creare, visualizzare e gestire un ruolo Application Invoker.

Quando si crea un'applicazione, si fornisce un ruolo di invoker. AWS Resilience Hub assume questo ruolo per accedere alle risorse quando si importano risorse o si avvia una valutazione. AWS Resilience Hub Per assumere correttamente il ruolo di invoker, la politica di fiducia del ruolo deve specificare il AWS Resilience Hub service principal (resiliencehub.amazonaws.com) come servizio affidabile.

Per visualizzare il ruolo di invoker dell'applicazione, scegli Applicazioni dal riquadro di navigazione, quindi scegli Aggiorna autorizzazioni dal menu Azioni nella pagina Applicazione.

È possibile aggiungere o rimuovere le autorizzazioni da un ruolo di richiamo dell'applicazione in qualsiasi momento oppure configurare l'applicazione in modo che utilizzi un ruolo diverso per l'accesso alle risorse dell'applicazione.

Argomenti

- the section called “Creazione di un ruolo di invoker nella console IAM”
- the section called “Gestione dei ruoli con IAM API”
- the section called “Definizione della politica di fiducia tramite JSON file”

Creazione di un ruolo di invoker nella console IAM

Per consentire l'accesso AWS Resilience Hub a AWS servizi e risorse, è necessario creare un ruolo di invoker nell'account principale utilizzando la console. IAM Per ulteriori informazioni sulla creazione di ruoli utilizzando la IAM console, vedere Creazione di un ruolo per un AWS servizio (console).

Per creare un ruolo di invoker nell'account principale utilizzando la console IAM

1. Apri la console IAM all'indirizzo `https://console.aws.amazon.com/iam/`.
2. Dal riquadro di navigazione, scegli Ruoli, quindi scegli Crea ruolo.
3. Seleziona Criteri di fiducia personalizzati, copia i seguenti criteri nella finestra Criteri di fiducia personalizzati, quindi scegli Avanti.

> **Note**
>
> Se le tue risorse si trovano in account diversi, devi creare un ruolo in ciascuno di questi account e utilizzare la politica di fiducia degli account secondari per gli altri account.

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

4. Nella sezione Politiche di autorizzazione della pagina Aggiungi autorizzazioni, inserisci `AWSResilienceHubAsssessmentExecutionPolicy` le politiche di filtro per proprietà o nome della politica e premi invio.
5. Seleziona la politica e scegli Avanti.
6. Nella sezione Dettagli del ruolo, inserisci un nome di ruolo univoco (ad esempio`AWSResilienceHubAssessmentRole`) nella casella Nome ruolo.

   Questo campo accetta solo caratteri alfanumerici e «`+=,.@-_/`».
7. (Facoltativo) Inserisci una descrizione del ruolo nella casella Descrizione.
8. Selezionare Create Role (Crea ruolo).

   Per modificare i casi d'uso e le autorizzazioni, nel passaggio 6, scegli il pulsante Modifica che si trova a destra delle sezioni Passaggio 1: Seleziona entità attendibili o Passaggio 2: Aggiungi autorizzazioni.

Dopo aver creato il ruolo invoker e il ruolo di risorsa (se applicabile), puoi configurare l'applicazione per utilizzare questi ruoli.

> **Note**
>
> È necessario disporre `iam:passRole` dell'autorizzazione dell'IAMutente/ruolo corrente per il ruolo invoker durante la creazione o l'aggiornamento dell'applicazione. Tuttavia, non è necessaria questa autorizzazione per eseguire una valutazione.

Gestione dei ruoli con IAM API

La politica di fiducia di un ruolo fornisce al principale specificato il permesso di assumere il ruolo. Per creare i ruoli usando AWS Command Line Interface (AWS CLI), usa il `create-role` comando. Durante l'utilizzo di questo comando, è possibile specificare la politica di fiducia in linea. L'esempio seguente mostra come concedere al AWS Resilience Hub servizio l'autorizzazione principale per assumere il proprio ruolo.

> **Note**
>
> Il requisito per evitare le virgolette (`' '`) nella JSON stringa può variare in base alla versione della shell.

Esempio **`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"
    }
  ]
}'
```

Definizione della politica di fiducia tramite JSON file

È possibile definire la politica di fiducia per il ruolo utilizzando un JSON file separato e quindi eseguire il `create-role` comando. Nell'esempio seguente, **`trust-policy.json`**è un file che contiene la politica di attendibilità nella directory corrente. Questa politica è associata a un ruolo mediante l'esecuzione del **`create-role`**comando. L'output del **`create-role`** comando è mostrato nell'output di esempio. Per aggiungere autorizzazioni al ruolo, usa il attach-policy-to-rolecomando e puoi iniziare aggiungendo la politica `AWSResilienceHubAsssessmentExecutionPolicy` gestita. Per ulteriori informazioni su questa politica gestita, consultathe section called “AWSResilienceHubAsssessmentExecutionPolicy”.

Esempio **`trust-policy.json`**

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

Esempio **`create-role`**

```
aws iam create-role --role-name AWSResilienceHubAssessmentRole --assume-role-policy-document file://trust-policy.json
```

Esempio di output

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

Esempio **`attach-policy-to-role`**

```
aws iam attach-role-policy --role-name AWSResilienceHubAssessmentRole --
policy-arn arn:aws:iam::aws:policy/
AWSResilienceHubAsssessmentExecutionPolicy
```

Ruoli in AWS account diversi per l'accesso su più account - opzionale

Se le risorse si trovano in account secondari/di risorse, è necessario creare ruoli in ciascuno di questi account per consentire una valutazione corretta della AWS Resilience Hub candidatura. La procedura di creazione dei ruoli è simile al processo di creazione del ruolo dell'invoker, ad eccezione della configurazione della politica di fiducia.

> **Note**
>
> È necessario creare i ruoli negli account secondari in cui si trovano le risorse.

Argomenti

- the section called “Creazione di un ruolo nella IAM console per gli account secondari/di risorse”
- the section called “Gestione dei ruoli con IAM API”
- the section called “Definizione della politica di fiducia tramite JSON file”

Creazione di un ruolo nella IAM console per gli account secondari/di risorse

Per consentire l'accesso AWS Resilience Hub ai AWS servizi e alle risorse in altri AWS account, è necessario creare ruoli in ciascuno di questi account.

Per creare un ruolo nella IAM console per gli account secondari/di risorsa utilizzando la console IAM

1. Apri la console IAM all'indirizzo `https://console.aws.amazon.com/iam/`.
2. Dal riquadro di navigazione, scegli Ruoli, quindi scegli Crea ruolo.
3. Seleziona Criteri di fiducia personalizzati, copia i seguenti criteri nella finestra Criteri di fiducia personalizzati, quindi scegli Avanti.

   > **Note**
   >
   > Se le tue risorse si trovano in account diversi, devi creare un ruolo in ciascuno di questi account e utilizzare la politica di fiducia degli account secondari per gli altri account.

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

4. Nella sezione Politiche di autorizzazione della pagina Aggiungi autorizzazioni, inserisci `AWSResilienceHubAsssessmentExecutionPolicy` le politiche di filtro per proprietà o nome della politica e premi invio.
5. Seleziona la politica e scegli Avanti.
6. Nella sezione Dettagli del ruolo, inserisci un nome di ruolo univoco (ad esempio`AWSResilienceHubAssessmentRole`) nella casella Nome ruolo.
7. (Facoltativo) Inserisci una descrizione del ruolo nella casella Descrizione.
8. Selezionare Create Role (Crea ruolo).

   Per modificare i casi d'uso e le autorizzazioni, nel passaggio 6, scegli il pulsante Modifica che si trova a destra delle sezioni Passaggio 1: Seleziona entità attendibili o Passaggio 2: Aggiungi autorizzazioni.

Inoltre, devi anche aggiungere l'`sts:assumeRole`autorizzazione al ruolo di invoker per consentirgli di assumere i ruoli nei tuoi account secondari.

Aggiungi la seguente politica al tuo ruolo di invoker per ciascuno dei ruoli secondari che hai creato:

```
{
    "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"
      ]
}
```

Gestione dei ruoli con IAM API

La politica di fiducia di un ruolo fornisce al principale specificato il permesso di assumere il ruolo. Per creare i ruoli usando AWS Command Line Interface (AWS CLI), usa il `create-role` comando. Quando utilizzi questo comando, puoi specificare la policy di attendibilità in linea. L'esempio seguente mostra come concedere al responsabile del AWS Resilience Hub servizio l'autorizzazione ad assumere il proprio ruolo.

> **Note**
>
> Il requisito per evitare le virgolette (`'  '`) nella JSON stringa può variare in base alla versione della shell.

Esempio **`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"}]}'
```

È inoltre possibile definire la politica di attendibilità per il ruolo utilizzando un JSON file separato. Nell'esempio seguente, `trust-policy.json` è un file che si trova nella directory attuale.

Definizione della politica di fiducia tramite JSON file

È possibile definire la politica di fiducia per il ruolo utilizzando un JSON file separato e quindi eseguire il `create-role` comando. Nell'esempio seguente, **`trust-policy.json`**è un file che contiene la politica di attendibilità nella directory corrente. Questa politica è associata a un ruolo mediante l'esecuzione del **`create-role`**comando. L'output del **`create-role`** comando è mostrato nell'output di esempio. Per aggiungere autorizzazioni a un ruolo, usa il attach-policy-to-rolecomando e puoi iniziare aggiungendo la politica `AWSResilienceHubAsssessmentExecutionPolicy`

gestita. Per ulteriori informazioni su questa politica gestita, consultathe section called "AWSResilienceHubAsssessmentExecutionPolicy".

Esempio **trust-policy.json**

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

Esempio **create-role**

```
aws iam create-role --role-name AWSResilienceHubAssessmentRole --assume-role-policy-
document file://trust-policy.json
```

Esempio di output

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

Esempio **`attach-policy-to-role`**

`aws iam attach-role-policy --role-name AWSResilienceHubAssessmentRole --policy-arn arn:aws:iam::aws:policy/AWSResilienceHubAsssessmentExecutionPolicy`.

Utilizzo delle autorizzazioni IAM utente correnti

Utilizzate questo metodo se desiderate utilizzare le vostre attuali autorizzazioni IAM utente per creare ed eseguire una valutazione. Puoi allegare la politica `AWSResilienceHubAsssessmentExecutionPolicy` gestita al tuo IAM utente o a un ruolo associato al tuo utente.

Configurazione di un account singolo

L'utilizzo della politica gestita sopra menzionata è sufficiente per eseguire una valutazione su un'applicazione gestita nello stesso account dell'IAMutente.

Configurazione della valutazione pianificata

È necessario creare un nuovo ruolo `AwsResilienceHubPeriodicAssessmentRole` per consentire l'esecuzione AWS Resilience Hub di attività relative alla valutazione pianificata.

> **Note**
>
> - Durante l'utilizzo dell'accesso basato sui ruoli (con il ruolo di invoker menzionato sopra) questo passaggio non è richiesto.
> - Il nome del ruolo deve essere. `AwsResilienceHubPeriodicAssessmentRole`

Per consentire AWS Resilience Hub l'esecuzione di attività pianificate relative alla valutazione

1. Allega la politica `AWSResilienceHubAsssessmentExecutionPolicy` gestita al ruolo.
2. Aggiungi la seguente politica, `primary_account_id` dov'è l' AWS account in cui è definita l'applicazione e dove verrà eseguita la valutazione. Inoltre, è necessario aggiungere la politica di attendibilità associata per il ruolo della valutazione pianificata, (`AwsResilienceHubPeriodicAssessmentRole`), che concede le autorizzazioni affinché il AWS Resilience Hub servizio assuma il ruolo della valutazione pianificata.

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

Politica di fiducia per il ruolo della valutazione pianificata () **`AwsResilienceHubPeriodicAssessmentRole`**

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

```
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "resiliencehub.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Configurazione tra più account

Le seguenti politiche di IAM autorizzazione sono necessarie se utilizzi AWS Resilience Hub con più account. Ogni AWS account potrebbe richiedere autorizzazioni diverse a seconda del caso d'uso. Durante la configurazione AWS Resilience Hub per l'accesso tra account diversi, vengono presi in considerazione i seguenti account e ruoli:

- Account principale: AWS account in cui si desidera creare l'applicazione ed eseguire le valutazioni.
- Account secondario/di risorse: AWS account in cui si trovano le risorse.

> **Note**
>
> - Durante l'utilizzo dell'accesso basato sui ruoli (con il ruolo di invoker menzionato sopra) questo passaggio non è richiesto.
> - Per ulteriori informazioni sulla configurazione delle autorizzazioni per accedere ad Amazon Elastic Kubernetes Service, consulta. the section called “Abilitare AWS Resilience Hub l'accesso al tuo EKS cluster Amazon”

Configurazione dell'account principale

È necessario creare un nuovo ruolo `AwsResilienceHubAdminAccountRole` nell'account principale e abilitare AWS Resilience Hub l'accesso per assumerlo. Questo ruolo verrà utilizzato per accedere a un altro ruolo nel tuo AWS account che contiene le tue risorse. Non dovrebbe avere le autorizzazioni per leggere le risorse.

> **Note**
>
> - Il nome del ruolo deve essere`AwsResilienceHubAdminAccountRole`.
> - Deve essere creato nell'account principale.
> - L'IAMutente/ruolo corrente deve avere l'`iam:assumeRole`autorizzazione per assumere questo ruolo.
> - `secondary_account_id_1/2/...`Sostituiscilo con gli identificatori di account secondari pertinenti.

La seguente politica fornisce le autorizzazioni di esecutore al tuo ruolo per accedere alle risorse in un altro ruolo del tuo account: 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"
      ]
    }
  ]
}
```

La politica di fiducia per il ruolo di amministratore (`AwsResilienceHubAdminAccountRole`) è la seguente:

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

Configurazione degli account secondari/di risorsa

In ciascuno dei tuoi account secondari, devi crearne uno nuovo `AwsResilienceHubExecutorAccountRole` e abilitare il ruolo di amministratore creato sopra per assumere questo ruolo. Poiché questo ruolo verrà utilizzato AWS Resilience Hub per analizzare e valutare le risorse dell'applicazione, richiederà anche le autorizzazioni appropriate.

Tuttavia, è necessario allegare la politica `AWSResilienceHubAsssessmentExecutionPolicy` gestita al ruolo e la politica del ruolo di esecutore.

La politica di attendibilità del ruolo dell'esecutore è la seguente:

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

AWS politiche gestite per AWS Resilience Hub

Una politica AWS gestita è una politica autonoma creata e amministrata da AWS. AWS le politiche gestite sono progettate per fornire autorizzazioni per molti casi d'uso comuni, in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Tieni presente che le policy AWS gestite potrebbero non concedere le autorizzazioni con il privilegio minimo per i tuoi casi d'uso specifici, poiché sono disponibili per tutti i clienti. AWS Ti consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente specifiche per i tuoi casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle politiche gestite. AWS Se AWS aggiorna le autorizzazioni definite in una politica AWS gestita, l'aggiornamento ha effetto su tutte le identità principali (utenti, gruppi e ruoli) a cui è associata la politica. AWS è più probabile che aggiorni una policy AWS gestita quando ne AWS servizio viene lanciata una nuova o quando diventano disponibili nuove API operazioni per i servizi esistenti.

Per ulteriori informazioni, consulta le politiche AWS gestite nella Guida IAM per l'utente.

AWSResilienceHubAsssessmentExecutionPolicy

Puoi allegarli `AWSResilienceHubAsssessmentExecutionPolicy` alle tue IAM identità. Durante l'esecuzione di una valutazione, questa politica concede le autorizzazioni di accesso ad altri AWS servizi per l'esecuzione delle valutazioni.

Dettagli dell'autorizzazione

Questa politica fornisce autorizzazioni adeguate per pubblicare allarmi AWS FIS e SOP modelli nel tuo bucket Amazon Simple Storage Service (Amazon S3). Il nome del bucket Amazon S3 deve iniziare con. `aws-resilience-hub-artifacts-` Se desideri pubblicare su un altro bucket Amazon S3, puoi farlo mentre chiami. `CreateRecommendationTemplate` API Per ulteriori informazioni, consulta. CreateRecommendationTemplate

Questa policy include le seguenti autorizzazioni:

- Amazon CloudWatch (CloudWatch): riceve tutti gli allarmi implementati che configuri in Amazon CloudWatch per monitorare l'applicazione. Inoltre, pubblichiamo `cloudwatch:PutMetricData` le CloudWatch metriche per il punteggio di resilienza dell'applicazione nel namespace. `ResilienceHub`

- Amazon Data Lifecycle Manager: ottiene e fornisce `Describe` le autorizzazioni per le risorse Amazon Data Lifecycle Manager associate al tuo account. AWS
- Amazon DevOps Guru: elenca e fornisce `Describe` le autorizzazioni per le risorse Amazon DevOps Guru associate al tuo account. AWS
- Amazon DocumentDB: elenca e fornisce `Describe` le autorizzazioni per le risorse Amazon DocumentDB associate al tuo account. AWS
- Amazon DynamoDB (DynamoDB): elenca e fornisce le `Describe` autorizzazioni per le risorse Amazon DynamoDB associate al tuo account. AWS
- Amazon ElastiCache (ElastiCache): fornisce `Describe` le autorizzazioni per ElastiCache le risorse associate al tuo AWS account.
- Amazon Elastic Compute Cloud (AmazonEC2): elenca e fornisce `Describe` le autorizzazioni per EC2 le risorse Amazon associate al tuo AWS account.
- Amazon Elastic Container Registry (AmazonECR): fornisce `Describe` le autorizzazioni per ECR le risorse Amazon associate al tuo AWS account.
- Amazon Elastic Container Service (AmazonECS): fornisce `Describe` le autorizzazioni per ECS le risorse Amazon associate al tuo AWS account.
- Amazon Elastic File System (AmazonEFS): fornisce `Describe` le autorizzazioni per EFS le risorse Amazon associate al tuo AWS account.
- Amazon Elastic Kubernetes Service (EKSAmazon): elenca e `Describe` fornisce le autorizzazioni per le risorse EKS Amazon associate al tuo account. AWS
- Amazon EC2 Auto Scaling: elenca e fornisce le `Describe` autorizzazioni per le risorse Amazon EC2 Auto Scaling associate al tuo account. AWS
- Amazon EC2 Systems Manager (SSM): fornisce `Describe` le autorizzazioni per SSM le risorse associate al tuo AWS account.
- Amazon Fault Injection Service (AWS FIS): elenca e fornisce `Describe` le autorizzazioni per AWS FIS esperimenti e modelli di esperimenti associati al tuo AWS account.
- Amazon FSx for Windows File Server (AmazonFSx): elenca e fornisce `Describe` le autorizzazioni per FSx le risorse Amazon associate al tuo AWS account.
- AmazonRDS: elenca e fornisce `Describe` le autorizzazioni per RDS le risorse Amazon associate al tuo AWS account.
- Amazon Route 53 (Route 53): elenca e fornisce `Describe` le autorizzazioni per le risorse Route 53 associate al tuo AWS account.

- Amazon Route 53 Resolver — Elenca e fornisce `Describe` le autorizzazioni per Amazon Route 53 Resolver le risorse associate al tuo AWS account.
- Amazon Simple Notification Service (AmazonSNS): elenca e fornisce `Describe` le autorizzazioni per SNS le risorse Amazon associate al tuo AWS account.
- Amazon Simple Queue Service (AmazonSQS): elenca e fornisce `Describe` le autorizzazioni per SQS le risorse Amazon associate al tuo AWS account.
- Amazon Simple Storage Service (Amazon S3): elenca e `Describe` fornisce le autorizzazioni per le risorse Amazon S3 associate al tuo account. AWS

> **Note**
>
> Durante l'esecuzione di una valutazione, se mancano delle autorizzazioni che devono essere aggiornate dalle policy gestite, AWS Resilience Hub completerà correttamente la valutazione utilizzando s3: permission. GetBucketLogging Tuttavia, AWS Resilience Hub mostrerà un messaggio di avviso che elenca le autorizzazioni mancanti e fornirà un periodo di grazia per aggiungerle. Se non aggiungi le autorizzazioni mancanti entro il periodo di prova specificato, la valutazione avrà esito negativo.

- AWS Backup — Elenca e ottiene `Describe` le autorizzazioni per le risorse Amazon EC2 Auto Scaling associate AWS al tuo account.
- AWS CloudFormation — Elenca e ottiene `Describe` le autorizzazioni per le risorse sugli AWS CloudFormation stack associati al tuo account. AWS
- AWS DataSync — Elenca e fornisce `Describe` le autorizzazioni per AWS DataSync le risorse associate all'account. AWS
- AWS Directory Service — Elenca e fornisce `Describe` le autorizzazioni per AWS Directory Service le risorse associate all'account AWS .
- AWS Elastic Disaster Recovery (Elastic Disaster Recovery) — Fornisce `Describe` le autorizzazioni per le risorse Elastic Disaster Recovery associate all'account AWS .
- AWS Lambda (Lambda): elenca e fornisce le `Describe` autorizzazioni per le risorse Lambda associate all'account. AWS
- AWS Resource Groups (Resource Groups): elenca e fornisce `Describe` le autorizzazioni per le risorse Resource Groups associate all' AWS account.
- AWS Service Catalog (Service Catalog): elenca e fornisce `Describe` le autorizzazioni per le risorse di Service Catalog associate all' AWS account dell'utente.

- AWS Step Functions — Elenca e fornisce `Describe` le autorizzazioni per AWS Step Functions le risorse associate all'account AWS .
- Elastic Load Balancing: elenca e fornisce `Describe` le autorizzazioni per le risorse Elastic Load Balancing associate all'account. AWS
- `ssm:GetParametersByPath`— Utilizziamo questa autorizzazione per gestire CloudWatch allarmi, test o quelli configurati per SOPs l'applicazione.

La seguente IAM politica è necessaria affinché un AWS account aggiunga le autorizzazioni per utenti, gruppi di utenti e ruoli che forniscono le autorizzazioni necessarie al team per accedere ai AWS servizi durante l'esecuzione delle valutazioni.

```
{
    "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 Hub aggiornamenti alle politiche gestite AWS

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite AWS Resilience Hub da quando questo servizio ha iniziato a tenere traccia di queste modifiche. Per ricevere avvisi automatici sulle

modifiche a questa pagina, iscriviti al RSS feed nella pagina della cronologia dei AWS Resilience Hub documenti.

Modifica	Descrizione	Data
AWSResilienceHubAssessmentExecutionPolicy— Modifica	AWS Resilience Hub aggiornato `AWSResilienceHubAsssessmentExecutionPolicy` per concedere `Describe` le autorizzazioni per consentire l'accesso a risorse e configurazioni su Amazon DocumentDB, Elastic Load Balancing e durante l'esecuzione delle valutazioni. AWS Lambda	1 agosto 2024
AWSResilienceHubAssessmentExecutionPolicy— Cambia	AWS Resilience Hub aggiornato `AWSResilienceHubAsssessmentExecutionPolicy` per concedere `Describe` le autorizzazioni per consentirti di leggere la configurazione di Amazon FSx for Windows File Server durante l'esecuzione delle valutazioni.	26 marzo 2024
AWSResilienceHubAssessmentExecutionPolicy— Cambia	AWS Resilience Hub aggiornato `AWSResilienceHubAsssessmentExecutionPolicy` per concedere `Describe` le autorizzazioni per consentire di leggere la AWS Step Functions configurazione	30 ottobre 2023

Modifica	Descrizione	Data
	durante l'esecuzione delle valutazioni.	
AWSResilienceHubAssessmentExecutionPolicy— Modifica	AWS Resilience Hub aggiornato `AWSResilienceHubAsssessmentExecutionPolicy` per concedere `Describe` le autorizzazioni per consentirti di accedere alle risorse su Amazon RDS durante l'esecuzione delle valutazioni.	5 ottobre 2023
AWSResilienceHubAssessmentExecutionPolicy— Nuovo	Questa AWS Resilience Hub politica fornisce l'accesso ad altri AWS servizi per l'esecuzione delle valutazioni.	26 giugno 2023
AWS Resilience Hub ha iniziato a tenere traccia delle modifiche	AWS Resilience Hub ha iniziato a tenere traccia delle modifiche per le sue politiche AWS gestite.	15 giugno 2023

AWS Resilience Hub riferimenti a personaggi e IAM autorizzazioni

Puoi concedere le IAM autorizzazioni ai personaggi con AWS Resilience Hub cui è necessario lavorare utilizzando la politica `AWSResilienceHubAsssessmentExecutionPolicy` AWS gestita e una delle seguenti politiche specifiche per persona. Per ulteriori informazioni sulla politica AWS gestita, vedere. the section called “AWSResilienceHubAsssessmentExecutionPolicy”

Politiche per i personaggi suggerite da AWS Resilience Hub:

- IAMautorizzazioni per la persona del gestore delle applicazioni dell'infrastruttura
- IAMautorizzazioni per la persona del responsabile della continuità operativa
- IAMautorizzazioni per la persona del proprietario dell'applicazione
- IAMautorizzazioni per concedere l'accesso in sola lettura

IAMautorizzazioni per la persona del gestore delle applicazioni dell'infrastruttura

La seguente politica concede le autorizzazioni necessarie richieste per il personaggio del gestore delle applicazioni di infrastruttura.

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

IAMautorizzazioni per la persona del responsabile della continuità operativa

La seguente politica concede le autorizzazioni necessarie richieste per il personaggio di Business continuity manager.

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

IAMautorizzazioni per la persona del proprietario dell'applicazione

La seguente politica concede le autorizzazioni necessarie richieste per la persona del proprietario dell'Applicazione.

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

IAMautorizzazioni per concedere l'accesso in sola lettura

La seguente politica concede le autorizzazioni necessarie per l'accesso in sola lettura.

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

```
      "Resource": "*"
    }
  ]
}
```

Importazione del file di stato Terraform in AWS Resilience Hub

AWS Resilience Hub supporta l'importazione di file di stato Terraform crittografati utilizzando la crittografia lato server () SSE con chiavi gestite di Amazon Simple Storage Service (SSE-S3) o con AWS Key Management Service chiavi gestite (-). SSE KMS Se i tuoi file di stato Terraform sono crittografati utilizzando chiavi di crittografia fornite dal cliente (SSE-C), non potrai importarli utilizzando. AWS Resilience Hub

L'importazione di file di stato Terraform AWS Resilience Hub richiede le seguenti IAM politiche a seconda di dove si trova il file di stato.

Importazione di file di stato Terraform da un bucket Amazon S3 situato nell'account principale

Le seguenti policy e IAM policy relative ai bucket Amazon S3 sono necessarie per consentire l'accesso in AWS Resilience Hub lettura ai file di stato Terraform che si trovano in un bucket Amazon S3 sull'account principale.

- Policy bucket: una policy bucket sul bucket Amazon S3 di destinazione, che si trova nell'account principale. Per maggiori informazioni, consulta il seguente esempio:

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

- Politica di identità: la politica di identità associata per il ruolo Invoker definito per questa applicazione o il ruolo AWS corrente IAM sull'account principale. AWS Resilience Hub AWS Per maggiori informazioni, consulta il seguente esempio:

```
{
  "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**
>
> Se si utilizza la politica `AWSResilienceHubAsssessmentExecutionPolicy` gestita, l'`ListBucket`autorizzazione non è richiesta.

> **Note**
>
> Se i tuoi file di stato Terraform sono crittografati utilizzandoKMS, devi aggiungere la seguente `kms:Decrypt` autorizzazione.

```
{
```

```
      "Effect": "Allow",
      "Action": [
              "kms:Decrypt",
      ],
      "Resource": "<arn_of_kms_key>"
}
```

Importazione di file di stato Terraform da un bucket Amazon S3 situato in un account secondario

- Policy bucket: una policy bucket sul bucket Amazon S3 di destinazione, che si trova in uno degli account secondari. Per maggiori informazioni, consulta il seguente esempio:

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

- Politica di identità: la politica di identità associata per il ruolo dell' AWS account, che viene eseguita AWS Resilience Hub sull'account principale. AWS Per maggiori informazioni, consulta il seguente esempio:

```
{
  "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**
>
> Se si utilizza la politica `AWSResilienceHubAsssessmentExecutionPolicy` gestita, `ListBucket` l'autorizzazione non è richiesta.

> **Note**
>
> Se i tuoi file di stato Terraform sono crittografati utilizzandoKMS, devi aggiungere la seguente `kms:Decrypt` autorizzazione.
>
> ```
> {
> ```

```
        "Effect": "Allow",
        "Action": [
                "kms:Decrypt",
        ],
        "Resource": "<arn_of_kms_key>"
}
```

Abilitazione AWS Resilience Hub dell'accesso al tuo cluster Amazon Elastic Kubernetes Service

AWS Resilience Hub valuta la resilienza di un cluster Amazon Elastic Kubernetes Service EKS (Amazon) analizzando l'infrastruttura del cluster Amazon. EKS AWS Resilience Hub utilizza la configurazione di controllo degli accessi (RBAC) basata sul ruolo di Kubernetes per valutare altri carichi di lavoro Kubernetes (K8s), che vengono distribuiti come parte del cluster Amazon. EKS AWS Resilience Hub Per interrogare il tuo EKS cluster Amazon per l'analisi e la valutazione del carico di lavoro, devi completare quanto segue:

- Crea o usa un ruolo AWS Identity and Access Management (IAM) esistente nello stesso account del EKS cluster Amazon.
- Abilita IAM l'accesso di utenti e ruoli al tuo EKS cluster Amazon e concedi autorizzazioni di sola lettura aggiuntive alle risorse K8s all'interno del cluster Amazon. EKS Per ulteriori informazioni sull'abilitazione IAM dell'accesso di utenti e ruoli al tuo EKS cluster Amazon, consulta Abilitare IAM l'accesso di utenti e ruoli al tuo cluster - Amazon EKS.

L'accesso al tuo EKS cluster Amazon tramite IAM entità è abilitato dall'AWS IAMAuthenticator for Kubernetes, che viene eseguito sul piano di controllo di Amazon. EKS L'Authenticator ottiene le informazioni di configurazione da. `aws-auth ConfigMap`

> **Note**
>
> - Per ulteriori informazioni su tutte le `aws-auth ConfigMap` impostazioni, consulta Full Configuration Format on. GitHub
> - Per ulteriori informazioni sulle diverse IAM identità, vedere Identità (utenti, gruppi e ruoli) nella Guida per l'IAMutente.

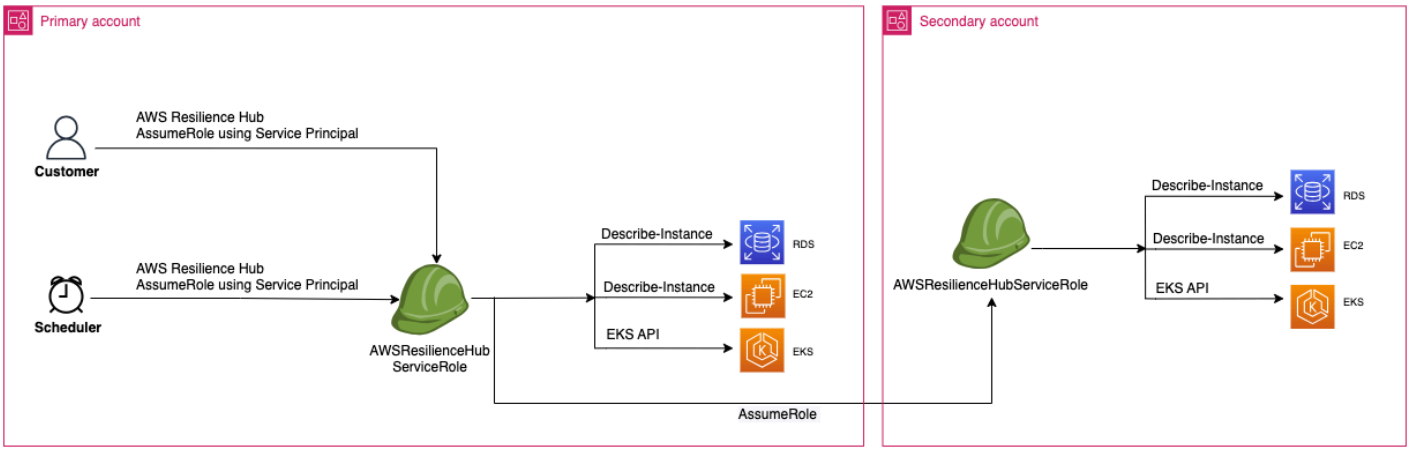
- Per ulteriori informazioni sulla configurazione del controllo degli accessi () basato sui ruoli di Kubernetes, consulta Using AuthorizationRBAC. RBAC

AWS Resilience Hub interroga le risorse all'interno del tuo EKS cluster Amazon utilizzando un IAM ruolo nel tuo account. Per accedere AWS Resilience Hub alle risorse all'interno del tuo EKS cluster Amazon, il IAM ruolo utilizzato da AWS Resilience Hub deve essere mappato a un gruppo Kubernetes con autorizzazioni di sola lettura sufficienti per le risorse all'interno del tuo cluster Amazon. EKS

AWS Resilience Hub consente di accedere alle risorse EKS del cluster Amazon utilizzando una delle seguenti opzioni di IAM ruolo:

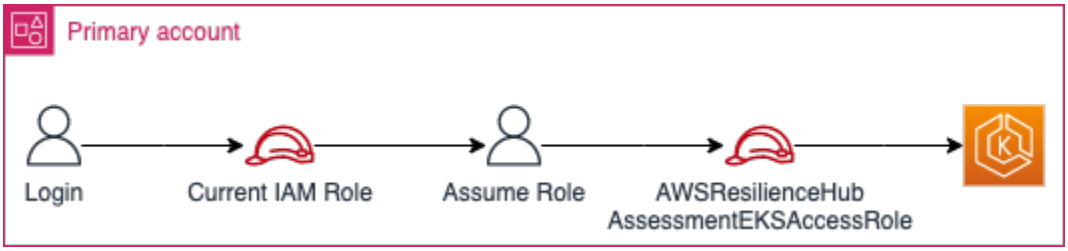
- Se l'applicazione è configurata per utilizzare l'accesso basato sui ruoli per accedere alle risorse, il ruolo invoker o il ruolo di account secondario assegnato AWS Resilience Hub durante la creazione di un'applicazione verrà utilizzato per accedere al cluster Amazon EKS durante la valutazione.

  Il seguente diagramma concettuale mostra come accedere AWS Resilience Hub ai cluster EKS Amazon quando l'applicazione è configurata come applicazione basata sui ruoli.

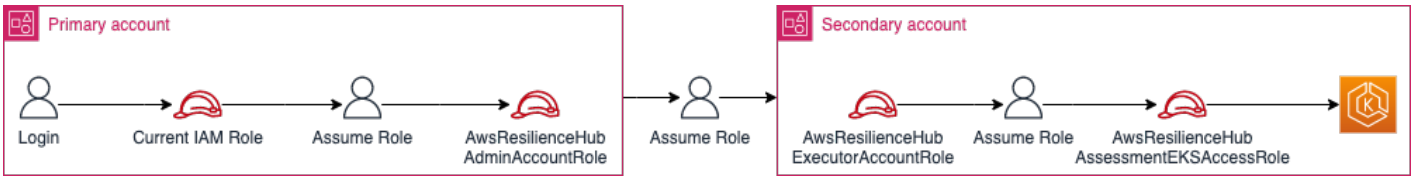


- Se la tua applicazione è configurata per utilizzare l'IAMutente corrente per accedere alle risorse, devi creare un nuovo IAM ruolo con lo stesso nome `AwsResilienceHubAssessmentEKSAccessRole` nello stesso account del EKS cluster Amazon. Questo IAM ruolo verrà quindi utilizzato per accedere al tuo EKS cluster Amazon.

  Il seguente diagramma concettuale mostra come AWS Resilience Hub accedere ai cluster EKS Amazon distribuiti nel tuo account principale quando l'applicazione è configurata per utilizzare le autorizzazioni utente correnti. IAM



Il seguente diagramma concettuale mostra come AWS Resilience Hub accede ai cluster EKS Amazon distribuiti su un account secondario quando l'applicazione è configurata per utilizzare le autorizzazioni utente correnti. IAM



Concedere AWS Resilience Hub l'accesso alle risorse del tuo cluster Amazon EKS

AWS Resilience Hub ti consente di accedere alle risorse situate nei EKS cluster Amazon a condizione che tu abbia configurato le autorizzazioni richieste.

Per concedere le autorizzazioni necessarie AWS Resilience Hub per la scoperta e la valutazione delle risorse all'interno del cluster Amazon EKS

1. Configura un IAM ruolo per accedere al EKS cluster Amazon.

   Se hai configurato l'applicazione utilizzando l'accesso basato sui ruoli, puoi saltare questo passaggio e procedere al passaggio 2 e utilizzare il ruolo che avevi usato per creare l'applicazione. Per ulteriori informazioni sull' AWS Resilience Hub utilizzo dei IAM ruoli, consulta. the section called “Come funziona AWS Resilience Hub con IAM”

   Se hai configurato la tua applicazione utilizzando le autorizzazioni IAM utente correnti, devi creare `AwsResilienceHubAssessmentEKSAccessRole` IAM un ruolo nello stesso account del EKS cluster Amazon. Questo IAM ruolo verrà quindi utilizzato durante l'accesso al tuo EKS cluster Amazon.

   Durante l'importazione e la valutazione della tua applicazione, AWS Resilience Hub utilizza un IAM ruolo per accedere alle risorse nel tuo cluster AmazonEKS. Questo ruolo deve essere creato nello stesso account del tuo EKS cluster Amazon e verrà mappato con un gruppo Kubernetes

che include le autorizzazioni richieste per AWS Resilience Hub valutare il tuo cluster Amazon. EKS

Se il tuo EKS cluster Amazon si trova nello stesso account dell'account AWS Resilience Hub chiamante, il ruolo deve essere creato utilizzando la seguente politica di IAM fiducia. In questa politica di IAM fiducia, `caller_IAM_role` viene utilizzato nell'account corrente APIs per chiamare il AWS Resilience Hub.

> **Note**
>
> `caller_IAM_role`Questo è il ruolo associato al tuo account AWS utente.

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

Se il tuo EKS cluster Amazon si trova in un account incrociato (un account diverso dall'account di AWS Resilience Hub chiamata), devi creare il `AwsResilienceHubAssessmentEKSAccessRole` IAM ruolo utilizzando la seguente politica di IAM fiducia:

> **Note**
>
> Come prerequisito, per accedere al EKS cluster Amazon distribuito in un account diverso da quello dell' AWS Resilience Hub utente, devi configurare l'accesso multiaccount. Per ulteriori informazioni, consulta la pagina

```
{
```

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

2. Crea `ClusterRole` e `ClusterRoleBinding` (o`RoleBinding`) ruoli per l'applicazione. AWS Resilience Hub

   Creando `ClusterRole` e `ClusterRoleBinding` concederai le autorizzazioni di sola lettura necessarie AWS Resilience Hub per analizzare e valutare le risorse che fanno parte di determinati namespace nel tuo cluster Amazon. EKS

   AWS Resilience Hub ti consente di limitarne l'accesso ai tuoi namespace per generare valutazioni di resilienza completando una delle seguenti operazioni:

   a. Concedi all'applicazione l'accesso in lettura su tutti i namespace. AWS Resilience Hub

      AWS Resilience Hub Per valutare la resilienza delle risorse in tutti i namespace all'interno di un EKS cluster Amazon, devi creare quanto segue e. `ClusterRole` `ClusterRoleBinding`

      - `resilience-hub-eks-access-cluster-role`(`ClusterRole`) — Definisce le autorizzazioni richieste AWS Resilience Hub per valutare il tuo EKS cluster Amazon.
      - `resilience-hub-eks-access-cluster-role-binding`(`ClusterRoleBinding`) — Definisce un gruppo denominato `resilience-hub-eks-access-group` nel tuo EKS cluster Amazon che concede ai suoi utenti le autorizzazioni necessarie per eseguire valutazioni della resilienza. AWS Resilience Hub

      Il modello per concedere l'accesso in lettura su tutti i namespace all'applicazione è il seguente: AWS Resilience Hub

```
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. Concessione AWS Resilience Hub dell'accesso alla lettura di namespace specifici.

È possibile limitare AWS Resilience Hub l'accesso alle risorse all'interno di un set specifico di namespace utilizzando. `RoleBinding` A tal fine, è necessario creare i seguenti ruoli:

- `ClusterRole`— Per accedere AWS Resilience Hub alle risorse in namespace specifici all'interno di un EKS cluster Amazon e valutarne la resilienza, devi creare i seguenti ruoli. `ClusterRole`
  - `resilience-hub-eks-access-cluster-role`— Speciifica le autorizzazioni necessarie per valutare le risorse all'interno di namespace specifici.

- `resilience-hub-eks-access-global-cluster-role`: specifica le autorizzazioni necessarie per valutare le risorse con ambito cluster, che non sono associate a uno spazio dei nomi specifico, all'interno dei cluster Amazon. EKS AWS Resilience Hub richiede le autorizzazioni per accedere a risorse con ambito cluster (come i nodi) sul tuo EKS cluster Amazon per valutare la resilienza della tua applicazione.

Il modello per creare il ruolo è il seguente`ClusterRole`:

```
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`ruolo: questo ruolo concede le autorizzazioni necessarie per accedere alle risorse all'interno AWS Resilience Hub di namespace specifici. Cioè, è necessario creare un `RoleBinding` ruolo in ogni spazio dei nomi per consentire AWS Resilience Hub l'accesso alle risorse all'interno dello spazio dei nomi specificato.

  > **Note**
  >
  > Se si utilizza `ClusterAutoscaler` la scalabilità automatica, è necessario creare anche in. `RoleBinding` `kube-system` Questo è necessario per valutare il tuo`ClusterAutoscaler`, che fa parte del namespace. `kube-system`
  > In questo modo, concederai AWS Resilience Hub le autorizzazioni necessarie per valutare le risorse all'interno del `kube-system` namespace durante la valutazione del tuo cluster Amazon. EKS

  Il modello per creare il `RoleBinding` ruolo è il seguente:

```
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`ruolo: questo ruolo concede le autorizzazioni necessarie per accedere AWS Resilience Hub alle risorse con ambito cluster.

Il modello per creare il ruolo è il seguente`ClusterRoleBinding`:

```
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. Aggiorna il `aws-auth ConfigMap` per `resilience-hub-eks-access-group` mapparlo con il IAM ruolo utilizzato per accedere al EKS cluster Amazon.

   Questo passaggio crea una mappatura tra il IAM ruolo utilizzato nella fase 1 e il gruppo Kubernetes creato nella fase 2. Questa mappatura concede le autorizzazioni ai IAM ruoli per l'accesso alle risorse all'interno del cluster Amazon. EKS

   > **Note**
   >
   > - `ROLE-NAME`si riferisce al IAM ruolo utilizzato per accedere al EKS cluster Amazon.
   >   - Se l'applicazione è configurata per utilizzare l'accesso basato sui ruoli, il ruolo deve essere il ruolo di invoker o il ruolo di account secondario a cui viene passato AWS Resilience Hub durante la creazione dell'applicazione.
   >   - Se l'applicazione è configurata per utilizzare l'IAMutente corrente per accedere alle risorse, deve essere il. `AwsResilienceHubAssessmentEKSAccessRole`
   > - `ACCOUNT-ID`deve essere l'ID dell' AWS account del EKS cluster Amazon.

Puoi crearlo `aws-auth ConfigMap` utilizzando uno dei seguenti modi:

- Uso di `eksctl`

  Utilizzate il seguente comando per aggiornare `aws-authConfigMap`:

  ```
  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
  ```

- È possibile modificare manualmente `aws-auth ConfigMap` aggiungendo i dettagli del IAM ruolo alla `mapRoles` sezione dei dati `ConfigMap` sottostanti. Utilizzate il seguente comando per modificare il `aws-authConfigMap`.

  ```
  kubectl edit -n kube-system configmap/aws-auth
  ```

  `mapRoles`la sezione è composta dai seguenti parametri:

  - `rolearn`— L'Amazon Resource Name (ARN) del IAM ruolo da aggiungere.
    - ARNSintassi —`arn:aws:iam::<ACCOUNT-ID>:role/<ROLE-NAME>`.
  - `username`— Il nome utente all'interno di Kubernetes da mappare al ruolo (). IAM `AwsResilienceHubAssessmentEKSAccessRole`
  - `groups`— I nomi dei gruppi devono corrispondere ai nomi dei gruppi creati nella Fase 2 (). `resilience-hub-eks-access-group`

  > **Note**
  >
  > Se la `mapRoles` sezione non esiste, è necessario aggiungerla manualmente.

  Utilizza il seguente modello per aggiungere i dettagli del IAM ruolo alla `mapRoles ConfigMap` sezione dei dati sottostanti.

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

```
      username: AwsResilienceHubAssessmentEKSAccessRole
```

Attivazione AWS Resilience Hub della pubblicazione su Amazon Simple Notification Service di argomenti

Questa sezione spiega come abilitare la pubblicazione AWS Resilience Hub di notifiche sull'applicazione negli argomenti di Amazon Simple Notification Service (AmazonSNS). Per inviare notifiche a un SNS argomento di Amazon, assicurati di disporre di quanto segue:

- Un' AWS Resilience Hub applicazione attiva.
- Un SNS argomento Amazon esistente a AWS Resilience Hub cui inviare notifiche. Per ulteriori informazioni sulla creazione di un SNS argomento Amazon, consulta Creazione di un SNS argomento Amazon.

AWS Resilience Hub Per abilitare la pubblicazione di notifiche sul tuo SNS argomento Amazon, devi aggiornare la politica di accesso dell'SNSargomento Amazon con quanto segue:

```
{
  "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**
>
> Quando utilizzi AWS Resilience Hub per pubblicare messaggi da Regioni che hanno aderito all'iniziativa su argomenti che si trovano in Regioni abilitate per impostazione predefinita, devi modificare la politica delle risorse creata per l'SNSargomento Amazon. Modifica il valore

del principale da `resiliencehub.amazonaws.com` a. `resiliencehub.<opt-in-region>.amazonaws.com`

Se utilizzi un SNS argomento Amazon Server Side Encrypted (SSE), devi assicurarti che AWS Resilience Hub disponga dell'`Decrypt`accesso `GenerateDataKey` e* alla chiave di SNS crittografia Amazon.

Per fornire `Decrypt` e `GenerateDataKey*` accedere a AWS Resilience Hub, devi includere le seguenti autorizzazioni per la politica di AWS Key Management Service accesso.

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

Limitazione delle autorizzazioni per includere o escludere i consigli AWS Resilience Hub

AWS Resilience Hub consente di limitare le autorizzazioni per includere o escludere consigli per applicazione. È possibile limitare le autorizzazioni per includere o escludere i consigli per applicazione utilizzando la seguente politica di IAM attendibilità. In questa politica di IAM fiducia, `caller_IAM_role` (associata al tuo account AWS utente) viene utilizzata nell'account corrente APIs per AWS Resilience Hub richiamare la richiesta.

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

Sicurezza dell'infrastruttura in AWS Resilience Hub

In quanto servizio gestito, AWS Resilience Hub è protetto dalle procedure di sicurezza della rete AWS globale descritte nel white paper Amazon Web Services: Overview of Security Processes.

Utilizzi API le chiamate AWS pubblicate per accedere AWS Resilience Hub attraverso la rete. I client devono supportare Transport Layer Security (TLS) 1.2 o versione successiva. Consigliamo TLS 1.3 o versioni successive. I client devono inoltre supportare suite di crittografia con Perfect Forward Secrecy (PFS) come Ephemeral Diffie-Hellman () o Elliptic Curve Ephemeral Diffie-Hellman (). DHE ECDHE La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale. IAM In alternativa, è possibile utilizzare AWS Security Token Service (AWS STS) per generare le credenziali di sicurezza temporanee per sottoscrivere le richieste.

Controlli di resilienza per i servizi AWS

Questo capitolo fornisce i dettagli dei vari controlli di resilienza eseguiti dai AWS servizi supportati AWS Resilience Hub per garantire che il livello di resilienza delle applicazioni non sia influenzato. Questi controlli stimano il tempo di ripristino (RTO) e l'obiettivo del punto di ripristino (RPO) rispetto ai valori definiti nella politica di resilienza per ciascun componente dell'applicazione (). AppComponent Le valutazioni comprendono diversi tipi di interruzioni, ovvero guasti delle applicazioni, dell'infrastruttura, interruzioni della zona AZ e guasti regionali. Tuttavia, per eseguire questi controlli è necessario fornire le IAM autorizzazioni necessarie per consentirgli di accedere alle AWS Resilience Hub risorse. Per ulteriori informazioni sulle IAM autorizzazioni necessarie per consentire l'accesso AWS Resilience Hub alle risorse ed eseguire i controlli di resilienza descritti in questo capitolo, consulta. AWS politiche gestite per AWS Resilience Hub

AWS servizi

- Amazon Elastic File System
- Amazon Relational Database Service e 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
- Sistema di bilanciamento del carico elastico
- Amazon API Gateway
- Amazon DocumentDB
- NATGateway
- Amazon Route 53
- Amazon Route 53 Application Recovery Controller
- File server Amazon FSx per Windows

- AWS Step Functions

Amazon Elastic File System

Questa sezione elenca tutti i controlli e i consigli di resilienza specifici per Amazon Elastic File System.

Per ulteriori informazioni su Amazon Elastic File System, consulta la documentazione di Amazon Elastic File System.

Tipo di file system

AWS Resilience Hub controlla il tipo di file system: Regionale o One Zone. Il tipo di file system influisce sulla sua resilienza in caso di interruzioni dell'infrastruttura o della zona di disponibilità. Per ulteriori informazioni sui tipi di file system, consulta Disponibilità e durabilità dei file system Amazon EFS.

Backup del file system

AWS Resilience Hub verifica se è definito un AWS Backup piano per il filesystem distribuito. Inoltre, verifica se l'opzione di `Cross-Region` backup è abilitata, garantendo la copertura in caso di interruzioni a livello regionale, se richiesto dalla politica del cliente.

Replica dei dati

AWS Resilience Hub verifica se per il filesystem distribuito è definita una replica EFS dei dati Amazon a livello regionale o interregionale. La replica EFS dei dati di Amazon aiuta a migliorare le stime RTO e le stime RPO a livello di applicazione, infrastruttura, AZ e regione. Inoltre, AWS Resilience Hub verifica se è combinata con una soluzione In-Region AWS Backup per abilitare la resilienza del file system in caso di interruzione delle applicazioni.

Amazon Relational Database Service e Amazon Aurora

Questa sezione elenca tutti i controlli e i consigli di resilienza specifici per Amazon Relational Database Service e Amazon Aurora.

Per ulteriori informazioni su Amazon Relational Database Service e Amazon Aurora, consulta la documentazione di Amazon Relational Database Service.

Implementazione Single-AZ

AWS Resilience Hub verifica se il database è distribuito come singola istanza e, se determinato, indica che non supporta istanze secondarie e repliche di lettura.

Multi-AZ deployment (Implementazione Multi-AZ)

AWS Resilience Hub verifica se il database è distribuito con istanze secondarie o repliche di lettura. Se il database viene distribuito con repliche di lettura, AWS Resilience Hub convalida se è distribuito in una zona di disponibilità diversa per consentire il failover in caso di interruzione della zona di disponibilità.

Backup

AWS Resilience Hub verifica se le seguenti funzionalità di backup sono applicate a un'istanza di database distribuita.

- AWS Backup piano con opzione di backup automatico
- AWS Backup pianifica con una copia di backup interregionale se richiesto dalla politica del cliente
- Istantanee manuali per sistemi di backup di terze parti

Failover tra regioni

AWS Resilience Hub controlli RTO e RPO obiettivi definiti nella politica di resilienza per riprendersi dalle perturbazioni regionali. Inoltre, AWS Resilience Hub è in grado di identificare le seguenti architetture interregionali per far fronte alle interruzioni regionali:

- Un backup interno alla regione con una copia di un'istantanea interregionale
- Una replica di lettura in un'altra regione
- Un database globale Amazon Aurora con un cluster secondario in un'altra regione
- Un database globale Amazon Aurora con un cluster secondario headless in un'altra regione

Failover più rapido all'interno della regione

AWS Resilience Hub controlli RTO e RPO obiettivi definiti nella politica di resilienza durante interruzioni dell'infrastruttura o della zona di disponibilità. Inoltre, AWS Resilience Hub è in grado

di identificare le seguenti architetture regionali per far fronte alle interruzioni delle applicazioni, dell'infrastruttura e della zona di disponibilità:

- Un backup interno alla regione
- Una replica di lettura in una zona di disponibilità diversa
- Un cluster Aurora con una replica di lettura in un'altra AZ
- Un'istanza Multi-AZ di Amazon Relational Database Service (Amazon) RDS
- Un cluster Amazon RDS Multi-AZ
- Una singola istanza di Amazon RDS con una replica di lettura in un'altra zona

Amazon Simple Storage Service

Questa sezione elenca tutti i controlli e i consigli di resilienza specifici per Amazon Simple Storage Service (Amazon S3).

Per ulteriori informazioni su Amazon S3, consulta la documentazione di Amazon S3.

Controllo delle versioni

AWS Resilience Hub verifica se un bucket Amazon S3 è configurato con il controllo delle versioni abilitato.

Backup pianificato

AWS Resilience Hub verifica se è definito un AWS Backup piano per il bucket Amazon Simple Storage Service (Amazon S3) distribuito. Inoltre, verifica anche se l'opzione di backup interregionale è abilitata se la politica richiede una copertura per le interruzioni a livello regionale.

Ripristino del PC oint-in-time

Replica dei dati

AWS Resilience Hub se sono definite Same Region Replication (SRR) e Cross Region Replication (CRR) per il bucket Amazon S3 distribuito.

La replica dei dati di Amazon S3 migliora il carico di lavoro stimato RTO e il carico di lavoro stimato RPO a livello di applicazione, infrastruttura, AZ e regione. Inoltre, protegge anche dall'eliminazione fisica dell'oggetto, poiché l'eliminazione di una versione dell'oggetto non viene replicata nel bucket

Amazon S3 di destinazione. Inoltre, in base RTO agli obiettivi definiti nella tua politica di resilienza, AWS Resilience Hub verifica se Amazon S3 Replication Time Control (RTCS3) deve essere abilitato o meno. Questa funzionalità fatturabile replica il 99,99 percento degli oggetti bucket di origine entro 15 minuti.

- AWS Backup piano con opzione di backup automatico
- AWS Backup pianifica con una copia di backup interregionale se richiesto dalla politica del cliente
- Istantanee manuali per sistemi di backup di terze parti

Amazon DynamoDB

Questa sezione elenca tutti i controlli e i consigli di resilienza specifici per Amazon DynamoDB.

Per ulteriori informazioni su Amazon DynamoDB, consulta la documentazione di Amazon DynamoDB.

Backup pianificato

AWS Resilience Hub verifica se è già definito un backup per la tabella distribuita. Inoltre, verifica anche se il backup interregionale deve essere configurato per la vostra politica se richiede una copertura per le interruzioni a livello regionale.

Ripristino del PC oint-in-time

AWS Resilience Hub verifica se point-in-time recovery (PITR) è necessario in base all'obiettivo della politica di RPO resilienza. Tuttavia, il backup interregionale non è supportato per. PITR Pertanto, è possibile utilizzare un AWS Backup piano pianificato esistente con l'opzione di backup interregionale abilitata o crearne uno nuovo.

Tabella globale

Amazon Elastic Compute Cloud

Questa sezione elenca tutti i controlli e i consigli di resilienza specifici per Amazon Elastic Compute Cloud.

Per ulteriori informazioni su Amazon Elastic Compute Cloud, consulta la documentazione di Amazon Elastic Compute Cloud.

Istanza con stato

AWS Resilience Hub identifica un'EC2istanza Amazon come istanza con stato se viene soddisfatto uno dei seguenti criteri:

- L'`DeleteOnTermination`attributo If è impostato su false per almeno un volume Amazon Elastic Block Store (AmazonEBS) collegato a questa istanza.
- Se Amazon Data Lifecycle Manager o un AWS Backup piano sono collegati all'EC2istanza Amazon o ad almeno un volume Amazon. EBS
- AWS Elastic Disaster Recovery Viene utilizzato per replicare i volumi di storage delle EC2 istanze Amazon.

> **Note**
>
> Se un'EC2istanza Amazon non soddisfa nessuno dei criteri sopra indicati, la AWS Resilience Hub considera un'istanza Amazon EC2 senza stato.

Gruppi Auto Scaling

AWS Resilience Hub verifica la presenza di un gruppo di EC2 istanze Amazon stateless. Se scoperto, si consiglia di orchestrare lo stesso utilizzando i gruppi di Auto Scaling ASG () con configurazione Multi-AZ.

Se ne ASG viene identificata una esistente, ARH verificherà se è configurata su più zone di disponibilità. Se ASG viene definito anche utilizzando solo EC2 istanze Amazon spot, si consiglia di aumentarne la capacità con istanze EC2 Amazon on-demand per migliorare la resilienza

quando le EC2 istanze Amazon spot non sono disponibili.

EC2Flotta Amazon

AWS Resilience Hub identifica Amazon EC2 Fleet e verifica se è definita come implementazione Multi-AZ e anche se utilizza solo istanze Amazon EC2 spot.

La definizione di una EC2 flotta Amazon come implementazione Multi-AZ ne migliorerà la resilienza in caso di interruzione della zona di disponibilità.

L'ampliamento di una EC2 flotta Amazon con istanze on-demand ne migliorerà la resilienza quando le istanze spot non sono disponibili.

Amazon EBS

Questa sezione elenca tutti i controlli e i consigli sulla resilienza specifici di AmazonEBS.

Per ulteriori informazioni su AmazonEBS, consulta la EBSdocumentazione di Amazon.

Backup pianificato

AWS Resilience Hub verifica se uno o entrambi i seguenti elementi sono definiti per i tuoi EBS volumi Amazon.

- Una regola di backup per un EBS volume Amazon specifico collegato alla tua EC2 istanza Amazon.
- Una regola di backup per creare un'EC2istanza Amazon EBS basata AMI su Amazon.
- Istantanee manuali per sistemi di backup di terze parti.

Inoltre, se la tua politica richiede una copertura per le interruzioni a livello regionale, AWS Resilience Hub verifica se la regola di backup ha abilitato l'opzione di backup interregionale.

Backup e replica dei dati

AWS Resilience Hub identifica che un EBS volume Amazon è considerato un volume con stato se viene soddisfatto uno dei seguenti criteri:

- L'`DeleteOnTermination`attributo If è impostato su false per questo EBS volume Amazon.
- Se Amazon Data Lifecycle Manager o un AWS Backup piano è associato a questo volume Amazon EBS o all'EC2istanza Amazon a cui è collegato.
- AWS Elastic Disaster Recovery Viene utilizzato per replicare i volumi di storage delle EC2 istanze Amazon.

AWS Lambda

Questa sezione elenca tutti i controlli e i consigli di resilienza specifici per. AWS Lambda

Per ulteriori informazioni in merito AWS Lambda, consulta AWS Lambda la documentazione.

Cliente Amazon VPC Access

AWS Resilience Hub identifica una AWS Lambda funzione collegata al clienteVPC. La connessione AWS Lambda a sottoreti in diverse aree AZs di Amazon VPC consente la resilienza delle funzioni in caso di interruzione della zona di disponibilità.

Coda di lettere morte

AWS Resilience Hub controlla se a una AWS Lambda funzione è associata una coda di lettere morte (DLQ) per archiviare le richieste non riuscite. L'associazione di una AWS Lambda funzione DLQ a consente di prevenire la perdita di dati delle richieste e di riprovare a elaborare le richieste non riuscite in una fase successiva.

Amazon Elastic Kubernetes Service

Questa sezione elenca tutti i controlli e i consigli di resilienza specifici per Amazon Elastic Kubernetes Service (Amazon). EKS

Per ulteriori informazioni su AmazonEKS, consulta la EKSdocumentazione di Amazon.

Multi-AZ deployment (Implementazione Multi-AZ)

AWS Resilience Hub identifica se la distribuzione del pod è in esecuzione su più nodi di lavoro in più AZs nodi.

È necessario un EKS cluster Amazon aggiuntivo in un'altra regione se la tua politica di resilienza richiede una copertura in caso di interruzione regionale. Questo EKS cluster Amazon aggiuntivo è inoltre verificato per le distribuzioni di pod distribuite tra più nodi di lavoro in più sedi. AZs

Distribuzione vs. ReplicaSet

AWS Resilience Hub verifica se si utilizzano oggetti ReplicaSets o pod anziché distribuirli. La sostituzione degli oggetti ReplicaSets o pod con la distribuzione semplifica gli aggiornamenti del pod a una nuova versione del software e include altre utili funzionalità.

Installazione e manutenzione

AWS Resilience Hub verifica se per la distribuzione vengono utilizzate le seguenti best practice:

- Utilizzo di Pod Disruption Budget (PDB) — Using PDB consente di migliorare la disponibilità impostando un limite al numero di pod del carico di lavoro che possono essere interrotti in un dato momento.
- Sostituzione dei gruppi di nodi autogestiti con gruppi di nodi EKS gestiti da Amazon: questa sostituzione semplifica gli aggiornamenti delle immagini dei nodi di lavoro durante la manutenzione.
- Supporto di richieste dinamiche CPU e di memoria per implementazione: queste richieste aiutano Kubernetes a selezionare un nodo adatto alle esigenze di un pod.
- Configurazione delle sonde di vivibilità e prontezza per tutti i contenitori: la configurazione delle sonde di liveness aiuta a migliorare la resilienza riavviando i pod non funzionanti. La configurazione delle sonde di prontezza consente di migliorare la disponibilità deviando il traffico dai pod occupati.
- Configurazione di Karpenter, Cluster Autoscaler o: AWS Fargate queste configurazioni consentono all'infrastruttura di Amazon EKS Cluster di crescere e soddisfare le richieste di carico di lavoro.
- Configurazione di Horizontal Pod Autoscaler: questa configurazione aiuta Amazon EKS Cluster a scalare automaticamente il carico di lavoro per soddisfare la domanda di elaborazione delle richieste.

Amazon Simple Notification Service

Questa sezione elenca tutti i controlli e i consigli di resilienza specifici di Amazon Simple Notification Service (AmazonSNS).

Per ulteriori informazioni su AmazonSNS, consulta la SNSdocumentazione di Amazon.

Abbonamenti tematici

AWS Resilience Hub verifica se l'SNSargomento Amazon ha almeno 1 abbonamento allegato per garantire che i messaggi in arrivo non vadano persi.

Amazon Simple Queue Service

Questa sezione elenca tutti i controlli e i consigli di resilienza specifici per Amazon Simple Queue Service (AmazonSQS).

Per ulteriori informazioni su AmazonSQS, consulta la SQSdocumentazione di Amazon.

Coda di lettere morte

AWS Resilience Hub verifica se alla SQS coda Amazon è DLQ associata una coda per gestire i messaggi che non possono essere recapitati correttamente agli abbonati.

Amazon Elastic Container Service

Questa sezione elenca tutti i controlli e i consigli di resilienza specifici di Amazon Elastic Container Service (AmazonECS).

Per ulteriori informazioni su AmazonECS, consulta la ECSdocumentazione di Amazon.

Multi-AZ deployment (Implementazione Multi-AZ)

AWS Resilience Hub verifica se ECS le attività o i servizi Amazon vengono eseguiti in più parti in AZs base ad Amazon EC2 o al tipo di AWS Fargate avvio. È necessario un ECS cluster Amazon aggiuntivo in un'altra regione se la tua polizza richiede una copertura per le interruzioni regionali. Il cluster aggiuntivo viene inoltre verificato per l'esecuzione di attività o servizi in più AZs parti.

Sistema di bilanciamento del carico elastico

Questa sezione elenca tutti i controlli e i consigli di resilienza specifici per Elastic Load Balancing.

Per ulteriori informazioni su Elastic Load Balancing, consulta la documentazione di Elastic Load Balancing.

Multi-AZ deployment (Implementazione Multi-AZ)

AWS Resilience Hub verifica se Elastic Load Balancing è in esecuzione in modalità multipla. AZs

È necessario un Elastic Load Balancing aggiuntivo in un'altra regione se la tua polizza necessita di una copertura per le interruzioni regionali. L'Elastic Load Balancing aggiuntivo, situato in una regione diversa, viene inoltre verificato per la sua implementazione in più aree. AZs

Amazon API Gateway

Questa sezione elenca tutti i controlli e i consigli di resilienza specifici per Amazon API Gateway.

Per ulteriori informazioni su Amazon API Gateway, consulta la documentazione di Amazon API Gateway.

Distribuzione tra regioni

Se la tua politica deve prendere in considerazione le interruzioni regionali, AWS Resilience Hub verificherà se c'è un'ulteriore distribuzione della API risorsa Amazon API Gateway in un'altra regione.

Implementazione privata API Multi-AZ

AWS Resilience Hub verifica se il tuo API è definito come privato all'interno di Amazon API Gateway. Private APIs dovrebbe ricevere traffico tramite l'endpoint VPC dell'interfaccia Amazon distribuito su più utenti. AZs

Amazon DocumentDB

Questa sezione elenca tutti i controlli e i consigli specifici di Amazon DocumentDB.

Per ulteriori informazioni su Amazon DocumentDB, consulta la documentazione di Amazon DocumentDB.

Multi-AZ deployment (Implementazione Multi-AZ)

AWS Resilience Hub verifica se il cluster Amazon DocumentDB è distribuito in più di un cluster. AZs È necessario un cluster Amazon DocumentDB secondario aggiuntivo in una regione diversa se la politica richiede una copertura per le interruzioni regionali. Il cluster Amazon DocumentDB aggiuntivo, situato in una regione diversa, viene inoltre verificato per la sua esecuzione in più aree. AZs

Distribuzione di cluster elastici e Multi-AZ

AWS Resilience Hub verifica se gli shard del cluster Amazon DocumentDB Elastic utilizzano repliche di lettura distribuite in diverse aree. AZs

Cluster elastico e istantanee manuali

AWS Resilience Hub verifica se vengono create regolarmente istantanee manuali per un cluster Amazon DocumentDB Elastic. Le istantanee manuali consentono una persistenza più lunga e offrono flessibilità nell'impostazione della frequenza delle istantanee in base alle esigenze aziendali.

NATGateway

Questa sezione elenca tutti i controlli e i consigli specifici di NAT Gateway. Per ulteriori informazioni sui NAT gateway, vedere NATGateways.

Multi-AZ deployment (Implementazione Multi-AZ)

AWS Resilience Hub verifica se NAT Gateway è distribuito in più di uno. AZs

È necessaria un'ulteriore implementazione del NAT Gateway in un'altra regione se la politica prevede una copertura per le interruzioni regionali. Il NAT gateway aggiuntivo, situato in una regione diversa, viene inoltre verificato per verificarne l'implementazione in più AZs aree.

Amazon Route 53

Questa sezione elenca tutti i controlli e i consigli specifici di Amazon Route 53.

Per ulteriori informazioni su Amazon Route 53, consulta la documentazione di Amazon Route 53.

Multi-AZ deployment (Implementazione Multi-AZ)

AWS Resilience Hub verifica se il record della zona ospitata di Amazon Route 53 è definito con più destinazioni nella stessa regione e se tali destinazioni sono distribuite in più AZs destinazioni. Se la tua politica richiede una copertura per le interruzioni regionali, AWS Resilience Hub verifica se il record della zona ospitata di Amazon Route 53 è definito in più regioni con più destinazioni per regione e se tali obiettivi sono distribuiti in più regioni. AZs

Amazon Route 53 Application Recovery Controller

Questa sezione elenca tutti i controlli e i consigli specifici di Amazon Route 53 Application Recovery Controller (Route 53ARC).

Per ulteriori informazioni su Route 53ARC, consulta la ARCdocumentazione di Route 53.

Multi-AZ deployment (Implementazione Multi-AZ)

AWS Resilience Hub verifica se risorse simili sono distribuite in più regioni e consiglia, come best practice, di definire i controlli di ARC idoneità della Route 53 per aumentarne la disponibilità e la

prontezza in caso di interruzione regionale. Ti verrà comunicato che dovrai sostenere costi orari aggiuntivi.

File server Amazon FSx per Windows

Questa sezione elenca tutti i controlli e i consigli specifici di Amazon FSx for Windows File Server. Per ulteriori informazioni su Amazon FSx for Windows File Server, consulta la documentazione di Amazon FSx for Windows File Server.

Tipo di file system

AWS Resilience Hub controlla il tipo di filesystem: o. `Regional` `One Zone` Il tipo di file system influisce sulla sua resilienza in caso di interruzioni dell'infrastruttura o della zona di disponibilità. Per ulteriori informazioni sui tipi di filesystem, consulta Amazon. EFS

Backup del file system

AWS Resilience Hub controlla se AWS Backup è definito un file system per il filesystem distribuito. Inoltre, verifica anche se `cross-Region backup` l'opzione è abilitata se la politica richiede una copertura per le interruzioni a livello regionale.

Replica dei dati

AWS Resilience Hub verifica se per il file system distribuito è definita un'attività di replica AWS DataSync dei dati pianificata a livello regionale o interregionale.

AWS DataSync un'attività di replica dei dati pianificata può migliorare il carico di lavoro stimato e il carico di lavoro stimato a livello di infrastruttura, AZ RTO e regioneRPO. Inoltre, potrebbe essere combinata con un'operazione locale AWS Backup per il ripristino in caso di interruzione dell'applicazione.

AWS Step Functions

Questa sezione elenca tutti i controlli e i consigli specifici per. AWS Step Functions

Per ulteriori informazioni in merito AWS Step Functions, consulta AWS Step Functions la documentazione.

Controllo delle versioni e alias

AWS Resilience Hub verifica se il AWS Step Functions flusso di lavoro utilizza il controllo delle versioni e l'alias per migliorare i tempi di ridistribuzione.

Implementazione in più regioni

AWS Resilience Hub verifica se il AWS Step Functions flusso di lavoro dello stesso tipo di flusso di lavoro è distribuito in una regione diversa per il ripristino in caso di interruzione regionale.

Utilizzo di altri servizi

Questa sezione descrive AWS i servizi che interagiscono con AWS Resilience Hub.

Argomenti

AWS CloudFormation

AWS Resilience Hub è integrato con AWS CloudFormation, un servizio che ti consente di modellare e configurare le tue risorse AWSin modo da dedicare meno tempo alla creazione e alla gestione delle risorse e dell'infrastruttura. Crei un modello che descrive tutte le AWS risorse che desideri (ad esempio AWS::ResilienceHub:::ResiliencyPolicy e AWS::ResilienceHub:::App) e fornisce AWS CloudFormation e configura tali risorse per te.

Quando usi AWS CloudFormation, puoi riutilizzare il modello per configurare le risorse AWS Resilience Hub in modo coerente e continuo. Descrivi le tue risorse una sola volta, quindi fornisci ripetutamente le stesse risorse in più AWS account e regioni.

AWS Resilience Hub e modelli AWS CloudFormation

Per eseguire l'assegnazione e la configurazione delle risorse per AWS Resilience Hub e i servizi correlati, devi conoscere i modelli AWS CloudFormation. I modelli sono file di testo formattati in JSON o YAML. Questi modelli descrivono le risorse di cui intendi effettuare il provisioning negli stack AWS CloudFormation. Se non hai familiarità con JSON o YAML, puoi usare AWS CloudFormationDesigner per iniziare a utilizzare i modelli AWS CloudFormation. Per ulteriori informazioni, consulta Che cos'è AWS CloudFormationDesigner? nella Guida per l'utente di AWS CloudFormation.

AWS Resilience Hubsupporta la creazione AWS::ResilienceHub:::ResiliencyPolicy e l' AWS::ResilienceHub:::AppinserimentoAWS CloudFormation. Per ulteriori informazioni, inclusi esempi di modelli JSON e YAML per AWS::ResilienceHub:::ResiliencyPolicy e AWS::ResilienceHub:::App, consulta il riferimento ai tipi di AWS Resilience Hub risorse nella Guida per l'AWS CloudFormationutente.

È possibile utilizzare gli AWS CloudFormation stack per definire le applicazioni. AWS Resilience Hub Uno stack consente di gestire le risorse correlate come una singola unità. Uno stack può contenere tutte le risorse necessarie per eseguire un'applicazione Web, ad esempio un server Web o regole di rete.

Ulteriori informazioni su AWS CloudFormation

Per ulteriori informazioni su AWS CloudFormation, consulta le seguenti risorse:

- AWS CloudFormation
- Guida per l'utente di AWS CloudFormation
- Documentazione di riferimento dell'API AWS CloudFormation
- Guida per l'utente dell'interfaccia a riga di comando di AWS CloudFormation

AWS CloudTrail

AWS Resilience Hub è integrato con AWS CloudTrail, un servizio che fornisce una registrazione delle azioni intraprese da un utente, da un ruolo o da un AWS servizio in AWS Resilience Hub. CloudTrail acquisisce tutte le chiamate API AWS Resilience Hub come eventi. Le chiamate acquisite includono chiamate dalla AWS Resilience Hub console e chiamate di codice alle operazioni AWS Resilience Hub API. Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per. AWS Resilience Hub Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi. Utilizzando le informazioni raccolte da CloudTrail, puoi determinare a quale richiesta è stata inviata AWS Resilience Hub, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e dettagli aggiuntivi.

Per ulteriori informazioni in merito CloudTrail, consulta la Guida AWS CloudTrail per l'utente.

AWS Systems Manager

AWS Resilience Hub collabora con Systems Manager per automatizzare i passaggi delle SOP fornendo una serie di documenti SSM che è possibile utilizzare come base per tali SOP.

AWS Resilience Hub fornisce AWS CloudFormation modelli che contengono i ruoli IAM necessari per eseguire diversi documenti Systems Manager, un ruolo per documento con le autorizzazioni

richieste per il documento specifico. Dopo aver creato uno stack con il AWS CloudFormation modello, configurerà i ruoli IAM e salverà i metadati nel parametro Systems Manager per il documento di automazione Systems Manager da eseguire per diverse procedure di ripristino.

Per ulteriori informazioni sull'utilizzo delle SOP, vedere. Gestione delle procedure operative standard

AWS Trusted Advisor

AWS Trusted Advisor è una raccolta centralizzata di raccomandazioni sulle AWS best practice che consente di identificare, assegnare priorità e ottimizzare la distribuzione su. AWS AWS Trusted Advisor ispeziona l' AWS ambiente e quindi formula raccomandazioni verificando quando esistono opportunità per risparmiare denaro, migliorare la disponibilità e le prestazioni del sistema o contribuire a colmare le lacune di sicurezza. Questi controlli sono suddivisi in più categorie in base al loro scopo. Per ulteriori informazioni sulle diverse categorie di check-in AWS Trusted Advisor, consulta la Guida per l'AWS Supportutente.

AWS Trusted Advisor fornisce diversi consigli di resilienza di alto livello attraverso controlli di resilienza per ciascuna applicazione nella AWS Resilience Hub categoria Fault tolerance. La categoria di tolleranza ai guasti elenca tutti i controlli che testano le applicazioni per determinarne la resilienza e l'affidabilità. Questi controlli avvisano l'utente in caso di AppComponent errori e violazioni delle politiche che possono causare rischi di resilienza e influire sulla disponibilità delle applicazioni per la continuità aziendale. Fornisce inoltre raccomandazioni sulla resilienza che miglioreranno le possibilità di ridurre questi rischi nella sezione Azioni consigliate, che deve essere affrontata in. AWS Resilience Hub Per ulteriori informazioni sui consigli per ciascuna applicazione in AWS Trusted Advisor, si consiglia di visualizzare i consigli dettagliati forniti nel AWS Resilience Hub.

AWS Trusted Advisor fornisce i seguenti controlli per ogni applicazione in AWS Resilience Hub:

- AWS Resilience Hub punteggi di resilienza delle applicazioni: verifica il punteggio di resilienza delle applicazioni in base all'ultima valutazione effettuata AWS Resilience Hub e avvisa l'utente se i punteggi di resilienza sono inferiori a un valore specifico.

  Criteri di avviso

  - Verde: indica che l'applicazione ha un punteggio di resilienza pari o superiore a 70.
  - Giallo: indica che l'applicazione ha un punteggio di resilienza compreso tra 40 e 69.
  - Rosso: indica che l'applicazione ha un punteggio di resilienza inferiore a 40.

  Azione consigliata

Per migliorare il livello di resilienza e ottenere il miglior punteggio di resilienza possibile per l'applicazione, esegui una valutazione con la versione aggiornata più recente delle risorse dell'applicazione e, se applicabile, implementa i consigli operativi suggeriti. Per ulteriori informazioni sull'esecuzione, la revisione e l'implementazione delle valutazioni, la revisione e l'inclusione/esclusione delle raccomandazioni operative e l'implementazione delle stesse, consulta i seguenti argomenti:

- the section called “Esecuzione di valutazioni della resilienza”
- the section called “Revisione dei rapporti di valutazione”
- the section called “Revisione delle raccomandazioni sulla resilienza”
- the section called “Inclusione o esclusione di raccomandazioni operative”

- AWS Resilience Hub violazione dei criteri di applicazione: verifica se le AWS Resilience Hub applicazioni soddisfano gli obiettivi RTO e RPO impostati per un'applicazione e avvisa l'utente se l'applicazione non soddisfa gli obiettivi RTO e RPO.

  Criteri di avviso

  - Verde: indica che l'applicazione dispone di una policy e che l'RTO del carico di lavoro stimato e l'RPO del carico di lavoro stimato soddisfano gli obiettivi RTO e RPO.
  - Giallo: indica che l'applicazione dispone di una politica e non è stata valutata.
  - Rosso: indica che l'applicazione dispone di una politica e che l'RTO del carico di lavoro stimato e l'RPO del carico di lavoro stimato non soddisfano gli obiettivi RTO e RPO.

  Azione consigliata

  Per garantire che l'RTO del carico di lavoro stimato e l'RPO stimato del carico di lavoro dell'applicazione continuino a soddisfare gli obiettivi RTO e RPO definiti, esegui valutazioni regolarmente con la versione aggiornata più recente delle risorse dell'applicazione. Inoltre, se desideri assicurarti che la politica di resilienza della tua applicazione non venga violata, ti consigliamo di esaminare il rapporto di valutazione e implementare i consigli di resilienza suggeriti. Per ulteriori informazioni su come consentire AWS Resilience Hub l'esecuzione di valutazioni su base giornaliera per conto dell'utente, l'esecuzione delle valutazioni, la revisione dei consigli sulla resilienza e l'implementazione degli stessi, consulta i seguenti argomenti:

  - the section called “Modifica delle risorse delle applicazioni”(AWS Resilience Hub Per abilitare l'esecuzione delle valutazioni su base giornaliera per tuo conto, completa la procedura descritta in Modificare le impostazioni di notifica delle deviazioni della procedura di candidatura selezionando la casella di controllo Valuta automaticamente ogni giorno).

- the section called “Esecuzione di valutazioni della resilienza”
- the section called “Revisione dei rapporti di valutazione”
- the section called “Revisione delle raccomandazioni sulla resilienza”
- the section called “Inclusione o esclusione di raccomandazioni operative”

- AWS Resilience Hub età di valutazione della domanda: verifica l'ultima volta che è stata eseguita una valutazione per ciascuna delle applicazioni in. AWS Resilience Hub Ti avvisa se non hai eseguito una valutazione per il numero di giorni specificato.

  Criteri di avviso

  - Verde: indica che hai eseguito una valutazione della tua candidatura negli ultimi 30 giorni.
  - Giallo: indica che non hai eseguito una valutazione per la tua applicazione negli ultimi 30 giorni.

  Azione consigliata

  Esegui valutazioni regolarmente per gestire e migliorare il livello di resilienza delle tue applicazioni. AWS Se desideri AWS Resilience Hub valutare la tua applicazione su base giornaliera per tuo conto, puoi abilitarla selezionando la casella di controllo Valuta automaticamente questa applicazione ogni giorno nella AWS Resilience Hub notifica di drift. Per selezionare la casella di controllo Valuta automaticamente questa applicazione ogni giorno, compila la casella di controllo Per modificare la notifica di deviazione della procedura di candidatura in. ???

  > **Note**
  >
  > Questo controllo determina l'età di valutazione solo per le domande che sono state valutate almeno una volta. AWS Resilience Hub

- AWS Resilience Hub controllo dei componenti dell'applicazione: verifica se un componente dell'applicazione (AppComponent) nell'applicazione è irrecuperabile. In altre parole, se il problema AppComponent non viene ripristinato in caso di interruzione, è possibile che si verifichino perdite di dati sconosciute e tempi di inattività del sistema. Se il criterio di avviso è impostato su Rosso, indica che non AppComponent è recuperabile.

  Azione consigliata

  Per assicurarti che il tuo AppComponent sia ripristinabile, esamina e implementa i consigli sulla resilienza, quindi esegui una nuova valutazione. Per ulteriori informazioni sulla revisione dei

consigli sulla resilienza, consulta. the section called “Revisione delle raccomandazioni sulla resilienza”

Per ulteriori informazioni sull'utilizzo AWS Trusted Advisor, consulta la Guida per l'AWS Support utente.

Cronologia dei documenti per la Guida per AWS Resilience Hub l'utente

La tabella seguente descrive la documentazione per questa versione di. AWS Resilience Hub

- APIversione: più recente
- Ultimo aggiornamento della documentazione: 1 agosto 2024

Modifica	Descrizione	Data
AWS Resilience Hub introduce raccomandazioni di raggruppamento	AWS Resilience Hub introduce una nuova opzione di raggruppamento intelligente per raggruppare le risorse in Application Components () AppComponents durante l'onboarding delle applicazioni. Quando si eseguono valutazioni della resilienza a AWS Resilience Hub, è importante che le risorse siano accuratamente raggruppate in modo appropriato per ricevere consigli ottimizzati e attuabili . AppComponents Questa opzione è ideale per applicazioni complesse o interregionali per ridurre i tempi necessari per l'onboarding delle applicazioni e completa il flusso di lavoro di onboarding delle applicazioni esistente oggi disponibile.	1 agosto 2024

	Per ulteriori informazioni, consulta i seguenti argomenti: • the section called “Gestione dei componenti dell'applicazione” • the section called “AWS Resilience Hub consigli per il raggruppamento delle risorse”	
AWS Resilience Hub introduce un nuovo widget di riepilogo della valutazione	AWS Resilience Hub introduce un nuovo widget di riepilogo della valutazione che utilizza le funzionalità di intelligenza artificiale generativa di Amazon Bedrock per trasformare dati di resilienza complessi in informazioni altamente utilizzabili. Questi riepiloghi delle valutazioni estraggono i risultati critici, assegnano priorità ai rischi e consigliano misure per migliorare la resilienza. Concentrandovi sugli elementi di maggiore impatto, potete comprendere le valutazioni molto più facilmente, il che vi aiuta a ottenere informazioni ad alto impatto incentrate sugli elementi più critici del vostro atteggiamento di resilienza. Per ulteriori informazioni, consulta the section called “Riepilogo della valutazione”.	1 agosto 2024

AWS Resilience Hub estende il supporto per Amazon DocumentDB	Questa AWS Resilience Hub policy consente di concedere `Describe` autorizzazioni per accedere a risorse e configurazioni su Amazon DocumentDB, Elastic Load Balancing e durante l'esecuzione delle valutazioni. AWS Lambda Per ulteriori informazioni sulla policy gestita, consulta. AWS the section called “AWSResilienceHubAsssessmentExecutionPolicy”	1 agosto 2024

AWS Resilience Hub amplia le capacità di rilevamento della deriva della resilienza delle applicazioni	AWS Resilience Hub ha ampliato le sue capacità di rilevamento della deriva introducendo un nuovo tipo di rilevamento della deriva: la deriva delle risorse applicative. Questo miglioramento rileva le modifiche, come l'aggiunta o l'eliminazione di risorse all'interno delle fonti di input dell'applicazione. È possibile abilitare i servizi di valutazione AWS Resilience Hub pianificata e notifica della deriva ed essere avvisati ogni volta che si verifica una deriva. L'ultima valutazione della resilienza identifica le derive e presenta azioni correttive per riportare l'applicazione in conformità con la politica di resilienza. Per ulteriori informazioni, consulta i seguenti argomenti: • the section called “Rilevamento delle deviazioni” • the section called “Fase 5: Impostazione della valutazione programmata e della notifica di deviazione”	8 maggio 2024

AWS Trusted Advisor miglioramenti	AWS Resilience Hub ha esteso il supporto AWS Trusted Advisor aggiungendo un controllo per identificare i componenti dell'applicazione irrecuperabili (). AppComponents Per ulteriori informazioni, consulta the section called “AWS Trusted Advisor”.	28 marzo 2024
AWS Resilience Hub estende il supporto per gli allarmi consigliati	AWS Resilience Hub ha aggiornato il file `README.md` modello con valori che consentono di creare allarmi consigliati dall' AWS Resilience Hub interno AWS (come Amazon CloudWatch) o dall'esterno AWS. Per ulteriori informazioni, consulta the section called “Gestione degli allarmi”.	26 marzo 2024

AWS Resilience Hub estende il supporto per Amazon FSx for Windows File Server	AWS Resilience Hub estende il supporto di valutazione per le risorse di Amazon FSx for Windows File Server valutando al contempo la resilienza dell'applicazione. Per le applicazioni che utilizzano Amazon FSx for Windows File Server, AWS Resilience Hub fornisce una nuova serie di consigli sulla resilienza, che coprono le implementazioni in zona di disponibilità (AZ) e Multi-AZ, i piani di backup e la replica dei dati. AWS Resilience Hub supporta Amazon FSx for Windows File Server, inclusa la dipendenza del filesystem da Microsoft Active Directory , per distribuzioni sia a livello locale che interregionale. Per ulteriori informazioni, consulta i seguenti argomenti: • the section called “ AWS Resilience Hub risorse supportate” • the section called “AWSResilienceHubAsssessmentExecutionPolicy” • the section called “Raggruppamento di risorse in un componente applicativo”	26 marzo 2024

AWS Resilience Hub fornisce informazioni aggiuntive sul punteggio di resilienza	AWS Resilience Hub ha aggiornato l'esperienza utente di Resiliency Score per aiutarti a navigare e comprendere facilmente le azioni necessari e per migliorare il livello di resilienza delle tue applicazioni. Per ulteriori informazioni, consulta the section called “Comprendere i punteggi di resilienza”.	9 novembre 2023
AWS Resilience Hub estende il supporto per le applicazioni che includono risorse Amazon Elastic Kubernetes Service (Amazon) EKS	AWS Resilience Hub estende il supporto per le applicazioni che includono EKS risorse Amazon per includere nuove raccomandazioni operative. Durante l'esecuzione di una valutazione che include risorse provenienti dai EKS cluster Amazon, ora consiglieremo l'esecuzione di test e allarmi per contribuire a migliorare la resilienza delle applicazioni. Per ulteriori informazioni, consulta the section called “Gestione degli esperimenti di Amazon Fault Injection Service”.	9 novembre 2023

AWS Resilience Hub fornisce informazioni aggiuntive a livello di applicazione	AWS Resilience Hub fornisce informazioni aggiuntive a livello di applicazione sul carico di lavoro stimato RTO e sul carico di lavoro RPO stimato. Queste informazioni aggiuntive indicano il carico di lavoro stimato massimo possibile RTO e il carico di lavoro stimato RPO dell'appl icazione in base all'ultima valutazione riuscita. Questo valore è il carico di lavoro massimo stimato RTO e il carico di lavoro stimato per tutti i tipi RPO di interruzione. Per ulteriori informazioni, consulta the section called “Gestione delle applicazioni”.	30 ottobre 2023

AWS Resilience Hub estende il supporto per la valutazione delle risorse AWS Step Functions	AWS Resilience Hub estende il supporto di valutazione AWS Step Functions delle risorse valutando al contempo la resilienza dell'applicazione. AWS Resilience Hub analizza la AWS Step Functions configurazione, incluso il tipo di macchina a stati (flussi di lavoro Standard o Express). Inoltre, AWS Resilience Hub fornirà anche consigli che consentono di soddisfare gli obiettivi del tempo di ripristino stimati del carico di lavoro (RTO) e gli obiettivi del punto di ripristino del carico di lavoro stimato (). RPO Per valutare le applicazioni, comprese AWS Step Functions le risorse, è necessario impostare le autorizzazioni necessarie, utilizzando la policy AWS gestita o aggiungendo manualmente l'autorizzazione specifica AWS Resilience Hub per consentire la lettura della configurazione. AWS Step Functions Per ulteriori informazioni sulle autorizzazioni associate, vedere. the section called “AWSResilienceHubAssessmentExecutionPolicy”	30 ottobre 2023

AWS Resilience Hub consente di escludere le raccomandazioni operative	AWS Resilience Hub aggiunge la possibilità di escludere raccomandazioni operative tra cui allarmi, procedure operative standard (SOPs) e test di Amazon Fault Injection Service (AWS FIS). Durante l'esecuzione di una valutazione AWS Resilience Hub, ti vengono forniti tempi di ripristino stimati e consigli su come aumentare la resilienza dell'applicazione valutata. Utilizzando il flusso di lavoro relativo alle raccomandazioni di esclusione, ora avrai la possibilità di escludere gli allarmi consigliati e SOPs i AWS FIS test che non sono pertinenti per essi. Il flusso di lavoro di esclusione è utile se utilizzi una piattaforma diversa da quella suggerita o se hai già implementato la raccomandazione in un metodo alternativo. Per ulteriori informazioni, consulta i seguenti argomenti: • the section called “Inclusione o esclusione di raccomandazioni operative” • the section called “Limitazione delle autorizzazioni per includere o escludere	9 agosto 2023

	consigli AWS Resilience Hub ”	
Miglioramento della progettazione delle autorizzazioni per AWS Resilience Hub	AWS Resilience Hub introduce un nuovo design delle autorizzazioni per fornire flessibilità durante la configurazione dei ruoli AWS Identity and Access Management (IAM) per. AWS Resilience Hub Inoltre, consolida le autorizzazioni in un unico ruolo, con la possibilità di creare nomi di ruolo personalizzati significativi per te e i tuoi team. Una nuova policy gestita ti AWS Resilience Hub consentirà di disporre delle autorizzazioni appropriate per i servizi supportati. Se hai dimestichezza con l'attuale metodo di impostazione delle autorizzazioni, continueremo a supportare la configurazione manuale. Per ulteriori informazioni sulla politica AWS gestita, consultathe section called “AWSResilienceHubAssessmentExecutionPolicy”.	2 agosto 2023

Rilevamento della deriva della resilienza delle applicazioni con AWS Resilience Hub	AWS Resilience Hub consente di rilevare e comprendere in modo proattivo le azioni necessarie per risolvere la resilienza delle applicazioni. Consentire ad Amazon Simple Notification Service (AmazonSNS) di ricevere notifiche quando l'obiettivo del tempo di ripristino del carico di lavoro stimato (RTO) o l'obiettivo stimato del punto di ripristino del carico di lavoro (RPO) è passato dal raggiungimento dell'obiettivo a non soddisfare più gli obiettivi aziendali dell'organizzazione. Passare dall'individuazione reattiva dei problemi di resilienza durante l'esecuzione manuale di una valutazione alla ricezione proattiva di notifiche tramite SNS argomenti di Amazon ti consentirà di anticipare potenziali interruzioni in anticipo e di avere maggiore fiducia nel raggiungimento degli obiettivi di ripristino. Per ulteriori informazioni, consulta i seguenti argomenti: • the section called “Fase 5: Impostazione della valutazione programmata e della notifica di deviazione”	2 agosto 2023

- the section called “Modifica delle risorse delle applicazioni”

AWS Resilience Hub migliora il supporto per Amazon Relational Database Service e Amazon Aurora	AWS Resilience Hub estende il supporto di valutazione per il proxy Amazon Relationa l Database Service e le configurazioni di database headless e Amazon Aurora DB. Inoltre, durante la valutazione delle applicazioni che includono AmazonRDS, ora distingueremo tra diversi motori di database per fornire obiettivi di tempo di ripristino del carico di lavoro stimati più precisi ()RTOs. AWS Resilienc e Hub fornirà inoltre azioni aggiuntive per implementare le migliori pratiche di resilienza all'interno del vostro ambiente. AWS Le best practice possono includere approfondimenti sulle prestazioni con DevOps Guru for AmazonRDS, monitoraggio avanzato e automazione della distribuz ione blu/green sui motori di database supportati. Per ulteriori informazioni sulle autorizzazioni necessarie per includere le risorse AWS Resilience Hub di tutti i servizi supportati nella valutazio ne, consulta. the section called “AWSResilienceHubA sssessmentExecutionPolicy”	2 agosto 2023

AWS Resilience Hub estende il supporto per gli snapshot di Amazon Elastic Block Store	AWS Resilience Hub estende il supporto di valutazione per Amazon Elastic Block Store (AmazonEBS) per riconoscere le EBS istantanee Amazon, che vengono scattate all'interno della stessa EBS regione Amazon utilizzando directAPIs. Il supporto esteso si aggiunge al supporto attuale per i clienti che utilizzan o Amazon Data Lifecycle Manager (Amazon Data Lifecycle Manager) o Backup. AWS Per ulteriori informazioni, consulta Amazon Elastic Block Store (AmazonEBS).	2 agosto 2023

Miglioramenti di Amazon Elastic Compute Cloud	AWS Resilience Hub ha esteso il supporto per Amazon Elastic Compute Cloud (AmazonEC2). Per applicazioni di dimensioni diverse, AWS consente ai clienti che utilizzano Amazon EC2 di selezionare la configurazione appropriata per il loro caso d'uso. AWS Resilience Hub supporta la valutazione sulle seguenti EC2 configurazioni Amazon: • Istanze su richiesta. • Backup delle istanze eseguito a mano. AWS Backup AWS Elastic Disaster Recovery • Supporto per gruppi con scalabilità automatica con Amazon Route 53 Application Recovery Controller (Route 53) ARC In futuro, il supporto per la valutazione si estenderà fino a includere istanze spot, host dedicati, istanze dedicate, gruppi di collocamento e flotte. Per ulteriori informazioni, consulta the section called “AWS Resilience Hub riferimento alle autorizzazioni di accesso”.	27 giugno 2023

AWS aggiornamenti delle politiche gestiti	È stata aggiunta una nuova politica che fornisce l'accesso ad altri AWS servizi per l'esecuzione delle valutazioni. Per ulteriori informazioni, consulta the section called “AWSResilienceHubAsssessmentExecutionPolicy”.	26 giugno 2023
Nuovi allarmi di raccomandazione operativa di Amazon DynamoDB	Per le applicazioni che utilizzano Amazon DynamoDB AWS Resilience Hub , ora offre una nuova serie di allarmi che avvisano dei rischi di resilienza per le modalità di capacità on demand e provisioning e le tabelle globali. Per accedere ai nuovi allarmi, potrebbe essere necessario aggiornare la policy AWS Identity and Access Management (IAM) del ruolo che stai utilizzando. Per ulteriori informazioni, consulta the section called “AWS Resilience Hub riferimento alle autorizzazioni di accesso”.	2 maggio 2023

AWS Trusted Advisor miglioramenti	AWS Resilience Hub ha ampliato il supporto AWS Trusted Advisor e le applicazioni che utilizzano Amazon DynamoDB. Quando utilizzi AWS Trusted Advisor with AWS Resilience Hub, ora puoi ricevere una notifica quando un'applicazione non è stata valutata nei 30 giorni precedenti. Questa notifica richiede di rivalutare l'applicazione per capire se ci sono modifiche che potrebbero influire sulla sua resilienza. Per ulteriori informazioni sulla AWS Resilience Hub valutazione e il controllo dell'età, vedere. the section called “AWS Trusted Advisor”	2 maggio 2023

Supporto aggiuntivo per Amazon Simple Storage Service	Oltre all'attuale supporto di Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (Amazon S3) /Amazon S3 Same-Region Replication SRR (CRR), il controllo delle versioni e il AWS backup AWS Resilience Hub valuteranno ora Amazon S3 per punti di accesso multiregione, Amazon S3 Replication Time Control (Amazon S3) e Backup Configurazione Backup recovery (). RTC AWS point-in-time PITR Per ulteriori informazioni, consulta i seguenti argomenti: • the section called “AWS Resilience Hub riferimento alle autorizzazioni di accesso” • Gestione dello storage Amazon S3	21 marzo 2023

Supporto aggiuntivo per Amazon Elastic Kubernetes Service	AWS Resilience Hub ha aggiunto Amazon EKS cluster come risorsa supportata per la definizione, la convalida e il monitoraggio della resilienz a delle applicazioni. I clienti possono aggiungere EKS cluster Amazon ad applicazioni nuove o esistenti e ricevere valutazioni e consigli per migliorare la resilienza. I clienti possono aggiunger e risorse applicative utilizzan do AWS CloudFormation Terraform e. AWS Resource Groups AppRegistry Inoltre, i clienti possono aggiunger e uno o più EKS cluster Amazon direttamente in una o più regioni con uno o più namespace in ogni cluster. Ciò consente di AWS Resilienc e Hub fornire valutazioni e raccomandazioni singole e interregionali. Oltre a esaminare le implementazioni, le repliche e i pod, analizzer à la ReplicationControllers resilienza complessiva del cluster. AWS Resilience Hub AWS Resilience Hub supporta carichi di lavoro di EKS cluster Amazon stateless. Le nuove funzionalità sono disponibi li in tutte le AWS regioni in	21 marzo 2023

	cui AWS Resilience Hub è supportata. Per ulteriori informazioni, consulta i seguenti argomenti: • the section called “Fase 2: Gestisci le risorse dell'applicazione” • the section called “Aggiungi cluster EKS” • the section called “AWS Resilience Hub riferimento alle autorizzazioni di accesso” • AWS Servizi regionali	
Supporto aggiuntivo per Amazon Elastic File System	Oltre all'attuale supporto per il backup di Amazon Elastic File System (AmazonEFS), ora AWS Resilience Hub valuterà Amazon EFS for Amazon EFS Replication e la configurazione AZ. Per ulteriori informazioni, consulta i seguenti argomenti: • the section called “ AWS Resilience Hub risorse supportate” • Cos'è Amazon Elastic File System?	21 marzo 2023

Support per le sorgenti di input delle applicazioni	AWS Resilience Hub ora offre trasparenza sulle fonti delle applicazioni. Ti aiuta ad aggiungere, eliminare e reimportare le fonti di input dell'applicazione e a pubblicar e una nuova versione dell'appl icazione. Per ulteriori informazioni, consulta the section called “Modifica delle risorse delle applicazioni”.	21 febbraio 2023

Support per i parametri di configurazione dell'applicazione	AWS Resilience Hub ora fornisce un meccanismo di input per raccogliere informazioni aggiuntive sulle risorse associate alle applicazioni. Con queste informazioni, AWS Resilience Hub acquisirete una comprensione più approfondita delle vostre risorse e fornirete migliori consigli sulla resilienza. Per ulteriori informazioni, consulta i seguenti argomenti: • the section called “Parametri di configurazione dell'applicazione” • the section called “Fase 7: Configurazione dei parametri di configurazione dell'applicazione” • the section called “Aggiornamento dei parametri di configurazione dell'applicazione”	21 febbraio 2023

Supporto aggiuntivo per Amazon Elastic Block Store	Oltre all'attuale supporto dei volumi Amazon Elastic Block Store (AmazonEBS), ora AWS Resilience Hub valuterà EBS gli snapshot Amazon tramite Amazon Data Lifecycle Manager e EBS Amazon fast snapshot restore (). FSR Per ulteriori informazioni, consulta i seguenti argomenti: • the section called “AWS Resilience Hub riferimento alle autorizzazioni di accesso” • Amazon Elastic Block Store (AmazonEBS)	21 febbraio 2023

Integrazione con AWS Trusted Advisor	AWS Trusted Advisor gli utenti potranno visualizzare le applicazioni associate al proprio account che sono state valutate da AWS Resilience Hub. AWS Trusted Advisor mostra il punteggio di resilienz a più recente e fornisce uno stato che indica se la politica di resilienza mirata (RTOeRPO) è stata soddisfat ta o meno. Ogni volta che viene eseguita una valutazio ne, viene AWS Resilience Hub aggiornata AWS Trusted Advisor con i risultati più recenti. AWS Trusted Advisor è un servizio che analizza continuamente i tuoi AWS account e fornisce consigli per aiutarti a seguire le AWS migliori pratiche e le linee guida AWS Well-Architected. Per ulteriori informazioni, consulta the section called “AWS Trusted Advisor”.	18 novembre 2022

Supporto per Amazon Simple Notification Service (AmazonSNS)	AWS Resilience Hub ora valuta le applicazioni che utilizzano Amazon SNS analizzando la SNS configura zione di Amazon, inclusi gli abbonati, e fornisce consigli per soddisfare gli obiettivi di ripristino del carico di lavoro stimati dell'organizzazione (carico di lavoro stimato RTO e carico di lavoro stimato) per le applicazioni. RPO Amazon SNS è un servizio gestito che invia messaggi dagli editori (produttori) agli abbonati (consumatori). Per ulteriori informazioni, consulta i seguenti argomenti: • the section called “ AWS Resilience Hub risorse supportate” • the section called “Identity and Access Management” • the section called “Raggrupp amento di risorse in un componente applicativo”	16 novembre 2022

Supporto aggiuntivo per Amazon Route 53 Application Recovery Controller (Amazon Route 53ARC)	AWS Resilience Hub ora valuta Amazon Route 53 ARC for Elastic Load Balancing e Amazon Relational Database Service (RDSAmazon), che include la consulenza sui vantaggi di Amazon Route 53ARC. Estensione del supporto per AWS Resilienc e Hub la ARC valutazione di Amazon Route 53 oltre AWS Auto Scaling Group AWS ASG () e Amazon DynamoDB. Amazon Route 53 ARC offre un'elevata disponibilità per l'applicazione, consentendoti di eseguire rapidamente il failover dell'intera applicazione in una regione di failover. Per ulteriori informazioni, consulta i seguenti argomenti: • the section called “ AWS Resilience Hub risorse supportate” • the section called “Identity and Access Management”	16 novembre 2022

Support aggiuntivo per il AWS Backup	AWS Resilience Hub ora valuta Amazon Route 53 ARC for Elastic Load Balancing e Amazon Relational Database Service (RDSAmazon), che include la consulenza sui vantaggi di Amazon Route 53ARC. Estensione del supporto per AWS Resilienc e Hub la ARC valutazione di Amazon Route 53 oltre AWS Auto Scaling Group AWS ASG () e Amazon DynamoDB. Amazon Route 53 ARC offre un'elevata disponibilità per l'applicazione, consentendoti di eseguire rapidamente il failover dell'intera applicazione in una regione di failover. Per ulteriori informazioni, consulta i seguenti argomenti: • the section called “ AWS Resilience Hub risorse supportate” • the section called “Identity and Access Management”	16 novembre 2022
Contenuto aggiornato: sono state aggiunte nuove risorse relative ai componenti applicativi	Aggiunti Route53 e AWS Backup all'elenco delle risorse dei componenti applicativi supportate nella sezione di AppComponent raggruppamento.	1 luglio 2022

Nuovo contenuto: concetto dello stato di conformità delle applicazioni	È stato aggiunto il tipo di stato «Modifiche rilevate».	2 giugno 2022
Ti presentiamo AWS Resilienc e Hub	AWS Resilience Hub è ora disponibile. Questa guida descrive come utilizzarla AWS Resilience Hub per analizzare l'infrastruttura, ottenere consigli per migliorar e la resilienza delle AWS app, esaminare i punteggi di resilienza e altro ancora.	10 novembre 2021

Glossario AWS

Per la terminologia AWS più recente, consultare il glossario AWS nella documentazione di riferimento per Glossario AWS.

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.