Guida per l'utente

AWS Hub di resilienza

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

AWS Hub di resilienza: Guida per l'utente

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

I marchi e l'immagine commerciale di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in una qualsiasi modalità che possa causare confusione tra i clienti o in una qualsiasi modalità che denigri o discrediti Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà delle rispettive aziende, che possono o meno essere associate, collegate o sponsorizzate da Amazon.

Table of Contents

Che cos'è AWS Resilience Hub? 1
AWS Resilience Hub — Gestione della resilienza 2
Come AWS Resilience Hub funziona 2
AWS Resilience Hub — Test di resilienza 5
AWS Resilience Hub concetti 6
Resilienza 6
Obiettivo del punto di ripristino (RPO) 6
Obiettivo del tempo di ripristino (RTO) 6
Obiettivo stimato del tempo di ripristino del carico di lavoro 6
Obiettivo stimato del punto di ripristino del carico di lavoro 6
Applicazione 7
Componente dell'applicazione 7
Stato di conformità dell'applicazione 7
Rilevamento delle deviazioni 8
Valutazione della resilienza 8
Punteggio di resilienza 8
Tipo di interruzione 8
AWS FIS esperimenti 9
FERMARE 9
AWS Resilience Hub persone 10
AWS Resilience Hub risorse supportate 11
AWS Resilience Hub e MyApplications 15
Ulteriori informazioni 16
Nozioni di base 18
Prerequisiti 18
Aggiunta di un'applicazione 19
Inizia aggiungendo un'applicazione 20
Gestisci le risorse delle tue applicazioni 20
Aggiungi risorse alla tua AWS Resilience Hub applicazione 21
Imposta RTO e RPO 26
Imposta la valutazione programmata e la notifica di deriva 27
Autorizzazioni di configurazione 28
Configurare i parametri di configurazione dell'applicazione 30
Aggiungi tag alla tua applicazione 30

Rivedi e pubblica 31
Esegui una valutazione 31
Usando AWS Resilience Hub 33
AWS Resilience Hub sommario 33
Stato dell'applicazione 34
Principali consigli sull'infrastruttura per tipo di risorsa 35
Consigli sull'infrastruttura 35
Raccomandazioni operative non implementate 35
Consigli sugli allarmi 36
Raccomandazioni SOP 36
AWS FIS consigli sugli esperimenti 36
Applicazioni con derive 37
Punteggio di resilienza 37
Le 10 applicazioni più recenti per il punteggio di resilienza 37
Stato della domanda per politica 38
AWS Resilience Hub cruscotto 38
Stato della domanda 39
Punteggio di resilienza delle applicazioni nel tempo 39
Allarmi implementati 40
Esperimenti implementati 40
Gestione delle applicazioni 40
Visualizzazione del riepilogo dell'applicazione 43
Modifica delle risorse delle applicazioni 45
Gestione dei componenti dell'applicazione 53
Pubblica una nuova versione dell'applicazione 62
Visualizzazione delle versioni delle applicazioni 63
Visualizzazione delle risorse dell'applicazione 64
Eliminazione di un'applicazione 65
Parametri di configurazione dell'applicazione 66
Gestione delle politiche di resilienza 67
Creazione di politiche di resilienza 68
Accesso ai dettagli della politica di resilienza 71
Gestione delle valutazioni della resilienza in AWS Resilience Hub 73
Esecuzione di valutazioni della resilienza in AWS Resilience Hub 73
Revisione dei rapporti di valutazione 74
Eliminazione delle valutazioni di resilienza 83

Gestione delle valutazioni della resilienza dal widget Resiliency 84
Esecuzione di valutazioni della resilienza dal widget Resiliency 85
Revisione del riepilogo della valutazione nel widget Resiliency 87
Gestione degli allarmi 87
Creazione di allarmi sulla base delle raccomandazioni operative 88
Visualizzazione degli allarmi 91
Gestione delle procedure operative standard 94
Creazione di una SOP basata sui consigli AWS Resilience Hub 96
Creazione di un documento SSM personalizzato 97
Utilizzo di un documento SSM personalizzato anziché quello predefinito 98
Test SOPs 98
Visualizzazione delle procedure operative standard 98
Gestione degli AWS Fault Injection Service esperimenti 100
Avvio, creazione ed esecuzione AWS FIS di esperimenti 101
Visualizzazione degli esperimenti AWS FIS 104
AWS Fault Injection Service errori dell'esperimento/controllo dello stato 107
Comprendere i punteggi di resilienza 110
Accesso al punteggio di resilienza delle applicazioni 110
Calcolo dei punteggi di resilienza 113
Integrazione dei consigli nelle applicazioni 125
Modifica del modello AWS CloudFormation 127
AWS Resilience Hub APIs Usato per descrivere e gestire l'applicazione 131
Preparazione della domanda 131
Creazione di un'applicazione 131
Crea una politica di resilienza 132
Importa le risorse dell'applicazione e monitora lo stato delle importazioni 133
Pubblica la tua applicazione e assegna una politica di resilienza 136
Esecuzione e analisi dell'applicazione 137
Esegui e monitora una valutazione della resilienza 138
Crea una politica di resilienza 141
Modifica la tua applicazione 156
Aggiungere manualmente le risorse 156
Raggruppamento delle risorse in un unico componente dell'applicazione 157
Escludere una risorsa da un AppComponent 159
Sicurezza 161
Protezione dei dati 161

Crittografia dei dati a riposo 162
Crittografia in transito 163
Identity and Access Management 163
Destinatari 164
Autenticazione con identità 164
Gestione dell'accesso con policy 168
Come funziona AWS Resilience Hub con IAM 171
Configura i ruoli e le autorizzazioni IAM 184
Risoluzione dei problemi 185
AWS Resilience Hub riferimento alle autorizzazioni di accesso 187
AWS politiche gestite 201
AWS Resilience Hub riferimenti alle persone e alle autorizzazioni IAM 212
Importazione del file di stato Terraform in AWS Resilience Hub 215
Abilitazione AWS Resilience Hub dell'accesso al tuo cluster Amazon EKS 220
Attivazione AWS Resilience Hub della pubblicazione sui tuoi argomenti di Amazon SNS 231
Limitazione delle autorizzazioni per includere o escludere consigli AWS Resilience Hub 233
Sicurezza dell'infrastruttura 234
Controlli di resilienza per i servizi AWS 235
Amazon Elastic File System 236
Tipo di file system 236
Backup del file system 236
Replica dei dati 236
Amazon Relational Database Service e Amazon Aurora 236
Implementazione Single-AZ 237
Multi-AZ deployment (Implementazione Multi-AZ) 237
Backup 237
Failover tra regioni 237
Failover più rapido all'interno della regione 237
Amazon Simple Storage Service 238
Controllo delle versioni 238
Backup pianificato 238
Replica dei dati 238
Amazon DynamoDB 239
Backup pianificato 239
Tabella globale 239
Amazon Elastic Compute Cloud 240

Istanza con stato ... 240
Gruppi Auto Scaling ... 240
EC2 Flotta Amazon ... 240
Amazon EBS ... 241
Backup pianificato ... 241
Backup e replica dei dati ... 241
AWS Lambda ... 241
Cliente Amazon VPC Access ... 242
Coda di lettere morte ... 242
Amazon Elastic Kubernetes Service ... 242
Multi-AZ deployment (Implementazione Multi-AZ) ... 242
Distribuzione vs. ReplicaSet ... 242
Installazione e manutenzione ... 242
Amazon Simple Notification Service ... 243
Abbonamenti tematici ... 243
Amazon Simple Queue Service ... 243
Coda di lettere morte ... 243
Amazon Elastic Container Service ... 244
Multi-AZ deployment (Implementazione Multi-AZ) ... 244
Sistema di bilanciamento del carico elastico ... 244
Multi-AZ deployment (Implementazione Multi-AZ) ... 244
Amazon API Gateway ... 244
Distribuzione tra regioni ... 244
Implementazione di API private Multi-AZ ... 245
Amazon DocumentDB ... 245
Multi-AZ deployment (Implementazione Multi-AZ) ... 245
Distribuzione di cluster elastici e Multi-AZ ... 245
Cluster elastico e istantanee manuali ... 245
Gateway NAT ... 245
Multi-AZ deployment (Implementazione Multi-AZ) ... 245
Amazon Route 53 ... 246
Multi-AZ deployment (Implementazione Multi-AZ) ... 246
Amazon Application Recovery Controller (ARC) ... 246
Multi-AZ deployment (Implementazione Multi-AZ) ... 246
File server Amazon FSx per Windows ... 246
Tipo di file system ... 246

Backup del file system 247
Replica dei dati 247
AWS Step Functions 247
Controllo delle versioni e alias 247
Distribuzione tra regioni 247
Amazon ElastiCache (sistema operativo Redis) 247
Implementazione Single-AZ 248
Implementazione Single-AZ 248
Failover tra regioni 248
Backup 248
Failover più rapido a livello regionale 248
Utilizzo di altri servizi 250
AWS CloudFormation 250
AWS Resilience Hub e AWS CloudFormation modelli 250
Scopri di più su AWS CloudFormation 251
AWS CloudTrail 251
AWS Systems Manager 251
AWS Trusted Advisor 252
Cronologia dei documenti 256
AWS Glossario 290
..... ccxci

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, potete anche creare ed eseguire AWS Fault Injection Service esperimenti che imitano le interruzioni della vostra applicazione nella vita reale per aiutarvi 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 vostra 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
Amazon Application Recovery Controller (ARC) (ARC)	Cos'è Amazon Application Recovery Controller (ARC)

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 e MyApplications

AWS Resilience Hub — Gestione della resilienza

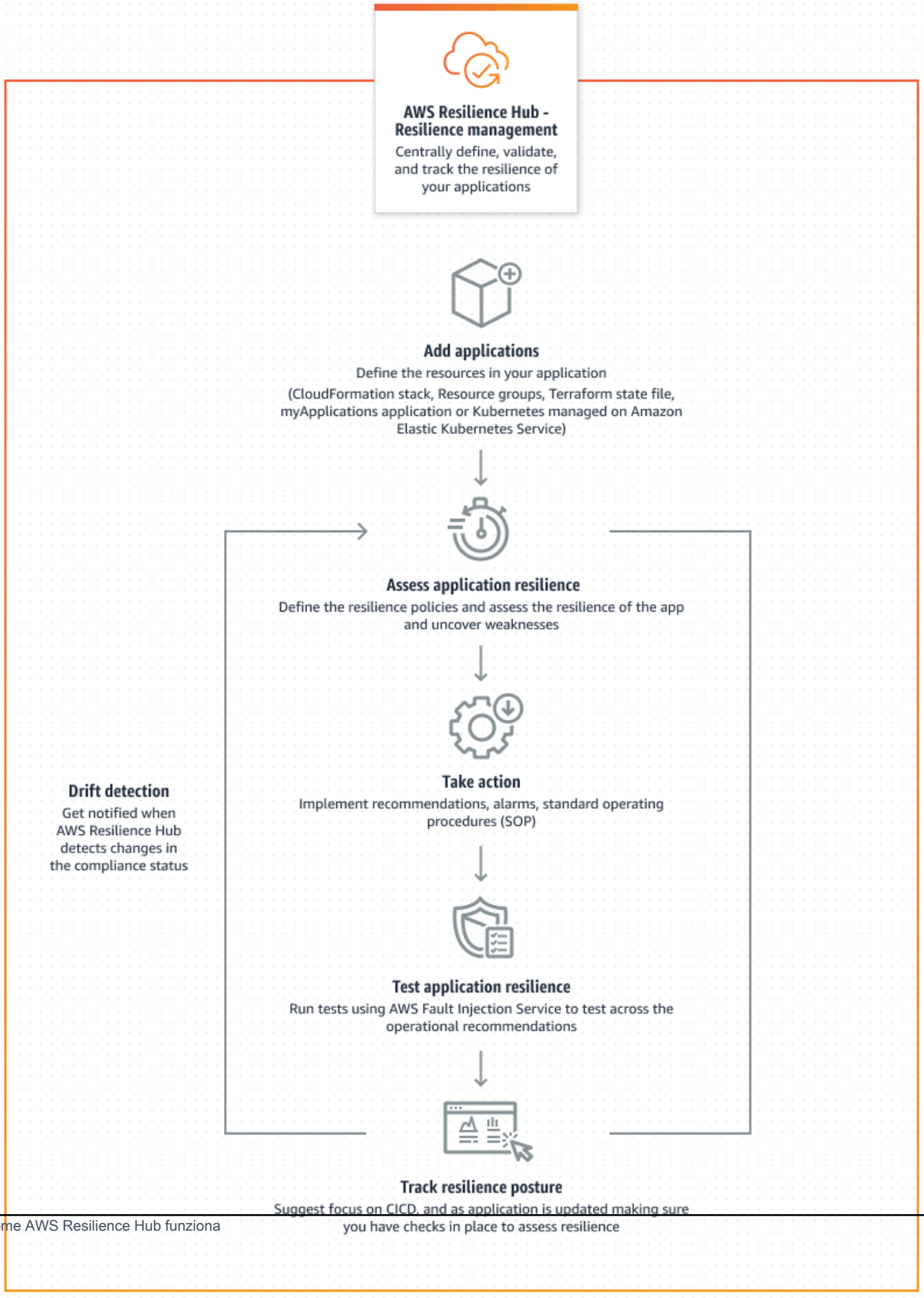
AWS Resilience Hub ti offre una posizione centrale per definire, convalidare e monitorare la resilienza della tua applicazione. AWS AWS Resilience Hub aiuta a proteggere le applicazioni dalle interruzioni e a ridurre i costi di ripristino per ottimizzare la continuità aziendale e contribuire a soddisfare 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 Recovery Time Objective (RTO) e del Recovery Point Objective (RPO) in condizioni diverse.
- 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, myApplications application or Kubernetes managed on Amazon Elastic Kubernetes Service)
Assess application resilience
Define the resilience policies and assess the resilience of the app and uncover weaknesses
Take action
Implement recommendations, alarms, standard operating procedures (SOP)
Test application resilience
Run tests using AWS Fault Injection Service to test across the operational recommendations
Track resilience posture
Suggest focus on CICD, and as application is updated making sure you have checks in place to assess resilience
Drift detection
Get notified when AWS Resilience Hub detects changes in the compliance status

Describe

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 MyApplications.

Definisci

Definisci le politiche di resilienza per le tue applicazioni. Queste politiche includono obiettivi RTO e RPO per 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 fino a quando l'RTO stimato del carico di lavoro e l'RPO stimato del carico di lavoro soddisfano gli obiettivi RTO e 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'avvio di Amazon RDS e problemi con la 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 visualizzare l'interruzione AWS Resilience Hub e avviare il processo di ripristino associato.

AWS Resilience Hub — Test di resilienza

AWS Resilience Hub supporta una maggiore integrazione con. AWS FIS Questa integrazione consente di AWS Resilience Hub offrire consigli personalizzati utilizzando AWS FIS azioni e scenari basati sul contesto specifico dell'applicazione da valutare. L'esecuzione degli esperimenti consigliati o l'esecuzione di test personalizzati utilizzando il AWS FIS servizio contribuiranno direttamente a migliorare il punteggio di resilienza dell'applicazione.

Queste AWS FIS azioni e scenari testano il livello di resilienza di un'applicazione creando eventi dirompenti in modo da poter osservare la risposta dell'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

AWS FIS opzione del menu a discesa	AWS FIS documentazione
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. Questo determina ciò che si considera 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. Questo determina ciò che viene considerato un intervallo di tempo accettabile in caso di indisponibilità del servizio.

Obiettivo stimato del tempo di ripristino del carico di lavoro

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

Obiettivo stimato del punto di ripristino del carico di lavoro

L'obiettivo stimato del punto di ripristino del carico di lavoro (RPO stimato del carico di lavoro) è l'RPO stimato che l'applicazione dovrebbe soddisfare in base alla definizione dell'applicazione importata, quindi esegui 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 obiettivi RTO e RPO definiti nella politica. Tutti i suoi componenti soddisfano gli obiettivi politici definiti. Ad esempio, hai selezionato un obiettivo RTO e RPO di 24 ore per le interruzioni tra AWS le 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 (SOP) di backup 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 gli obiettivi RTO e RPO definiti nella politica. Uno o più di essi AppComponents non soddisfano gli obiettivi politici. Ad esempio, è stato selezionato un obiettivo RTO e RPO 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. A scopo di 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.

AWS FIS esperimenti

AWS Resilience Hub consiglia di sperimentare utilizzando AWS FIS azioni 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 l'RTO stimato del carico di lavoro e l'RPO stimato del carico di lavoro. È possibile testare diverse configurazioni dell'applicazione e misurare se l'RTO e l'RPO di output soddisfano gli obiettivi definiti nella politica.

FERMARE

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, ne AWS Resilience Hub consiglia una serie SOPs e si consiglia di prepararli, testarli e SOPs misurarli 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 personaggi, consulta. the section called “AWS Resilience Hub riferimenti alle persone e alle autorizzazioni IAM”

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 (Amazon EC2)

> **Note**
>
> AWS Resilience Hub non supporta il vecchio formato Amazon Resource Name (ARN) per l'accesso alle risorse Amazon EC2 . Il nuovo formato ARN 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 formato ARN, consulta Migrazione della distribuzione Amazon ECS al nuovo formato ARN e Resource ID.

  - AWS Lambda
  - Amazon Elastic Kubernetes Service (Amazon EKS)
  - Amazon Elastic Container Service (Amazon ECS)
  - AWS Step Functions
- Database
  - Amazon Relational Database Service (Amazon RDS)
  - Amazon DynamoDB
  - Amazon DocumentDB
  - Amazon ElastiCache
- 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 (Amazon EBS)
  - Amazon Elastic File System (Amazon EFS)
  - Amazon Simple Storage Service (Amazon S3)
  - File server Amazon FSx per Windows
- Altri
  - Amazon API Gateway
  - Amazon Application Recovery Controller (ARC) (Amazon ARC)
  - 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
  - Servizi Amazon RDS
  - File server Amazon FSx per Windows
- Amazon ARC AWS Resilience Hub valuta solo Amazon DynamoDB global, Elastic Load Balancing, Amazon RDS e gruppi. 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 cluster Amazon EKS se il cluster Amazon EKS 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 sull'RTO del carico di lavoro stimato o sull'RPO stimato del carico di lavoro: le risorse che non influiscono sull'RTO del carico di lavoro stimato o sull'RPO del carico di lavoro 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-GW HTTP) 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'istanza Amazon RDS. 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 MyApplications AWS Resource Groups.
> - Durante il processo di importazione delle risorse di un'applicazione in AWS Resilience Hub, alcune risorse potrebbero essere ignorate. Quando le risorse vengono ignorate, significa che non possono essere importate affatto. Tuttavia, le risorse contrassegnate come non supportate attualmente non sono compatibili con, AWS Resilience Hub ma potrebbero esserlo in futuro, il che consente di includerle nella domanda di valutazione. Inoltre, AWS Resilience Hub potrebbe ignorare determinate risorse se non sono supportate da. AWS Resource Groups Per ulteriori informazioni sulle risorse supportate da AWS Resource Groups, consulta Tipi di risorse utilizzabili con AWS Resource Groups e Tag Editor.

AWS Resilience Hub e MyApplications

Il widget Resiliency nella dashboard di MyApplications semplifica il processo di valutazione e monitoraggio della resilienza delle applicazioni. Consente di valutare rapidamente la resilienza delle applicazioni definite in MyApplications senza la necessità di ricrearle manualmente nella console. AWS Resilience Hub Questo approccio integrato combina le funzionalità di gestione delle applicazioni di myApplications con le funzionalità di valutazione della resilienza di AWS Resilience Hub, consentendoti di sfruttare i punti di forza di entrambe le piattaforme. Riunendo le definizioni delle applicazioni e le funzionalità di valutazione della resilienza, il widget Resiliency semplifica il flusso di lavoro, consentendoti di accedere alle informazioni pertinenti e intraprendere azioni per migliorare la resilienza da una posizione centralizzata. Quando un'applicazione viene valutata dal widget Resiliency, esegue le seguenti operazioni: AWS Resilience Hub

- Crea l'applicazione selezionata in. AWS Resilience Hub
- Rileva e mappa automaticamente le risorse associate al modello.
- Crea e assegna una nuova politica di resilienza con valori predefiniti per Recovery Time Objective (RTO) e Recovery Point Objective (RPO). Sono quattro ore per RTO e un'ora per RPO. Dopo aver generato una valutazione, è possibile modificare la politica di resilienza o assegnare una politica diversa dalla console. AWS Resilience Hub Per ulteriori informazioni sull'aggiornamento della politica di resilienza e sull'associazione di una politica diversa, consulta. Gestione delle politiche di resilienza
- Valuta la resilienza dell'applicazione rispetto a RTO e RPO definiti nella politica di resilienza per identificare le aree che richiedono miglioramenti nell'architettura dell'applicazione. Gli scenari di errore includono guasti nelle zone di disponibilità, interruzioni regionali e altre potenziali interruzioni.
- Monitora continuamente le risorse dell'applicazione e le modifiche alla configurazione dopo la valutazione iniziale, fornendo avvisi o aggiornamenti se eventuali modifiche influiscono sulla resilienza dell'applicazione.

> **Note**
>
> Prima di iniziare le valutazioni, ti consigliamo di valutare i potenziali costi associati all'esecuzione delle valutazioni utilizzando. AWS Resilience HubPer informazioni dettagliate sui prezzi, consulta i AWS Resilience Hub prezzi.

Dopo aver valutato la tua applicazione, puoi accedere a tutte le funzionalità AWS Resilience Hub del widget selezionando Vai AWS Resilience Hub a per visualizzare i dettagli dell'applicazione nella AWS Resilience Hub console. Il processo di inclusione delle applicazioni di MyApplications in AWS Resilience Hub è regolato dalle regole e dai vincoli seguenti:

- È possibile associare una sola applicazione MyApplications a un'applicazione in. AWS Resilience Hub Cioè, è possibile associare un'applicazione MyApplications a un' AWS Resilience Hub applicazione eseguendo una valutazione dal widget Resiliency nella dashboard MyApplications o completando la Utilizzo delle applicazioni MyApplications procedura mentre si descrive l'applicazione nella console. AWS Resilience Hub
- È possibile includere, valutare e visualizzare solo le applicazioni MyApplications che si trovano all'interno degli stessi confini di AWS regione e AWS account dell'ambiente MyApplications. Le applicazioni create in AWS regioni diverse o con AWS account separati non saranno visibili o accessibili tramite questo widget.
- Puoi aggiungere, rimuovere e aggiornare risorse solo dalla dashboard di MyApplications. Quando si modificano le risorse dell'applicazione dalla dashboard di MyApplications, è necessario reimportarle AWS Resilience Hub per visualizzare le modifiche apportate alle risorse in. AWS Resilience Hub

Ulteriori informazioni

Per ulteriori informazioni sulla gestione delle applicazioni e delle risorse nella dashboard MyApplications, consulta i seguenti argomenti nella documentazione: AWS Console Home

- Su cosa è attivo MyApplications? AWS
- Creazione della prima applicazione in MyApplications
- Gestione delle risorse
- Widget di resilienza

Per ulteriori informazioni sulla descrizione delle applicazioni e sull'esecuzione delle valutazioni in AWS Resilience Hub, consulta i seguenti argomenti:

- Per eseguire per la prima volta una valutazione della resilienza per un'applicazione MyApplications esistente dal widget Resiliency
- Per eseguire nuovamente una valutazione della resilienza per un'applicazione MyApplications esistente dal widget Resiliency

- Revisione del riepilogo della valutazione nel widget Resiliency

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
- Aggiungere un'applicazione a AWS Resilience Hub

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 (primary/secondary/resourceaccount) in AWS Resilience Hub cui desideri utilizzare. 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 utilizzando il file JSON”

  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 in AWS Resilience Hub”
- 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.
- Stima della possibilità di raggiungere l'obiettivo RTO (Recovery Time Objective) e il Recovery Point Objective (RPO).
- Risoluzione dei problemi prima che vengano messi in produzione.

Questa sezione guida l'utente nell'aggiunta di un'applicazione. Raccogli risorse da un'applicazione MyApplications esistente, dagli AWS CloudFormation stack o crea una AWS Resource Groups politica di resilienza appropriata. 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 raggiungere gli obiettivi RTO e RPO del carico di lavoro stimato.

Argomenti

- Inizia aggiungendo un'applicazione
- Seleziona come viene gestita questa applicazione
- Aggiungere raccolte di risorse
- Imposta RTO e RPO

- Imposta le valutazioni pianificate e la notifica delle deviazioni
- Autorizzazioni di configurazione
- Configura i parametri di configurazione dell'applicazione
- Aggiunta di tag
- Rivedi e pubblica la tua AWS Resilience Hub applicazione
- Esegui una valutazione della tua AWS Resilience Hub applicazione

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 applicazione 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

Seleziona come viene gestita questa applicazione

Seleziona come viene gestita questa applicazione

Oltre agli AWS CloudFormation stack AWS Resource Groups, alle applicazioni MyApplications e ai file di stato Terraform, puoi aggiungere risorse che si trovano nei cluster Amazon Elastic Kubernetes Service (Amazon EKS). In altre parole, AWS Resilience Hub consente di aggiungere risorse che si

trovano nei cluster Amazon EKS come risorse opzionali. Questa sezione fornisce le seguenti opzioni, che ti aiutano a determinare la posizione delle risorse delle tue applicazioni.

- 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, applicazioni MyApplications e file di stato Terraform.

  Se si seleziona questa opzione, è necessario completare una delle procedure in. the section called “Aggiungere raccolte di risorse”
- Solo EKS: 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 ed EKS: seleziona questa opzione se desideri scoprire risorse da AWS CloudFormation stack AWS Resource Groups, file di stato Terraform e cluster Amazon EKS.

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

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

Next

Aggiungere raccolte di risorse

Aggiungere raccolte di risorse

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

- Aggiungere raccolte di risorse
- 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 delle applicazioni MyApplications
- Utilizzo dei file di stato Terraform

Utilizzo delle pile AWS CloudFormation

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 stack per scoprire le tue risorse basate sullo stack.
2. Scegli le pile dall'elenco a discesa Scegli 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 in entrambe, scegli la freccia destra adiacente a Aggiungi stack al di fuori della AWS regione e inserisci l'Amazon Resource Name (ARN) dello stack nella casella Inserisci un ARN dello stack, quindi scegli Aggiungi stack ARN. Per ulteriori informazioni in merito ARNs, 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 Scegli un gruppo di risorse.

Per utilizzarli AWS Resource Groups in una regione diversa Account AWS, diversa o in entrambe, scegli la freccia destra adiacente a Resource Group ARN: e inserisci il nome Amazon Resource Name (ARN) AWS Resource Groups nella casella Inserisci un gruppo di risorse ARN, quindi scegli Aggiungi ARN del gruppo di risorse. Per ulteriori informazioni in merito ARNs, consulta Amazon Resource Names (ARNs) nella AWS Guida generale.

Utilizzo delle applicazioni MyApplications

Scegli l'applicazione MyApplications in cui desideri includere AWS Resilience Hub

Per includere l'applicazione MyApplications in AWS Resilience Hub

1. Seleziona MyApplications.
2. Scegli un'applicazione dall'elenco a discesa Seleziona applicazione.

Utilizzo dei file di stato Terraform

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

> **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 campo URI S3 e scegli Aggiungi URL S3.

   Il limite per i file di stato Terraform è di 4 megabyte (MB).
3. Nella finestra di dialogo Scegli un archivio in S3, seleziona il tuo bucket Amazon Simple Storage Service dalla sezione Bucket.

4. Nella sezione Oggetti, seleziona una chiave e scegli Scegli.

Aggiungi cluster EKS

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

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

Scegli i cluster e i namespace Amazon EKS che contengono le risorse che desideri utilizzare nell'applicazione che stai descrivendo. I cluster Amazon EKS 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 cluster Amazon EKS, devi aggiungere manualmente i namespace pertinenti a ciascuno dei cluster Amazon EKS nella sezione Cluster e namespace EKS. Il nome dello spazio dei nomi deve corrispondere esattamente al nome dello spazio dei nomi sui cluster Amazon EKS.

Per aggiungere cluster Amazon EKS

1. In 1. Seleziona la sezione cluster EKS, scegli i cluster Amazon EKS dall'elenco a discesa Scegli i cluster EKS associati alla tua regione. Account AWS
2. Per utilizzare cluster Amazon EKS che si trovano in una regione diversa Account AWS, diversa o entrambe, scegli la freccia destra adiacente a Aggiungi un cluster EKS all'interno di un account

o regione diverso e inserisci il nome Amazon Resource Name (ARN) del cluster Amazon EKS nella casella Inserisci un ARN EKS, quindi scegli Aggiungi ARN EKS. Per ulteriori informazioni in merito ARNs, 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 “Abilitazione AWS Resilience Hub dell'accesso al tuo cluster Amazon EKS”

Per aggiungere namespace dai cluster Amazon EKS selezionati

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

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

   - Nome cluster EKS: indica il nome dei cluster Amazon EKS 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 cluster Amazon EKS selezionati nell'applicazione. Puoi identificare lo stato utilizzando le seguenti opzioni:
     - Namespace richiesto: 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 uno spazio dei nomi, nella finestra di dialogo Aggiorna namespace, scegli Aggiungi un nuovo spazio dei nomi.

   La finestra di dialogo Aggiorna namespaces mostra tutti i namespace che hai selezionato dal tuo cluster Amazon EKS, come opzione modificabile.
3. Nella finestra di dialogo Aggiorna gli spazi dei nomi, 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 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 cluster Amazon EKS, scegli Applica namespace a tutti i cluster EKS.

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

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

Next

Imposta RTO e RPO

Imposta RTO e RPO

È possibile definire una nuova politica di resilienza con obiettivi personalizzati. RTO/RPO targets, or you can choose an existing resiliency policy with predefined RTO/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 nella casella Inserisci il nome della politica (sotto Nome).

   Abbiamo precompilato questo campo con un nome generato automaticamente. Puoi scegliere di utilizzare lo stesso nome o fornire un nome diverso.
3. (Facoltativo) Inserisci una descrizione per la politica di resilienza nella casella Descrizione.
4. Definite il vostro RTO/RPO nella sezione Obiettivi RTO/RPO.

> **Note**
>
> - Abbiamo precompilato un RTO e un RPO predefiniti per la tua applicazione. Puoi modificare l'RTO e l'RPO ora o dopo aver valutato l'applicazione.
> - 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 si immette un valore zero nei campi RTO e RPO, i risultati 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.

5. Per definire RTO/RPO per la tua infrastruttura e AZ, scegli la freccia destra per espandere la sezione RTO e RPO dell'infrastruttura.
6. Nei target RTO/RPO, inserisci un valore numerico nella casella, quindi scegli l'unità di tempo che il valore rappresenta sia per RTO che per RPO.

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

   In RTO e RPO, inserite un valore numerico nella casella, quindi scegliete l'unità di tempo che il valore rappresenta sia per RTO che per RPO.

Next

the section called “Imposta la valutazione programmata e la notifica di deriva”

Imposta le valutazioni pianificate 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 ruolo IAM appropriato.
   - Se l'applicazione è configurata con le attuali autorizzazioni utente IAM, 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 (Amazon SNS). Per fornire un argomento su Amazon SNS, nella sezione Fornisci un argomento SNS, seleziona l'opzione Scegli un argomento SNS e seleziona un argomento Amazon SNS dall'elenco a discesa Scegli un argomento SNS.

   > **Note**
   >
   > - AWS Resilience Hub Per consentire la pubblicazione di notifiche sui tuoi argomenti Amazon SNS, l'argomento Amazon SNS 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 argomenti di Amazon SNS”
   > - 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 argomenti di Amazon SNS che si trovano in una regione diversa Account AWS o diversa, o entrambi, seleziona Inserisci l'argomento SNS ARN e inserisci il nome Amazon Resource Name (ARN) dell'argomento Amazon SNS nella casella Fornisci un argomento SNS. Per ulteriori informazioni in merito ARNs, consulta Amazon Resource Names (ARNs) nella AWS Guida generale.

Next

Autorizzazioni di configurazione

Autorizzazioni di configurazione

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 i ruoli IAM e le autorizzazioni IAM

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

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

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

   - AWS Console IAM: se scegli questa opzione, devi completare la procedura in Per creare il tuo AWS Resilience Hub ruolo nella console IAM.
   - AWS CLI: se scegli questa opzione, devi completare tutti i passaggi in AWS CLI.
   - CloudFormation modello: se scegli questa opzione, a seconda del tipo di account (account primario o account secondario), devi creare i ruoli utilizzando il modello appropriato AWS CloudFormation .
2. Scegli la freccia destra per espandere la sezione Aggiungi ruolo/i IAM da un account incrociato - Facoltativo.
3. Per selezionare i ruoli IAM da un account incrociato, inserisci il ARNs ruolo IAM nella casella Enter an IAM role ARN. Assicurati che i ARNs ruoli IAM che stai inserendo non appartengano all'account corrente.
4. Se desideri utilizzare l'utente IAM corrente per scoprire le risorse della tua applicazione, scegli la freccia destra per espandere Usa la sezione Utilizza le autorizzazioni utente IAM correnti e seleziona Capisco che devo configurare manualmente le autorizzazioni per abilitare la funzionalità richiesta all'interno. AWS Resilience Hub

   Se selezioni questa opzione, alcune AWS Resilience Hub funzionalità (come la notifica di deviazione) potrebbero non funzionare come previsto e gli input che hai fornito per la creazione di una nuova applicazione verranno ignorati.

Next

Configura i parametri di configurazione dell'applicazione

Configura i 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

Aggiunta di tag

Aggiunta di 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

Rivedi e pubblica la tua AWS Resilience Hub applicazione

Rivedi e pubblica la tua AWS Resilience Hub applicazione

Dopo aver creato l'applicazione, potete comunque esaminarla e modificarne le risorse. Al termine, scegliete Pubblica per pubblicare l'applicazione.

> **Note**
>
> AWS Resilience Hub analizza le risorse dell'applicazione in background e verifica se possono essere raggruppate in modo più efficiente per migliorare l'accuratezza delle valutazioni.
> Se AWS Resilience Hub identifica le risorse che possono essere raggruppate in pertinenti AppComponents, visualizza un avviso informativo relativo ai consigli di raggruppamento delle risorse nella scheda Struttura dell'applicazione della pagina dell'applicazione ed è possibile esaminarle scegliendo Rivedi consigli. Per ulteriori informazioni, consulta the section called “AWS Resilience Hub consigli per il raggruppamento delle risorse”.

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

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

Next

Esegui una valutazione della tua AWS Resilience Hub applicazione

Esegui una valutazione della tua 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 riepilogo
- AWS Resilience Hub cruscotto
- Descrizione e gestione delle applicazioni AWS Resilience Hub
- Gestione delle politiche di resilienza
- Esecuzione e gestione delle valutazioni della resilienza in AWS Resilience Hub
- Esecuzione e gestione delle valutazioni della resilienza dal widget Resilienza
- Gestione degli allarmi
- Gestione delle procedure operative standard
- Gestione degli AWS Fault Injection Service esperimenti
- Comprendere i punteggi di resilienza
- Integrazione dei consigli operativi nella tua applicazione con AWS CloudFormation

AWS Resilience Hub riepilogo

AWS Resilience Hub fornisce un riepilogo visivo con diagrammi e grafici che consente di at-a-glance visualizzare lo stato di resilienza dell'applicazione su più AWS servizi e risorse. Questo riepilogo visivo completo e conciso consente di identificare rapidamente potenziali lacune di resilienza, assegnare priorità alle azioni e tenere traccia dei progressi nel miglioramento della capacità dell'applicazione di riprendersi dalle interruzioni. Quando scegli Esporta e se esporti i parametri per la prima volta, AWS Resilience Hub crea un nuovo bucket Amazon S3 nella regione da cui stai accedendo. AWS Resilience Hub Questo bucket Amazon S3 viene creato solo per la prima volta e verrà utilizzato per salvare i parametri esportati una volta completato con successo. Sono previsti costi aggiuntivi per l'archiviazione dei dati esportati in Amazon S3. Per ulteriori informazioni su questi addebiti, consulta i prezzi di Amazon S3.

Le tabelle e i grafici nei widget ti aiutano a comprendere quanto segue:

- Panoramica del punteggio di resilienza complessivo dell'applicazione e dello stato operativo attuale.
- Potenziali violazioni delle policy o deviazioni dalle migliori pratiche, evidenziando le applicazioni che non sono conformi alle policy stabilite o che si sono discostate dalle configurazioni consigliate. Inoltre, evidenzia anche aree specifiche che consentono di stabilire le priorità e affrontarle.
- Risorse o applicazioni critiche che richiedono attenzione immediata.
- Raccomandazioni per migliorare le pratiche di resilienza, come l'implementazione di allarmi, lo svolgimento di AWS Fault Injection Service (AWS FIS) esperimenti e la definizione di procedure operative standard. Questi consigli vengono tracciati nel tempo e consentono di monitorare l'avanzamento dell'implementazione e misurare l'impatto sulla resilienza complessiva dell'applicazione.

Widget

- Stato dell'applicazione
- Principali consigli sull'infrastruttura per tipo di risorsa
- Consigli sull'infrastruttura
- Raccomandazioni operative non implementate
- Consigli sugli allarmi
- Raccomandazioni SOP
- AWS FIS consigli sugli esperimenti
- Applicazioni con derive
- Punteggio di resilienza
- Le 10 applicazioni più recenti per il punteggio di resilienza
- Stato della domanda per politica

Stato dell'applicazione

Questo widget indica se le applicazioni sono conformi o meno alla politica di resilienza. Scegli il numero adiacente al numero delle applicazioni nel pop-up per visualizzare tutte le applicazioni associate nel riquadro Applicazioni. Per visualizzare tutte le applicazioni che hai creato, scegli Visualizza applicazioni. Per ulteriori informazioni sulla gestione delle applicazioni in AWS Resilience Hub, vedereVisualizzazione del riepilogo di un' AWS Resilience Hub applicazione.

Principali consigli sull'infrastruttura per tipo di risorsa

Questo widget mostra il numero di raccomandazioni sull'infrastruttura per ogni tipo di AWS risorsa fornite nell'ultima valutazione riuscita per migliorarne il livello di resilienza. Puoi identificare i dettagli passandoci sopra con il mouse o navigando verso di essi. Per visualizzare tutte le applicazioni che hai creato, scegli Visualizza applicazioni. Per ulteriori informazioni sui consigli relativi all'infrastruttura, consultaRevisione delle raccomandazioni sulla resilienza.

Consigli sull'infrastruttura

Questo widget elenca fino a 10 applicazioni con il numero massimo di raccomandazioni sull'infrastruttura fornite nell'ultima valutazione riuscita per migliorarne il livello di resilienza. Per visualizzare tutte le applicazioni che hai creato, scegli Visualizza applicazioni. Per ulteriori informazioni sui consigli relativi all'infrastruttura, consultaRevisione delle raccomandazioni sulla resilienza.

È possibile identificare i dettagli utilizzando quanto segue:

- Nome dell'applicazione: nome dell'applicazione che hai fornito durante la definizione AWS Resilience Hub.
- Numero: indica il numero di raccomandazioni sull'infrastruttura fornite AWS Resilience Hub nell'ultima valutazione riuscita. Scegli il numero per visualizzare tutti i consigli sull'infrastruttura forniti nel rapporto di valutazione.
- Ultima valutazione: indica la data e l'ora in cui la domanda è stata valutata con successo l'ultima volta.

Raccomandazioni operative non implementate

Questo widget elenca fino a 10 applicazioni con il numero massimo di raccomandazioni operative non implementate fornite nell'ultima valutazione riuscita per migliorarne il livello di resilienza. Per visualizzare tutte le applicazioni che hai creato, scegli Visualizza applicazioni. Per ulteriori informazioni sui consigli operativi, vedereRevisione delle raccomandazioni operative.

È possibile identificare i dettagli utilizzando quanto segue:

- Nome dell'applicazione: nome dell'applicazione che hai fornito durante la definizione AWS Resilience Hub.

- Conteggio: indica il numero di raccomandazioni operative fornite AWS Resilience Hub nell'ultima valutazione riuscita. Scegli il numero per visualizzare tutte le raccomandazioni operative non implementate nel rapporto di valutazione.
- Ora dell'ultima valutazione: indica la data e l'ora in cui la domanda è stata valutata con successo l'ultima volta.

Consigli sugli allarmi

Questo widget elenca tutti i consigli sugli CloudWatch allarmi di Amazon forniti per migliorare la posizione di resilienza in un periodo di tempo selezionato. Le diverse categorie (Implementato, Non implementato ed Escluso) indicano lo stato di implementazione nell'applicazione. Puoi visualizzare il numero di CloudWatch allarmi consigliati da Amazon per ogni categoria passando il mouse su di essi o navigando verso di essi. Per visualizzare tutte le applicazioni che hai creato, scegli Visualizza applicazioni. Per ulteriori informazioni sui consigli sugli allarmi, consultaRevisione delle raccomandazioni operative.

Raccomandazioni SOP

Questo widget elenca tutte le raccomandazioni sulla procedura operativa standard (SOP) fornite per migliorare la posizione di resilienza in un periodo di tempo selezionato. Le diverse categorie (Implementato, Non implementato ed Escluso) indicano lo stato di implementazione nell'applicazione. È possibile visualizzare il numero di raccomandazioni SOP per ciascuna categoria passando il mouse su di esse o navigando verso di esse. Per visualizzare tutte le applicazioni che hai creato, scegli Visualizza applicazioni. Per ulteriori informazioni sui consigli operativi, vedereRevisione delle raccomandazioni operative.

AWS FIS consigli sugli esperimenti

Questo widget elenca tutti i consigli AWS FIS sperimentali forniti per migliorare la postura di resilienza in un periodo di tempo selezionato. Le diverse categorie (Implementato, Non implementato, Implementato parzialmente ed Escluso) indicano lo stato di implementazione nell'applicazione. È possibile visualizzare il numero di consigli sugli AWS FIS esperimenti per ciascuna categoria passando il mouse su di essi o navigando verso di essi. Per visualizzare tutte le applicazioni che hai creato, scegli Visualizza applicazioni. Per ulteriori informazioni sui consigli sugli AWS FIS esperimenti, consultaGestione delle procedure operative standard.

Applicazioni con derive

Questo widget elenca tutte le applicazioni che hanno abbandonato lo stato di conformità precedente nell'ultima valutazione positiva. Per visualizzare tutte le applicazioni che hai creato, scegli Visualizza applicazioni. Per ulteriori informazioni sulla gestione delle applicazioni in AWS Resilience Hub, vedereVisualizzazione del riepilogo di un' AWS Resilience Hub applicazione.

È possibile identificare i dettagli utilizzando quanto segue:

- Nome dell'applicazione: nome dell'applicazione che hai fornito durante la definizione AWS Resilience Hub.
- Modifiche delle politiche: scegliete il numero adiacente al nome dell'applicazione per visualizzare tutti i componenti dell'applicazione che erano conformi alla politica nella valutazione precedente ma non erano conformi nella valutazione corrente.
- Variazioni delle risorse: scegliete il numero seguente per visualizzare tutte le risorse che sono state modificate rispetto alla loro configurazione nell'ultima importazione.

Punteggio di resilienza

Questo widget mostra l'andamento del punteggio di resilienza dell'applicazione in un periodo di tempo selezionato per un massimo di cinque applicazioni. È possibile visualizzare il punteggio di resilienza di un'applicazione passando il mouse sulla riga associata al nome dell'applicazione o navigando verso di essa, quindi scegliendo il nome dell'applicazione per visualizzare il riepilogo dell'applicazione. Per visualizzare tutte le applicazioni che hai creato, scegli Visualizza applicazioni. Per ulteriori informazioni sul punteggio di resilienza, vedereComprendere i punteggi di resilienza.

Le 10 applicazioni più recenti per il punteggio di resilienza

Questo widget elenca fino a 10 applicazioni con i punteggi di resilienza più bassi risultanti dalle valutazioni più recenti, evidenziando le applicazioni che richiedono un'attenzione immediata per migliorarne la resilienza. Per visualizzare tutte le applicazioni che hai creato, scegli Visualizza applicazioni. Per ulteriori informazioni sul punteggio di resilienza, vedereComprendere i punteggi di resilienza.

È possibile identificare i dettagli utilizzando quanto segue:

- Nome dell'applicazione: nome dell'applicazione che hai fornito durante la definizione AWS Resilience Hub.

- Punteggio di resilienza: il punteggio di resilienza complessivo determinato da AWS Resilience Hub per l'applicazione dopo l'esecuzione della valutazione.
- Ora dell'ultima valutazione: indica la data e l'ora in cui la domanda è stata valutata con successo l'ultima volta.

Stato della domanda per politica

Questo widget elenca tutte le tue politiche e il numero di applicazioni che le hanno violate, rispettate o che devono ancora essere valutate in base a tali norme. Per visualizzare tutte le politiche che hai creato, scegli Visualizza politiche. Per ulteriori informazioni sul punteggio di resilienza, vedereGestione delle politiche di resilienza.

È possibile identificare i dettagli utilizzando quanto segue:

- Nome della politica: indica il nome della politica che hai fornito durante la definizione in AWS Resilience Hub.
- Tipo: indica il tipo di politica (politica di resilienza) allegata all'applicazione.
- Nome della policy: indica il numero di applicazioni che hanno violato gli obiettivi RTO e RPO definiti nella politica di resilienza.
- App soddisfatte: indica il numero di applicazioni conformi alla politica di resilienza.
- App non valutate: indica il numero di applicazioni che devono ancora essere valutate rispetto alla politica di resilienza.
- Punteggio di resilienza: il punteggio di resilienza complessivo determinato da AWS Resilience Hub per l'applicazione dopo l'esecuzione della valutazione.
- Ora dell'ultima valutazione: indica la data e l'ora in cui la domanda è stata valutata con successo l'ultima volta.

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 and (). CloudWatch AWS 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 () SOPs 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 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 AWS FIS.

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 l'RTO del carico di lavoro stimato e l'RPO stimato del carico di lavoro non soddisfano gli obiettivi RTO e 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 tua candidatura non viene valutata automaticamente ogni giorno AWS Resilience Hub e che devi valutare manualmente la tua candidatura.
- 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.
  - Non alla deriva: indica che si stima che l'applicazione soddisfi ancora gli obiettivi RTO e RPO definiti nella policy. Inoltre, indica anche che le risorse all'interno delle fonti di input, incluse nella versione corrente dell'applicazione, non sono state aggiunte o rimosse.
- RTO del carico di lavoro stimato: indica l'RTO del carico di lavoro stimato massimo possibile dell'applicazione. Questo valore è l'RTO del carico di lavoro massimo stimato per tutti i tipi di interruzione in base all'ultima valutazione riuscita.
- RPO stimato del carico di lavoro: indica l'RPO stimato massimo possibile del carico di lavoro dell'applicazione. Questo valore è l'RTO massimo stimato del carico di lavoro per tutti i tipi di interruzione dell'ultima valutazione effettuata con esito positivo.
- 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 merito ARNs, consulta Amazon Resource Names (ARNs) nella AWS Guida generale.

> **Note**
>
> AWS Resilience Hub può valutare in modo completo la resilienza delle risorse Amazon ECS 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
- Modifica delle risorse delle AWS Resilience Hub applicazioni
- Gestione dei componenti dell'applicazione
- Pubblicazione di una nuova versione AWS Resilience Hub dell'applicazione
- Visualizzazione di tutte le versioni AWS Resilience Hub dell'applicazione
- Visualizzazione delle risorse dell' AWS Resilience Hub applicazione
- Eliminazione di un'applicazione AWS Resilience Hub

- Parametri di configurazione dell'applicazione

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 riquadro 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
- Riepilogo
- Resilienza delle applicazioni
- Allarmi implementati
- Esperimenti implementati

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 raccomandazione nel riepilogo della valutazione prima di utilizzare l'output di un LLM.

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 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 il SOP corretto.

Ad esempio, supponiamo che ciò AWS Resilience Hub consigli un test con un allarme e un SOP. Quando il test viene eseguito, l'allarme avvia il SOP associato, che viene quindi 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 AWS Fault Injection Service esperimenti.

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 sulle fonti 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 le 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 indicatiImposta le valutazioni pianificate e la notifica delle deviazioni, quindi torna a questa procedura.
5. Scegli Abilita .

   L'attivazione della notifica di deviazione 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 indicatiImposta le valutazioni pianificate e la notifica delle deviazioni, quindi torna a questa procedura.
5. Seleziona 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 inAutorizzazioni di configurazione, 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, scegliete il nome dell'applicazione che desiderate 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 sorgenti 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 sorgente 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, applicazioni MyApplications 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 “Aggiungi risorse alla tua 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, questa 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'applicazione MyApplications 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' 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. Le fonti di input includono AWS CloudFormation pile, applicazioni MyApplications 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 EC2 istanza Amazon 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 inAggiungere raccolte di risorse, quindi tornate a questa procedura.

   c. Seleziona 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 della risorsa.
e. Scegli Aggiungi.

7. Per modificare il nome della risorsa, selezionate una risorsa, scegliete Modifica nome risorsa da Azioni, quindi completate i seguenti passaggi:
   a. Immettete l'ID logico della risorsa nella casella Nome risorsa.
   b. Seleziona 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 della risorsa.
   b. Seleziona 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 il file AppComponents della 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. Seleziona 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 si dispone di un database

primario e di replica, entrambi i database appartengono allo stesso AppComponent database. 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::ElastiCache::CacheCluster`
  - `AWS::ElastiCache::GlobalReplicationGroup`
  - `AWS::ElastiCache::ReplicationGroup`
  - `AWS::ElastiCache::ServerlessCache`
  - `AWS::RDS::DBCluster`
  - `AWS::RDS::DBInstance`
- `AWS::ResilienceHub::NetworkingAppComponent`
  - `AWS::EC2::NatGateway`
  - `AWS::ElasticLoadBalancing::LoadBalancer`
  - `AWS::ElasticLoadBalancingV2::LoadBalancer`

    - `AWS::Route53::RecordSet`
- `AWS:ResilienceHub::NotificationAppComponent`
    - `AWS::SNS::Topic`
- `AWS::ResilienceHub::QueueAppComponent`
    - `AWS::SQS::Queue`
- `AWS::ResilienceHub::StorageAppComponent`
    - `AWS::Backup::BackupPlan`
    - `AWS::EC2::Volume`
    - `AWS::EFS::FileSystem`
    - `AWS::FSx::FileSystem`

      > **Note**
      >
      > Attualmente, AWS Resilience Hub supporta solo Amazon FSx for Windows File Server.

    - `AWS::S3::Bucket`

Argomenti

- Raggruppamento di risorse in un componente applicativo

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 al AppComponent momento dell'importazione, ma il raggruppamento potrebbe non essere sempre accurato al 100%. Alcune risorse sono bloccate per il raggruppamento manuale e verranno raggruppate automaticamente quando applicabile, poiché questi servizi hanno dipendenze rigorose che richiedono configurazioni di raggruppamento specifiche. Per un elenco completo dei servizi bloccati per il raggruppamento manuale, consulta. the section called “Servizi bloccati per il raggruppamento manuale”

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 le risorse che possono essere raggruppate in nuove risorse AppComponents, visualizza la stessa voce delle raccomandazioni e consente di accettarle 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 insieme 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 l'RTO del carico di lavoro stimato e l'RPO del carico di lavoro stimato per generare raccomandazioni.

Di seguito sono riportati alcuni esempi di raggruppamenti corretti:

- Raggruppa database e repliche primari in un unico database. AppComponent
- Raggruppa EC2 le istanze Amazon che eseguono la stessa applicazione in un'unica AppComponent istanza.
- Raggruppa i servizi Amazon ECS in una regione e fai il failover dei servizi Amazon ECS in un'altra regione in un'unica regione. AppComponent

Per ulteriori informazioni sulla revisione e sull'inclusione dei consigli di 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

Servizi bloccati per il raggruppamento manuale

AWS Resilience Hub ti impedisce di raggruppare manualmente le risorse di determinati AWS servizi per evitare errori di configurazione che potrebbero influire sulla valutazione della resilienza e sui consigli per l'applicazione. Questi servizi vengono raggruppati automaticamente in base alle dipendenze e alle configurazioni. Quando si definisce un'applicazione comprensiva di queste risorse, questa ne analizza le relazioni AWS Resilience Hub, le dipendenze e i requisiti di resilienza per creare raggruppamenti ottimali che garantiscano risultati di valutazione accurati.

Elenco dei AWS servizi bloccati per il raggruppamento manuale:

- Amazon API Gateway
- Amazon DocumentDB
- Amazon DynamoDB
- Amazon Elastic Block Store
- Amazon Elastic File System
- Amazon Relational Database Service
- Amazon S3
- Amazon Simple Queue Service
- FSx per Windows File Server
- Gateway NAT

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**
>
> Puoi concedere le autorizzazioni IAM necessarie per lavorare utilizzando una AWS Resilience Hub policy `AWSResilienceHubAsssessmentExecutionPolicy` AWS gestita. Per ulteriori informazioni sulla policy AWS gestita, consultaAWSResilienceHubAsssessmentExecutionPolicy.

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 scopre 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 MyApplications 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 di Bozza.
5. Scegliere la scheda Resources (Risorse).
6. Seleziona la casella di controllo adiacente a Logical ID per selezionare la risorsa.
7. Scegli Cambia 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 inModifica 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 della resilienza in AWS Resilience Hub

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 MyApplications 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, applicazioni MyApplications 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.

- 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 50 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, ad esempio EC2 istanze.

- Zona di disponibilità (AZ) dell'infrastruttura cloud: 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 “Inizia aggiungendo un'applicazione” alla finethe section called “Aggiungi tag alla tua 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 mentre 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 della resilienza in AWS Resilience Hub

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

I consigli sugli allarmi consentono di impostare allarmi che rilevano interruzioni. Le raccomandazioni SOP forniscono script che gestiscono i processi di ripristino più comuni, come il ripristino da un backup. I consigli sui 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.

Argomenti:

- Esecuzione di valutazioni della resilienza in AWS Resilience Hub
- Revisione dei rapporti di valutazione
- Eliminazione delle valutazioni di resilienza

Esecuzione di valutazioni della resilienza in AWS Resilience Hub

È possibile eseguire valutazioni della resilienza da più postazioni in. AWS Resilience Hub Per ulteriori informazioni sulla tua applicazione, consulta. the 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 sezione 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 i tag per cercare e filtrare le risorse AWS

Report di valutazione

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 RTO e RPO effettive e determina se il componente applicativo è in grado di raggiungere gli obiettivi della policy.

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. Scegliete 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 MyApplications 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 RTO stimato del carico di lavoro.

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 RPO stimato del carico di lavoro.

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.

- RTO stimato

  Indica se la configurazione della politica è in linea con i requisiti della politica. Forniamo due valori, il nostro RTO stimato e il vostro RTO mirato. Ad esempio, se vedi un valore di 2 ore per l'RTO mirato e 40 milioni per l'RTO del carico di lavoro stimato, ciò indica che forniamo un RTO del carico di lavoro stimato di 40 minuti, mentre l'RTO attuale dell'applicazione è di due ore. Il calcolo dell'RTO stimato del carico di lavoro si basa sulla configurazione, non sulla policy. Di conseguenza, un database con zone di disponibilità multiple avrà lo stesso carico di lavoro RTO stimato in caso di errore della zona di disponibilità, indipendentemente dalla politica selezionata.
- Deriva RTO

  Indica la durata entro la quale l'applicazione si è allontanata dall'RTO del carico di lavoro stimato della valutazione precedente con esito positivo. Forniamo due valori, il nostro RTO stimato e la deriva RTO. Ad esempio, se vedi un valore di 2 ore per l'RTO stimato e di 40 m per il valore RTO

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

- RPO stimato

  Mostra la politica RPO effettiva del carico di lavoro AWS Resilience Hub stimato, in base alla politica RPO mirata impostata per ogni componente dell'applicazione. Ad esempio, è possibile che l'obiettivo RPO nella politica di resilienza per i guasti della zona di disponibilità sia stato impostato 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 obiettivo RTO e RPO che puoi scegliere di non fornire è la regione. Per alcune applicazioni, è utile pianificare il ripristino quando esiste una dipendenza cruciale da un servizio AWS, che potrebbe non essere disponibile nell'intera regione.

  Se scegli questa opzione, ad esempio impostando obiettivi RTO o RPO per la regione, riceverai un tempo di ripristino stimato e consigli operativi per tali errori.
- Deriva RPO

  Indica la durata entro la quale l'applicazione si è allontanata dall'RPO del carico di lavoro stimato della valutazione precedente con esito positivo. Forniamo due valori, l'RPO stimato e la deriva RPO. Ad esempio, se vedi un valore di 2 ore nell'ambito dell'RPO stimato e di 40 m in quello dell'RPO, ciò indica che l'applicazione si discosta di 40 minuti dall'RPO del carico di lavoro stimato della precedente valutazione con esito positivo.

Revisione delle raccomandazioni sulla resilienza

I consigli sulla resilienza valutano i componenti dell'applicazione e consigliano come ottimizzarli in base all'RTO stimato del carico di lavoro e all'RPO stimato del carico di lavoro, 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 obiettivi RTO e RPO regionali, AWS Resilience Hub visualizza Optimize for Region RTO/RPO nelle opzioni consigliate. Se non sono impostati obiettivi RTO e RPO regionali, viene visualizzato l'RTO/RPO di Optimize for Availability Zone (AZ). Per ulteriori informazioni sull'impostazione degli obiettivi RTO/RPO regionali durante la creazione di politiche di resilienza, vedere. Creazione di politiche di resilienza
- I valori RTO del carico di lavoro stimato e RPO del carico di lavoro stimato per le applicazioni e le relative configurazioni sono determinati considerando la quantità di dati e i singoli dati. AppComponents Tuttavia, questi valori sono solo stime. È necessario utilizzare i propri test (ad esempio AWS Fault Injection Service) per verificare i tempi di ripristino effettivi dell'applicazione.

Ottimizzazione per Availability Zone RTO/RPO

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

Ottimizzazione per Region RTO/RPO

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

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 stimato (RTO e RPO)

  L'RTO del carico di lavoro stimato e l'RPO del carico di lavoro stimato dopo le modifiche.

AWS Resilience Hub valuta se un componente applicativo (AppComponent) è conforme a una policy di resilienza. Se AppComponent non è conforme a una policy 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 la soluzione selezionata AppComponent non possa essere rispettato entro i limiti di. AppComponent Esempi di AppComponent vincoli includono il tipo di risorsa, la dimensione dello storage 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 l'URI di Amazon Simple Storage Service anziché utilizzare CLI/API con 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 esperimenti SOPs, 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 un URL di Amazon Simple Storage Service (Amazon S3).
- 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 i 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 in AWS Resilience Hub” 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. È possibile 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 consigliate SOPs, 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 una SOP dalla colonna Stato.

   b. In Azioni, scegli Escludi selezionati per escludere i selezionati SOPs dall'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 includere SOPs, 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.

Esecuzione e gestione delle valutazioni della resilienza dal widget Resilienza

AWS Resilience Hub consente di eseguire valutazioni per le applicazioni create e gestite nel widget MyApplications in Resiliency. Ogni volta che si apportano modifiche a un'applicazione, si consiglia di eseguire una valutazione della resilienza dal widget Resiliency o dalla console. AWS Resilience Hub Durante questa valutazione, la configurazione di ogni componente dell'applicazione viene valutata rispetto a politiche e best practice consolidate. Sulla base di questa valutazione, la valutazione genera raccomandazioni per l'impostazione degli allarmi, la creazione di procedure operative standard (SOPs) e l'implementazione di strategie di test. L'implementazione di questi consigli di configurazione può migliorare la velocità e l'efficienza delle procedure di ripristino, garantendo una risposta più rapida agli incidenti e riducendo al minimo i potenziali tempi di inattività.

I consigli sugli allarmi consentono di impostare allarmi che rilevano interruzioni. Le raccomandazioni SOP forniscono script che gestiscono i processi di ripristino più comuni, come il ripristino da un backup. I consigli sui 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.

Argomenti:

- Esecuzione di valutazioni della resilienza dal widget Resiliency
- Revisione del riepilogo della valutazione nel widget Resiliency

Esecuzione di valutazioni della resilienza dal widget Resiliency

Per le applicazioni create nel widget MyApplications, ora puoi eseguire valutazioni di resilienza dal widget Resiliency e dalla console. AWS Resilience Hub Per ulteriori informazioni sull'esecuzione delle valutazioni della resilienza dalla console, consulta. AWS Resilience Hub Esecuzione di valutazioni della resilienza in AWS Resilience Hub

Per eseguire per la prima volta una valutazione della resilienza per un'applicazione MyApplications esistente dal widget Resiliency

1. Accedi alla console di gestione.AWS
2. Espandi la barra laterale sinistra e scegli MyApplications.
3. Seleziona l'applicazione per la quale desideri eseguire la valutazione.

   Come prerequisito, assicurati di aver aggiunto il widget Resilienza nella tua AWS console. Per aggiungere questo widget, completa i seguenti passaggi.

   a. Nella parte superiore o inferiore destra della dashboard di Console Home, scegli +Aggiungi widget.
   b. Scegli l'indicatore di trascinamento, rappresentato da sei punti verticali nella parte superiore sinistra della barra del titolo del widget, quindi trascinalo nella dashboard di Console Home.
4. Scegli l'applicazione Assess.
5. Per selezionare un ruolo IAM esistente che verrà utilizzato per accedere alle risorse nell'account corrente, seleziona Usa un ruolo IAM, quindi seleziona un ruolo IAM dall'elenco a discesa Seleziona un ruolo IAM.

   Se desideri utilizzare l'utente IAM corrente per scoprire le risorse dell'applicazione, scegli Usa le attuali autorizzazioni utente IAM e seleziona Capisco che devo configurare manualmente le autorizzazioni per abilitare la funzionalità richiesta AWS Resilience Hub nella sezione Use the current IAM user to discover application resources.
6. Scegli Assess.

   In alternativa, attiva la valutazione automatica giornaliera AWS Resilience Hub per consentire di valutare la tua applicazione ogni giorno senza costi aggiuntivi.

   AWS Resilience Hub esegue le seguenti azioni:

- Crea un'applicazione AWS Resilience Hub e rileva e mappa automaticamente le risorse associate.
- Crea e assegna una nuova politica di resilienza con valori predefiniti per Recovery Time Objective (RTO) e Recovery Point Objective (RPO). Cioè, quattro ore per RTO e un'ora per RPO. Dopo aver generato una valutazione, è possibile modificare la politica di resilienza o assegnare una politica diversa dalla console. AWS Resilience Hub Per ulteriori informazioni sull'aggiornamento della politica di resilienza e sull'associazione di una politica diversa, consulta Gestione delle politiche di resilienza.
- Valuta la resilienza dell'applicazione rispetto a RTO e RPO, monitora continuamente le risorse e le modifiche alla configurazione e pubblica i risultati.

> **Note**
>
> Prima di iniziare le valutazioni, è consigliabile valutare i potenziali costi associati all'esecuzione delle valutazioni utilizzando. AWS Resilience HubPer informazioni dettagliate sui prezzi, consulta la pagina relativa ai AWS Resilience Hub prezzi.

Per eseguire nuovamente una valutazione della resilienza per un'applicazione MyApplications esistente dal widget Resiliency

1. Accedi alla console di gestione.AWS
2. Espandi la barra laterale sinistra e scegli MyApplications.
3. Seleziona l'applicazione che desideri rivalutare.

   Come prerequisito, assicurati di aver aggiunto il widget Resilienza nella tua console. AWS Per aggiungere questo widget, completa i seguenti passaggi.

   a. Nella parte superiore o inferiore destra della dashboard di Console Home, scegli +Aggiungi widget.
   b. Scegli l'indicatore di trascinamento, rappresentato da sei punti verticali nella parte superiore sinistra della barra del titolo del widget, quindi trascinalo nella dashboard di Console Home.
4. Scegli Reassessment dal widget Resiliency.

   In alternativa, attiva la valutazione automatica giornaliera AWS Resilience Hub per consentire la valutazione quotidiana della tua applicazione senza costi aggiuntivi.

Revisione del riepilogo della valutazione nel widget Resiliency

Il widget Resiliency mostra un'istantanea dei risultati della valutazione che fornirà le informazioni più importanti e utilizzabili sulla resilienza dell'applicazione MyApplications, sulle potenziali vulnerabilità, sugli indicatori chiave di prestazione () e sulle azioni di miglioramento consigliate. KPIs Puoi saperne di più sulla posizione di resilienza dell'applicazione dalla valutazione più recente utilizzando quanto segue:

- Cronologia del punteggio di resilienza: questo grafico mostra l'andamento del punteggio di resilienza dell'applicazione per un massimo di un anno.
- Punteggio di resilienza: indica il punteggio di resilienza dell'applicazione valutato nella valutazione più recente. Questo punteggio riflette la precisione con cui l'applicazione segue i nostri consigli per soddisfare la politica di resilienza dell'applicazione e per implementare allarmi, procedure operative standard () ed esperimenti (SOPs). AWS Fault Injection Service AWS FIS Scegliete il numero per visualizzare informazioni aggiuntive nella sezione Punteggio di resilienza nella scheda Riepilogo della console. AWS Resilience Hub Per ulteriori informazioni, consulta Report di valutazione.
- Violazioni delle politiche: scegli il numero seguente per visualizzare tutti i componenti dell'applicazione (AppComponents) che violano le politiche allegate all'applicazione nel riquadro del rapporto di valutazione nella console. AWS Resilience Hub Per ulteriori informazioni, consulta Report di valutazione.
- Modifiche delle politiche: indica le politiche AppComponents che hanno rispettato la politica della valutazione precedente ma non sono state conformi nella valutazione corrente. Scegli il numero seguente per visualizzarlo AppComponents nel riquadro del rapporto di valutazione della console. AWS Resilience Hub Per ulteriori informazioni, consulta Report di valutazione.
- Derive delle risorse: scegli il numero seguente per visualizzare tutte le risorse derivanti dalla valutazione più recente nel riquadro del rapporto di valutazione nella console. AWS Resilience Hub Per ulteriori informazioni, consulta Report di valutazione.
- Vai a Resilience Hub: scegli questa opzione per aprire l'applicazione nella console. AWS Resilience Hub

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 della tua applicazione

cambiano, dovresti eseguire una valutazione della resilienza per assicurarti di disporre degli CloudWatch allarmi Amazon corretti per l'applicazione aggiornata.

Inoltre, AWS Resilience Hub ora rileva e integra automaticamente tutti gli CloudWatch allarmi Amazon già configurati nelle sue valutazioni della resilienza, fornendo una visione più completa dello stato di resilienza dell'applicazione. Questa nuova funzionalità combina AWS Resilience Hub le raccomandazioni con l'attuale configurazione di monitoraggio, semplificando la gestione degli allarmi e migliorando l'accuratezza della valutazione. Se hai implementato un CloudWatch allarme Amazon e AWS Resilience Hub non lo rileva automaticamente, puoi escludere l'allarme e selezionare il motivo come Già implementato. Per ulteriori informazioni sull'esclusione dei consigli, consultaInclusione o esclusione di raccomandazioni operative.

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 sulla base delle raccomandazioni operative
- Visualizzazione degli allarmi

Creazione di allarmi sulla base delle 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 un URL Amazon S3, 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: 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 in AWS Resilience Hub” 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 INSUFFICIENT_DATA in Amazon. CloudWatch Scegliendo il numero seguente, la tabella Allarmi verrà filtrata per visualizzare tutti gli allarmi implementati e inattivi.

- 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: l'ARN del 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 link alla cartella Allarmi.
4. Per copiare il percorso Amazon S3, seleziona la casella di controllo davanti al file JSON e scegli Copia URL.
5. 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.

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 l'URL di Amazon S3, 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.
- FIS in 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 INSUFFICIENT_DATA in Amazon. CloudWatch Scegli il numero seguente per visualizzare tutti gli allarmi implementati e inattivi nella scheda Consigli operativi.
   - Modello di origine: fornisce l'Amazon Resource Name (ARN) dello AWS CloudFormation stack che contiene i dettagli dell'allarme.
   - Risorsa: visualizza 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: 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 INSUFFICIENT_DATA in Amazon. CloudWatch Scegliendo il numero seguente, la tabella Allarmi verrà filtrata per visualizzare tutti gli allarmi implementati e inattivi.
- 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 vostre prestazioni SOPs in anticipo per garantire un ripristino tempestivo in caso di interruzione operativa.

In base ai componenti dell'applicazione, AWS Resilience Hub consiglia SOPs la preparazione. AWS Resilience Hub collabora con Systems Manager per automatizzare le fasi del processo SOPs fornendo una serie di documenti SSM che è possibile utilizzare come base per tali operazioni. SOPs

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
- Creazione di un documento SSM personalizzato
- Utilizzo di un documento SSM personalizzato anziché quello predefinito
- Test SOPs
- Visualizzazione delle procedure operative standard

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 i suggerimenti consigliati SOPs e includerli nella propria 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 in AWS Resilience Hub” 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 SOPs quelli implementati 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 SOPs

Come accennato in precedenza, è consigliabile aggiungere AWS FIS esperimenti alle pipeline CI/CD per testarle SOPs regolarmente; in questo modo si garantisce che siano pronti all'uso in caso di interruzione.

Prova sia quelli forniti che quelli personalizzati AWS Resilience Hub. SOPs

Visualizzazione delle procedure operative standard

Per visualizzare le applicazioni SOPs implementate

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 delle procedure operative standard implementate mostra l'elenco delle SOPs procedure operative generate dai consigli SOP.

   È possibile identificare i propri in SOPs 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 di riferimento.
- ID risorsa: identificatore della risorsa per la quale è implementata la raccomandazione SOP.

Per visualizzare le valutazioni consigliate SOPs

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 procedure consigliate SOPs 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 AWS Fault Injection Service esperimenti

Questa sezione descrive come gestire AWS Fault Injection Service (AWS FIS) gli esperimenti in AWS Resilience Hub. Si eseguono AWS FIS esperimenti per misurare la resilienza delle AWS risorse e la quantità di tempo necessaria per il ripristino in seguito a incidenti relativi a applicazioni, infrastrutture, zone di disponibilità e AWS regioni.

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 riprendersi dai 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 AWS FIS gli 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 AWS FIS alle azioni.

Puoi utilizzare gli AWS FIS esperimenti nel loro stato predefinito o personalizzarli in base alle tue esigenze. Per ulteriori informazioni sulla gestione AWS FIS degli esperimenti da AWS Resilience Hub console e AWS FIS console, consulta i seguenti argomenti:

- AWS Resilience Hub console
  - Visualizzazione degli esperimenti AWS FIS
    - Per visualizzare l'elenco degli AWS FIS esperimenti implementati dalle applicazioni
    - Per visualizzare gli AWS FIS esperimenti consigliati dalle valutazioni
  - the section called “ AWS FIS Esperimenti in corso”
  - the section called “AWS Fault Injection Service errori dell'esperimento/controllo dello stato”
- AWS FIS consolle
  - Gestire i tuoi AWS FIS esperimenti
  - Utilizzo della libreria di AWS FIS scenari
  - Gestione dei modelli di AWS FIS esperimento

Avvio, creazione ed esecuzione AWS FIS di esperimenti

AWS Resilience Hub semplifica AWS FIS gli esperimenti integrandosi con AWS FIS gli esperimenti. Fornisce consigli personalizzati e consente di avviare AWS FIS esperimenti con modelli precompilati mappati ai componenti dell'applicazione (AppComponents), consentendo test di resilienza efficienti.

Per avviare un esperimento da Raccomandazioni operative AWS FIS

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 in AWS Resilience Hub” e poi torna a questo passaggio.
6. Scegli la scheda Raccomandazioni operative.
7. Scegli la freccia destra prima degli esperimenti di Fault injection.

Questa sezione elenca tutti gli AWS FIS esperimenti consigliati dall'applicazione AWS Resilience Hub per testare lo stress e migliorarne la resilienza. In base all'implementazione, gli AWS FIS esperimenti sono classificati nei seguenti stati:

- Implementato: indica che gli esperimenti consigliati da AWS Resilience Hub sono implementati nell'applicazione. Scegliete il numero seguente per visualizzare tutti gli esperimenti implementati nella tabella Esperimenti.
- Implementato parzialmente: indica che gli esperimenti consigliati da AWS Resilience Hub sono parzialmente implementati nell'applicazione. Scegliete il numero seguente per visualizzare tutti gli esperimenti parzialmente implementati nella tabella Esperimenti.
- Non implementato: indica che gli esperimenti consigliati da non AWS Resilience Hub sono implementati nell'applicazione. Scegliete il numero seguente per visualizzare tutti gli esperimenti non implementati nella tabella Esperimenti.
- Esclusi: indica che gli esperimenti consigliati da AWS Resilience Hub sono esclusi dall'applicazione. Scegliete il numero seguente per visualizzare tutti gli esperimenti esclusi nella tabella Esperimenti. Per ulteriori informazioni sull'inclusione e l'esclusione degli esperimenti consigliati, consulta Inclusione o esclusione dei consigli operativi.

La tabella degli esperimenti elenca tutti gli AWS FIS esperimenti implementati che influiscono sul punteggio di resilienza dell'applicazione. È possibile identificare gli AWS FIS esperimenti utilizzando le seguenti informazioni:

- Nome dell'azione: indica l' AWS FIS azione consigliata per l'applicazione. Scegli il nome dell'azione per visualizzare tutte le azioni consigliate nella AppComponents pagina dei dettagli dell'AWS FIS esperimento. Quando lo Stato è impostato su Non tracciabile, indica che l' AWS FIS esperimento è uno scenario. Scegli il nome dello scenario per visualizzarne i dettagli nella pagina della libreria Scenario della AWS FIS console.
- Stato: indica lo stato di implementazione corrente dell' AWS FIS esperimento. Ovvero, implementato, parzialmente implementato, non implementato ed escluso.

> **Note**
>
> AWS FIS scenario è una funzionalità disponibile solo su console con più azioni predefinite. Quindi, AWS Resilience Hub non può tracciarlo e imposterà lo Stato su Non tracciabile.

- Descrizione: descrive l'obiettivo dell' AWS FIS azione.

8. Seleziona un' AWS FIS azione per la quale desideri avviare un esperimento.

   Nella sezione dedicata ai consigli sugli AWS FIS esperimenti, puoi saperne di più sugli esperimenti che devi implementare AppComponents utilizzando le seguenti informazioni:

   - Nome: nome del gruppo AppComponent in cui sono raggruppate le risorse.
   - Stato: indica lo stato di implementazione corrente dell' AWS FIS azione. Ovvero, implementato, parzialmente implementato, non implementato ed escluso.

     > **Note**
     >
     > AWS FIS scenario è una funzionalità disponibile solo su console con più azioni predefinite. Quindi, AWS Resilience Hub non può tracciarlo e imposterà lo Stato su Non tracciabile.

   - Selezione dell'obiettivo: indica in che modo le risorse verranno incluse nell'esperimento quando si sceglie Avvia esperimento. Se AWS Resilience Hub non determina automaticamente le risorse target, passa il mouse sul rispettivo campo di selezione Target per istruzioni su come aggiungerle.
   - Risorse: indica il numero di risorse raggruppate sotto. AppComponent Scegliete il numero per visualizzare queste risorse nella finestra di dialogo Risorse. È possibile identificare le risorse utilizzando quanto segue:
     - ID logico: indica l'ID logico della risorsa. Un ID logico è un nome utilizzato per identificare le risorse nel file di stato Terraform AWS CloudFormation, nell'applicazione MyApplications, nella AWS Resource Groups risorsa o nel cluster Amazon Elastic Kubernetes Service.
     - ID fisico: indica 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: indica la AWS regione in cui si trova la risorsa.

9. Selezionate una AppComponent e scegliete Includi o Escludi rispettivamente per includerla o escluderla AppComponent nell' AWS FIS esperimento.
10. Scegliete Inizia esperimento.

    AWS Resilience Hub ti reindirizzerà alla pagina dei dettagli di Specificare il modello nella AWS FIS console, aprendola in una nuova scheda.

11. Per creare un modello di esperimento, completa i passaggi in Per creare un modello di esperimento utilizzando la console.

    Inoltre, dopo aver inserito i dettagli del modello e aver scelto Avanti nella pagina Specificare i dettagli del modello della AWS FIS console seguendo i passaggi riportati in Per creare un modello di esperimento utilizzando la console, tenta AWS Resilience Hub automaticamente di mappare le azioni e gli obiettivi per i tipi di risorse nella pagina Azioni e obiettivi. Tuttavia, per migliorare la copertura, puoi aggiungere manualmente azioni e obiettivi scegliendo rispettivamente Aggiungi azione e Aggiungi obiettivo, e completare il resto della procedura per creare l'esperimento.

Esecuzione di AWS FIS esperimenti

Dopo aver creato un esperimento nella AWS FIS console, segui i passaggi in Avviare un esperimento da un modello per eseguire un esperimento nella AWS FIS console. Se desideri AWS Resilience Hub rilevare gli esperimenti più recenti in cui hai eseguito AWS FIS, devi eseguire una nuova valutazione. Per ulteriori informazioni sull'esecuzione delle valutazioni, vedereEsecuzione di valutazioni della resilienza in AWS Resilience Hub.

Visualizzazione degli esperimenti AWS FIS

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 l'elenco degli AWS FIS esperimenti attivi dalla dashboard, scegli Dashboard dal menu di navigazione a sinistra.

Nella tabella Esperimenti implementati, puoi identificare gli AWS FIS esperimenti utilizzando le seguenti informazioni:

- ID esperimento: identificatore dell' AWS FIS esperimento.
- Azione: indica l' AWS FIS azione associata all' AWS FIS esperimento. Inoltre, se è presente più di un'azione, evidenzia il numero di AWS FIS azioni associate all' AWS FIS esperimento. Puoi identificare i dettagli passandoci sopra con il mouse o navigando verso di essi.
- ID del modello di esperimento: identificatore del modello di AWS FIS esperimento utilizzato per creare l'esperimento. AWS FIS

Per visualizzare l'elenco degli AWS FIS esperimenti implementati dalle applicazioni

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 Esperimenti di iniezione in caso di errore.

   Nella tabella Esperimenti implementati, puoi identificare gli AWS FIS esperimenti implementati nella tua applicazione utilizzando le seguenti informazioni:

   - ID esperimento: identificatore dell' AWS FIS esperimento.
   - Azione: indica l' AWS FIS azione associata all' AWS FIS esperimento. Inoltre, se è presente più di un'azione, evidenzia il numero di AWS FIS azioni associate all' AWS FIS esperimento. Puoi identificare i dettagli passandoci sopra con il mouse o navigando verso di essi.
   - ID del modello di esperimento: identificatore del modello di AWS FIS esperimento utilizzato per creare l'esperimento. AWS FIS

Per visualizzare gli AWS FIS 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 Valutazioni, 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.
   - Resilienza: indica se l'applicazione si è allontanata dagli obiettivi RTO e RPO definiti nella politica di resilienza allegata o meno rispetto alla precedente valutazione riuscita.
   - Versione dell'app: versione dell'applicazione che è stata valutata.
   - 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 Valutazioni.
5. Scegli Raccomandazioni operative.
6. Scegli la freccia destra prima degli esperimenti di Fault injection.

   Questa sezione elenca tutti gli AWS FIS esperimenti consigliati dall'applicazione AWS Resilience Hub per testare lo stress e migliorarne la resilienza. In base all'implementazione, gli AWS FIS esperimenti sono classificati nei seguenti stati:

   - Implementato: indica che gli esperimenti consigliati da AWS Resilience Hub sono implementati nell'applicazione. Scegliete il numero seguente per visualizzare tutti gli esperimenti implementati nella tabella Esperimenti.
   - Implementato parzialmente: indica che gli esperimenti consigliati da AWS Resilience Hub sono parzialmente implementati nell'applicazione. Scegliete il numero seguente per visualizzare tutti gli esperimenti parzialmente implementati nella tabella Esperimenti.
   - Non implementato: indica che gli esperimenti consigliati da non AWS Resilience Hub sono implementati nell'applicazione. Scegliete il numero seguente per visualizzare tutti gli esperimenti non implementati nella tabella Esperimenti.
   - Esclusi: indica che gli esperimenti consigliati da AWS Resilience Hub sono esclusi dall'applicazione. Scegliete il numero seguente per visualizzare tutti gli esperimenti esclusi nella tabella Esperimenti. Per ulteriori informazioni sull'inclusione e l'esclusione degli esperimenti consigliati, consulta Inclusione o esclusione dei consigli operativi.

   La tabella degli esperimenti elenca tutti gli AWS FIS esperimenti implementati che influiscono sul punteggio di resilienza dell'applicazione. È possibile identificare gli AWS FIS esperimenti utilizzando le seguenti informazioni:

   - Nome dell'azione: indica l' AWS FIS azione consigliata per l'applicazione. Quando lo Stato è impostato su Non tracciabile, indica che l' AWS FIS esperimento è uno scenario. Scegli il nome dello scenario per visualizzarne i dettagli nella pagina della libreria Scenario della AWS FIS console.
   - Stato: indica lo stato di implementazione corrente dell' AWS FIS esperimento. Ovvero, implementato, parzialmente implementato, non implementato ed escluso.

> **Note**
>
> AWS FIS scenario è una funzionalità disponibile solo su console con più azioni predefinite. Quindi, AWS Resilience Hub non può tracciarlo e imposterà lo Stato su Non tracciabile.

- Descrizione: descrive l'obiettivo dell' AWS FIS azione.

AWS Fault Injection Service errori dell'esperimento/controllo dello stato

AWS Resilience Hub consente di tenere traccia dello stato dell'esperimento avviato. Per ulteriori informazioni, consulta la Per visualizzare gli AWS FIS esperimenti consigliati dalle valutazioni procedura.

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 un SOP. Il test viene eseguito, attiva l'allarme e avvia la SOP associata. Se funzionano correttamente e se l'applicazione soddisfa la politica 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 delle raccomandazioni relative agli allarmi, alle SOP e ai test, consultathe section called “Inclusione o esclusione di raccomandazioni operative”.

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) that need to be fixed to resolve the breaches in your application's resiliency policy. Choose the value to view the RTO/RPOdettagli nel rapporto di valutazione dell'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:
     - Conformità RTO/RPO: 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 le stime RTO/RPO 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.

- SOPs implementato: 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.
- Esperimenti FIS 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. Scegliete il valore accanto a RTO/RPO per visualizzare i dettagli nella scheda Raccomandazioni sulla resilienza del rapporto di valutazione dell'applicazione.
  - Raccomandazioni operative : indica le raccomandazioni operative che non sono state implementate o eseguite 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 AppComponents e tipi di interruzione” la sezione.

Alcuni componenti del punteggio possono essere ottenuti solo tramite l'API. `ScoringComponentResiliencyScore` Per ulteriori informazioni sull'API, consulta 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.	`T = ((Total number of tests implemented) + (Total number of tests excluded)) / (Total number of tests recommended)`	Se hai implementato 10 test ed escluso 5 test su 20 test AWS Resilience Hub consigliati, la copertura dei test viene calcolata come segue:

Componente di punteggio	Descrizione	Formula	Esempio
	Note Per calcolare il punteggio di resilienza, i test consigliati devono essere stati eseguiti con successo negli ultimi 30 giorni perché sia considerato AWS Resilience Hub implementato.	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 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.	`T = (10 + 5) / 20` Cioè, `T = .75 or 75 points`

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
Copertura SOP () 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 consigliati SOPs, la copertura SOP viene calcolata come segue: `S = (10 + 5) / 20` Cioè, `S = .75 or 75 points`

Componente di punteggio	Descrizione	Formula	Esempio

Conformità RTO/RPO () 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 obiettivi RTO e RPO regionali, P viene calcolato come segue:
			`P = (20 + 30)/ 100`
			Cioè, `P = .5 or 50 points`
			• Se non sono stati impostati obiettivi RTO e RPO 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, puoi ottenere il punteggio di resilienza AppComponents e i tipi di interruzione solo tramite il seguente AWS Resilience Hub: 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 test SOPs, 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 RTO o RPO regionali per la tua polizza, 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, SOPs ai test e agli obiettivi della politica

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 formato JSON 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."
      }
    }
  }
}
```

Modifica del modello AWS CloudFormation

Il modo più semplice per integrare un allarme, una SOP o una AWS FIS risorsa nell'applicazione principale consiste semplicemente nell'aggiungerlo come altra risorsa nel modello che descrive il modello di applicazione. Il file in formato JSON 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\"]}"
```

al seguente:

```
"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 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”

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 l'`CreateApp`API e fornire un nome di applicazione univoco. Per ulteriori informazioni sull'API, consulta https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_CreateApp.html.

L'esempio seguente mostra come creare una nuova applicazione `newApp` AWS Resilience Hub utilizzando l'`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 l'API. `CreateResiliencyPolicy` Per ulteriori informazioni sull'API, consulta https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_CreateResiliencyPolicy.html.

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

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`— Questa API consente di importare risorse nella versione bozza dell'applicazione da diverse fonti di input. Per ulteriori informazioni sull'API, consulta https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_ImportResourcesToDraftAppVersion.html.
- `PublishAppVersion`— Questa API pubblica una nuova versione dell'applicazione insieme a quella aggiornata AppComponents. Per ulteriori informazioni sull'API, consulta https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_PublishAppVersion.html.
- `DescribeDraftAppVersionResourcesImportStatus`— Questa API consente di monitorare lo stato di importazione delle risorse in una versione dell'applicazione. Per ulteriori

informazioni sull'API, consulta https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_DescribeDraftAppVersionResourcesImportStatus.html.

L'esempio seguente mostra come importare risorse nell'applicazione AWS Resilience Hub utilizzando l'`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 AWS Resilience Hub utilizzando l'`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 AWS Resilience Hub utilizzando l'`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 pubblicare la 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, utilizza `PublishAppVersion` l'API. Per ulteriori informazioni sull'API, consulta https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_PublishAppVersion.html.

   L'esempio seguente mostra come pubblicare la bozza dell'applicazione AWS Resilience Hub utilizzando l'`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 l'`UpdateApp`API. Per ulteriori informazioni sull'API, consulta https://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 AWS Resilience Hub utilizzando `UpdateApp` l'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"
    }
}
```

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 l'RTO del carico di lavoro stimato e l'RPO stimato definiti nella politica di resilienza. La valutazione confronta la configurazione di ogni componente applicativo con la policy e fornisce raccomandazioni in materia di allarmi, SOP e test.

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 resilienza AWS Resilience Hub

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

- `StartAppAssessment`— Questa API crea una nuova valutazione per un'applicazione. Per ulteriori informazioni sull'API, consulta https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_StartAppAssessment.html.
- `DescribeAppAssessment`— Questa API descrive una valutazione per l'applicazione e fornisce lo stato di completamento della valutazione. Per ulteriori informazioni sull'API, consulta https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_DescribeAppAssessment.html.

L'esempio seguente mostra come iniziare a eseguire una nuova valutazione AWS Resilience Hub utilizzando l'`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 AWS Resilience Hub utilizzando l'`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 segue APIs.

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

> **Note**
>
> Per ottenere i consigli sui test SOP e FIS, usa e. `ListSopRecommendations` `ListTestRecommendations` APIs

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

> **Note**
>
> Per ottenere i consigli sui test SOP e FIS, sostituiscili con o. `ListSopRecommendations` `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 l'`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"
                }
```

```
            ]
        }
    ]
}
```

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 l'`CreateAppVersionResource`API. Per ulteriori informazioni sull'API, consulta https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_CreateAppVersionResource.html.

È necessario fornire i seguenti parametri a questa API:

- 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 AWS Resilience Hub utilizzando l'`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 risorse APIs.

- `UpdateAppVersionResource`— Questa API aggiorna i dettagli delle risorse di un'applicazione. Per ulteriori informazioni sull'API, consulta UpdateAppVersionResource.
- `DeleteAppVersionAppComponent`— Questa API elimina il file AppComponent dall'applicazione. Per ulteriori informazioni sull'API, consulta DeleteAppVersionAppComponent.

L'esempio seguente mostra come aggiornare i dettagli delle risorse dell'applicazione AWS Resilience Hub utilizzando l'`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 il vuoto AppComponent creato negli esempi precedenti di AWS Resilience Hub utilizzo dell'`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 l'`UpdateAppVersionResource`API. Queste risorse non verranno prese in considerazione durante il calcolo della resilienza dell'applicazione. Per ulteriori informazioni sull'API, consulta https://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 AWS Resilience Hub utilizzando l'`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 ulteriori informazioni sui programmi di conformità applicabili AWS Resilience Hub, consulta AWS Servizi 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
- Identity and Access Management per AWS Resilience Hub
- Sicurezza dell'infrastruttura in AWS Resilience Hub

Protezione dei dati in AWS Resilience Hub

Il modello di responsabilità AWS condivisa modello di 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 Servizi AWS utilizzati. Per ulteriori informazioni sulla privacy dei dati, vedi le Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al Modello di responsabilità condivisa AWS e GDPR nel Blog sulla sicurezza AWS .

Ai fini della protezione dei dati, consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center or 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.
- Usa SSL/TLS per comunicare con le risorse. AWS È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con. AWS CloudTrail Per informazioni sull'utilizzo dei CloudTrail percorsi per acquisire AWS le attività, consulta Lavorare con i CloudTrail percorsi nella Guida per l'AWS CloudTrail utente.
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- 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 moduli crittografici convalidati FIPS 140-3 per accedere AWS tramite un'interfaccia a riga di comando o un'API, usa un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-3.

Ti consigliamo 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 Servizi AWS utilizzando la console, l'API o. AWS CLI 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. Quando fornisci un URL a un server esterno, ti suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta al server.

Crittografia dei dati 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 Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle risorse. AWS Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare AWS le risorse di Resilience Hub. IAM è uno strumento Servizio AWS che puoi utilizzare senza costi aggiuntivi.

Argomenti

- Destinatari
- Autenticazione con identità
- Gestione dell'accesso con policy
- Come funziona AWS Resilience Hub con IAM
- Configura i ruoli e le autorizzazioni IAM
- Risoluzione dei problemi relativi all'identità e all'accesso a AWS Resilience Hub
- AWS Resilience Hub riferimento alle autorizzazioni di accesso
- AWS politiche gestite per AWS Resilience Hub
- AWS Resilience Hub riferimenti alle persone e alle autorizzazioni IAM
- Importazione del file di stato Terraform in AWS Resilience Hub
- Abilitazione AWS Resilience Hub dell'accesso al tuo cluster Amazon Elastic Kubernetes Service
- Attivazione AWS Resilience Hub della pubblicazione su Amazon Simple Notification Service di argomenti

- Limitazione delle autorizzazioni per includere o escludere i consigli AWS Resilience Hub

Destinatari

Il modo in cui utilizzi 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. Devi inviare le richieste all'amministratore IAM per cambiare le autorizzazioni degli utenti del servizio. Esamina le informazioni contenute in questa pagina per comprendere i concetti di base relativi a IAM. Per saperne di più su come la tua azienda può utilizzare IAM con AWS Resilience Hub, consulta. Come funziona AWS Resilience Hub con IAM

Amministratore IAM: se sei un amministratore IAM, potresti voler conoscere i dettagli su come scrivere policy per gestire l'accesso a AWS Resilience Hub. Per visualizzare esempi di policy basate sull'identità di AWS Resilience Hub che puoi utilizzare in IAM, consulta. 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. Devi essere autenticato (aver effettuato l' Utente root dell'account AWS accesso AWS) come utente IAM o assumendo un ruolo IAM.

Puoi accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAM Identity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Quando accedi AWS utilizzando la federazione, assumi 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 (CLI) per firmare crittograficamente le tue richieste utilizzando le tue credenziali. Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sul metodo consigliato per la firma delle richieste, consulta Signature Version 4 AWS per le richieste API nella Guida per l'utente IAM.

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'utente di AWS IAM Identity Center e Utilizzo dell'autenticazione a più fattori (MFA)AWS in IAM nella Guida per l'utente IAM.

Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte Servizi AWS 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 un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione Attività che richiedono le credenziali dell'utente root nella Guida per l'utente IAM.

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 Servizi AWS 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 Servizi AWS 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 ulteriori informazioni su IAM Identity Center, consulta Cos'è IAM Identity Center? nella Guida per l'utente di AWS IAM Identity Center .

Utenti e gruppi IAM

Un utente IAM è un'identità interna Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le chiavi di accesso. Tuttavia, se si hanno casi d'uso specifici che richiedono credenziali a lungo termine con utenti IAM, si consiglia di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente IAM.

Un gruppo IAM 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 amministrare le risorse IAM.

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 Casi d'uso per utenti IAM nella Guida per l'utente IAM.

Ruoli IAM

Un ruolo IAM è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. Per assumere temporaneamente un ruolo IAM in AWS Management Console, puoi passare da un ruolo utente a un ruolo IAM (console). Puoi assumere un ruolo chiamando un'operazione AWS CLI o AWS API o utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta Utilizzo di ruoli IAM nella Guida per l'utente IAM.

I ruoli IAM 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 ulteriori informazioni sulla federazione dei ruoli, consulta Create a role for a third-party identity provider (federation) nella Guida per l'utente IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .

- Autorizzazioni utente IAM temporanee: un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso multi-account: è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per informazioni sulle differenze tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.
- Accesso a più servizi: alcuni Servizi AWS utilizzano le funzionalità di altri Servizi AWS. 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 inoltrato (FAS): quando utilizzi un utente o un ruolo IAM 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. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, combinate con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le operazioni. Per i dettagli delle policy relative alle richieste FAS, consulta Forward access sessions.
  - Ruolo di servizio: un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Create a role to delegate permissions to an Servizio AWS nella Guida per l'utente IAM.
  - Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS 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 amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un' EC2 istanza e che AWS CLI effettuano richieste AWS API. Questa soluzione è preferibile alla memorizzazione delle chiavi di accesso all'interno dell' EC2 istanza. Per assegnare un AWS ruolo a un' EC2 istanza 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' EC2 istanza di ottenere credenziali temporanee. Per ulteriori informazioni, consulta Utilizzare un ruolo IAM per concedere le autorizzazioni alle applicazioni in esecuzione su EC2 istanze Amazon nella IAM User Guide.

Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e collegandole 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 documenti JSON. Per ulteriori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente IAM.

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire operazioni 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 operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Le policy IAM definiscono le autorizzazioni relative a un'operazione, a prescindere dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'operazione `iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dall' AWS Management Console AWS CLI, dall'o dall' AWS API.

Policy basate sull'identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente 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 nel tuo Account AWS. Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scelta fra policy gestite e policy inline nella Guida per l'utente IAM.

Policy basate sulle risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Esempi di policy basate sulle risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket 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 operazioni 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. Servizi AWS

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

Liste 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. ACLs sono 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 informazioni ACLs, consulta la panoramica della lista di controllo degli accessi (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 delle autorizzazioni è una funzionalità avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a un'entità IAM (utente o ruolo 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 IAM nella Guida per l'utente IAM.
- Politiche di controllo del servizio (SCPs): SCPs sono politiche JSON 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 di proprietà dell' Account AWS 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. L'SCP limita le autorizzazioni per le entità presenti negli account dei membri, inclusa ciascuna di esse. Utente root dell'account AWS Per ulteriori informazioni su Organizations and SCPs, consulta le politiche di controllo dei servizi nella Guida AWS Organizations per l'utente.
- Politiche di controllo delle risorse (RCPs): RCPs sono politiche JSON che puoi utilizzare per impostare le autorizzazioni massime disponibili per le risorse nei tuoi account senza aggiornare le politiche IAM allegate a ciascuna risorsa di tua proprietà. L'RCP limita le autorizzazioni per le risorse negli account dei membri e può influire sulle autorizzazioni effettive per le identità, incluse le Utente root dell'account AWS, indipendentemente dal fatto che appartengano o meno all'organizzazione. Per ulteriori informazioni su Organizations e RCPs, incluso un elenco di Servizi AWS tale supporto RCPs, vedere Resource control policies (RCPs) nella Guida per l'AWS Organizations 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 Policy di sessione nella Guida per l'utente IAM.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire o meno una richiesta quando sono coinvolti più tipi di policy, consulta la logica di valutazione delle policy nella IAM User Guide.

Come funziona AWS Resilience Hub con IAM

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

Funzionalità IAM che puoi utilizzare con AWS Resilience Hub

Funzionalità IAM	AWS Supporto per 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 policy)	Parziale
Credenziali temporanee	Sì
Inoltro delle sessioni di accesso (FAS)	Sì
Ruoli di servizio	Sì

Per avere una visione di alto livello di come AWS Resilience Hub e altri AWS servizi funzionano con la maggior parte delle funzionalità IAM, consulta AWS i servizi che funzionano con IAM nella IAM User Guide.

Politiche basate sull'identità per Resilience Hub AWS

Supporta le policy basate su identità: sì

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente IAM.

Con le policy basate su identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. 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 informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta Guida di riferimento agli elementi delle policy JSON IAM nella Guida per l'utente di IAM.

Esempi di politiche 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 policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Esempi di policy basate sulle risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket 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 operazioni 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. Servizi AWS

Per consentire l'accesso multi-account, puoi specificare un intero account o entità IAM in un altro account come principale in una policy 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 amministratore IAM dell'account affidabile

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 Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Azioni politiche per AWS Resilience Hub

Supporta le operazioni di policy: si

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

L'elemento `Action`di una policy JSON descrive le operazioni che è possibile utilizzare per consentire o negare l'accesso a un criterio. Le azioni politiche in genere hanno lo stesso nome dell'operazione AWS API associata. Ci sono alcune eccezioni, ad esempio le operazioni di sola autorizzazione che non hanno un'operazione API corrispondente. 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 le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento JSON `Resource`della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Le istruzioni devono includere un elemento `Resource`o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). È possibile eseguire questa operazione per operazioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le operazioni 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 relativi ARNs, consulta Resources defined by AWS Resilience Hub nel Service Authorization Reference. Per sapere con quali azioni è possibile specificare l'ARN di ciascuna risorsa, vedere 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 le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire operazioni 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. È possibile 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.

È possibile anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, è possibile autorizzare un utente IAM ad accedere a una risorsa solo se è stata taggata con il relativo nome utente IAM. Per ulteriori informazioni, consulta Elementi delle policy IAM: variabili e tag nella Guida per l'utente di IAM.

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'utente IAM.

Per visualizzare un elenco delle chiavi di condizione di AWS Resilience Hub, consulta Condition keys for AWS Resilience Hub nel Service Authorization 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

Supporti ACLs: 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. ACLs sono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy JSON.

ABAC con Resilience Hub AWS

Supporta ABAC (tag nelle policy): parzialmente

Il controllo dell'accesso basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, questi attributi sono chiamati tag. Puoi allegare tag a entità IAM (utenti o ruoli) e a molte AWS risorse. L'assegnazione di tag alle entità e alle risorse è il primo passaggio di ABAC. In seguito, vengono progettate policy ABAC per consentire operazioni quando il tag dell'entità principale corrisponde al tag sulla risorsa a cui si sta provando ad accedere.

La strategia ABAC è utile in ambienti soggetti a una rapida crescita e aiuta in situazioni in cui la gestione delle policy diventa impegnativa.

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 su ABAC, consulta Definizione delle autorizzazioni con autorizzazione ABAC nella Guida per l'utente IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta Utilizzo del controllo degli accessi basato su attributi (ABAC) nella Guida per l'utente di IAM.

Utilizzo di credenziali temporanee con AWS Resilience Hub

Supporta le credenziali temporanee: sì

Alcune Servizi AWS non funzionano quando accedi utilizzando credenziali temporanee. Per ulteriori informazioni, incluse quelle che Servizi AWS funzionano con credenziali temporanee, consulta la sezione relativa alla Servizi AWS compatibilità con IAM nella IAM User Guide.

Stai utilizzando credenziali temporanee se accedi AWS Management Console utilizzando qualsiasi metodo tranne nome utente e 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 sullo scambio dei ruoli, consulta Passaggio da un ruolo utente a un ruolo IAM (console) nella Guida per l'utente IAM.

È possibile creare manualmente credenziali temporanee utilizzando l'API or. AWS CLI AWS 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, consulta Credenziali di sicurezza provvisorie in IAM.

Sessioni di accesso diretto per Resilience Hub AWS

Supporta l'inoltro delle sessioni di accesso (FAS): sì

Quando utilizzi un utente o un ruolo IAM 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. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS,

in combinazione con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le operazioni. Per i dettagli delle policy relative alle richieste FAS, consulta Forward access sessions.

Ruoli di servizio per AWS Resilience Hub

Supporta i ruoli di servizio: sì

Un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Create a role to delegate permissions to an Servizio AWS nella Guida per l'utente IAM.

> **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 l' AWS API. Per concedere agli utenti l'autorizzazione a eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta Creazione di policy IAM (console) nella Guida per l'utente IAM.

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

Argomenti

- Best practice per le policy
- Utilizzo della console Resilience AWS 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 operazioni 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 Policy gestite da AWSo Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente IAM.
- Applica le autorizzazioni con privilegio minimo: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. È possibile 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 di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso a operazioni e risorse è possibile aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente IAM.

- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano alla sintassi della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta Convalida delle policy per il Sistema di analisi degli accessi IAM nella Guida per l'utente IAM.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta Protezione dell'accesso API con MFA nella Guida per l'utente IAM.

Per maggiori informazioni sulle best practice in IAM, consulta Best practice di sicurezza in IAM nella Guida per l'utente di IAM.

Utilizzo della console Resilience AWS 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 AWS CLI o l'API. AWS Al contrario, concedi l'accesso solo alle operazioni che corrispondono all'operazione API 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 Aggiunta di 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 in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono cpllegate alla relativa identità utente. Questa politica include le autorizzazioni per completare questa azione sulla console o utilizzando l'API o a livello di codice. AWS CLI AWS

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

```
            "Resource": "*"
        }
    ]
}
```

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/*" }
      }
    }
  ]
}
```

Configura i ruoli e le autorizzazioni IAM

AWS Resilience Hub ti consente di configurare i ruoli IAM che desideri utilizzare durante l'esecuzione delle valutazioni per la tua 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 “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 utente IAM corrente: AWS Resilience Hub utilizzerà l'utente IAM corrente per accedere alle risorse dell'applicazione. Quando le tue risorse si trovano in un account diverso, AWS Resilience Hub assumerà i seguenti ruoli IAM 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 più 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 sei autorizzato a eseguire un'operazione, le tue policy devono essere aggiornate per poter eseguire l'operazione.

L'errore di esempio seguente si verifica quando l'utente IAM `mateojackson` prova a utilizzare la console per visualizzare i dettagli relativi a una risorsa *`my-example-widget`* fittizia ma non dispone di autorizzazioni `resiliencehub:`*`GetWidget`* fittizie.

```
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 aiuto, contatta il tuo AWS amministratore. 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 Servizi AWS 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.

Il seguente errore di esempio si verifica quando un utente IAM 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 scoprire come fornire l'accesso alle tue risorse su tutto Account AWS ciò che possiedi, consulta Fornire l'accesso a un utente IAM in un altro Account AWS di tua proprietà nella IAM User Guide.

- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a soggetti Account AWS di proprietà di terze parti nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (Federazione delle identità) nella Guida per l'utente IAM.
- Per informazioni sulle differenze di utilizzo tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente 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 policy IAM applicabili a utenti, gruppi o ruoli.

Ogni AWS Resilience Hub applicazione può essere configurata per utilizzare the section called "Ruolo invoker" (un ruolo IAM) o utilizzare le attuali autorizzazioni utente IAM (insieme a una serie di ruoli predefiniti per la valutazione pianificata e tra più account). In questo ruolo, puoi allegare una policy che definisce le autorizzazioni richieste AWS Resilience Hub per accedere ad altre AWS risorse o risorse applicative. 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.

> **Note**
>
> Se definisci gli endpoint VPC per le tue risorse di carico di lavoro, assicurati che le policy degli endpoint VPC forniscano l'accesso in sola lettura per l'accesso alle risorse. AWS Resilience Hub Per ulteriori informazioni, consulta Controllare l'accesso agli endpoint VPC utilizzando le policy degli endpoint.

Argomenti

- the section called “Utilizzo del ruolo IAM”
- the section called “Utilizzo delle attuali autorizzazioni utente IAM”

Utilizzo del ruolo IAM

AWS Resilience Hub utilizzerà un ruolo IAM esistente predefinito per accedere alle risorse nell'account primario 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 il permesso di accedere al tuo modello CFN 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 invoker nella console IAM”
- the section called “Gestione dei ruoli con l'API IAM”
- the section called “Definizione della politica di fiducia utilizzando il file JSON”

Creazione di un ruolo invoker nella console IAM

Per abilitare l'accesso AWS Resilience Hub a AWS servizi e risorse, devi creare un ruolo invoker nell'account principale utilizzando la console IAM. Per ulteriori informazioni sulla creazione di ruoli utilizzando la console IAM, consulta Creating a role for an AWS service (console).

Per creare un ruolo invoker nell'account principale utilizzando la console IAM

1. Aprire 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 attendibilità 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**
>
> Al momento della creazione o `iam:passRole` dell'aggiornamento dell'applicazione, è necessario disporre dell'autorizzazione dell'utente/ruolo IAM corrente per il ruolo invoker. Tuttavia, non è necessaria questa autorizzazione per eseguire una valutazione.

Gestione dei ruoli con l'API IAM

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 stringa JSON 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 utilizzando il file JSON

È possibile definire la politica di fiducia per il ruolo utilizzando un file JSON separato e quindi eseguire il `create-role` comando. Nell'esempio seguente, **`trust-policy.json`**è un file che contiene la politica di fiducia 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 del ruolo 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 console IAM per account secondari/di risorse”
- the section called “Gestione dei ruoli con l'API IAM”
- the section called “Definizione della politica di fiducia utilizzando il file JSON”

Creazione di un ruolo nella console IAM per account secondari/di risorse

Per consentire l'accesso AWS Resilience Hub ai AWS servizi e alle risorse in altri AWS account, devi creare ruoli in ciascuno di questi account.

Per creare un ruolo nella console IAM per gli account secondari/di risorsa utilizzando la console IAM

1. Aprire la console IAM all'indirizzo `https://console.aws.amazon.com/iam/`.
2. Dal pannello di navigazione, scegli Ruoli, quindi scegli Crea ruolo.
3. Seleziona Criteri di attendibilità 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 l'API IAM

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 stringa JSON 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"}]}'
```

Puoi inoltre definire la policy di attendibilità per il ruolo utilizzando un file JSON separato. Nell'esempio seguente, `trust-policy.json` è un file che si trova nella directory attuale.

Definizione della politica di fiducia utilizzando il file JSON

È possibile definire la politica di fiducia per il ruolo utilizzando un file JSON separato e quindi eseguire il `create-role` comando. Nell'esempio seguente, **`trust-policy.json`**è un file che contiene la politica di fiducia 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 attuali autorizzazioni utente IAM

Utilizza questo metodo se desideri utilizzare le tue attuali autorizzazioni utente IAM per creare ed eseguire una valutazione. Puoi allegare la policy `AWSResilienceHubAsssessmentExecutionPolicy` gestita al tuo utente IAM o a un ruolo associato al tuo utente.

Configurazione di un account singolo

L'utilizzo della policy gestita sopra menzionata è sufficiente per eseguire una valutazione su un'applicazione gestita nello stesso account dell'utente IAM.

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 policy di autorizzazione IAM 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 “Abilitazione AWS Resilience Hub dell'accesso al tuo cluster Amazon EKS”

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'utente/ruolo IAM 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 Servizio AWS viene lanciata una nuova o quando diventano disponibili nuove operazioni API per i servizi esistenti.

Per ulteriori informazioni, consulta Policy gestite da AWSnella Guida per l'utente di IAM.

AWSResilienceHubAsssessmentExecutionPolicy

Puoi collegarli `AWSResilienceHubAsssessmentExecutionPolicy` alle tue identità IAM. Durante l'esecuzione di una valutazione, questa policy 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 modelli SOP 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 chiamando l'API. `CreateRecommendationTemplate` 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 ElastiCache (Redis OSS) Serverless (ElastiCache (Redis OSS) Serverless): fornisce `Describe` le autorizzazioni per le configurazioni serverless ElastiCache (Redis OSS) associate al tuo account. AWS
- Amazon Elastic Compute Cloud (Amazon EC2): elenca e fornisce `Describe` le autorizzazioni per EC2 le risorse Amazon associate al tuo AWS account.

- Amazon Elastic Container Registry (Amazon ECR): fornisce `Describe` le autorizzazioni per le risorse Amazon ECR associate al tuo account. AWS
- Amazon Elastic Container Service (Amazon ECS) — Fornisce `Describe` le autorizzazioni per le risorse Amazon ECS associate al tuo account. AWS
- Amazon Elastic File System (Amazon EFS): fornisce `Describe` autorizzazioni per le risorse Amazon EFS associate al tuo AWS account.
- Amazon Elastic Kubernetes Service (Amazon EKS): elenca e `Describe` fornisce le autorizzazioni per le risorse Amazon EKS 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 le risorse SSM associate al tuo account. AWS
- AWS Fault Injection Service (AWS FIS) — Elenca e fornisce `Describe` le autorizzazioni per AWS FIS esperimenti e modelli di esperimenti associati al tuo account. AWS
- Amazon FSx for Windows File Server (Amazon FSx): elenca e fornisce `Describe` le autorizzazioni per FSx le risorse Amazon associate al tuo AWS account.
- Amazon RDS: elenca e fornisce `Describe` le autorizzazioni per le risorse Amazon RDS associate al tuo account. AWS
- 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 (Amazon SNS): elenca e `Describe` fornisce le autorizzazioni per le risorse Amazon SNS associate al tuo account. AWS
- Amazon Simple Queue Service (Amazon SQS): elenca e fornisce le autorizzazioni `Describe` per le risorse Amazon SQS associate al tuo account. AWS
- 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 policy IAM 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:DescribeServerlessCaches",
                "elasticahce:DescribeServerlessCacheSnapshots",
                "elasticache:DescribeSnapshots",
                "elasticfilesystem:DescribeFileSystems",
                "elasticfilesystem:DescribeLifecycleConfiguration",
                "elasticfilesystem:DescribeMountTargets",
                "elasticfilesystem:DescribeReplicationConfigurations",
                "elasticloadbalancing:DescribeListeners",
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticloadbalancing:DescribeTargetGroups",
                "elasticloadbalancing:DescribeTargetHealth",
                "fis:GetExperiment",
                "fis:GetExperimentTemplate",
                "fis:ListExperiments",
                "fis:ListExperimentResolvedTargets",
                "fis:ListExperimentTemplates",
                "fsx:DescribeFileSystems",
                "lambda:GetFunctionConcurrency",
                "lambda:GetFunctionConfiguration",
                "lambda:ListAliases",
                "lambda:ListEventSourceMappings",
                "lambda:ListFunctionEventInvokeConfigs",
                "lambda:ListVersionsByFunction",
```

```
                "rds:DescribeDBClusterSnapshots",
                "rds:DescribeDBClusters",
                "rds:DescribeDBInstanceAutomatedBackups",
                "rds:DescribeDBInstances",
                "rds:DescribeDBProxies",
                "rds:DescribeDBProxyTargets",
                "rds:DescribeDBSnapshots",
                "rds:DescribeGlobalClusters",
                "rds:ListTagsForResource",
                "resource-groups:GetGroup",
                "resource-groups:ListGroupResources",
                "route53-recovery-control-config:ListClusters",
                "route53-recovery-control-config:ListControlPanels",
                "route53-recovery-control-config:ListRoutingControls",
                "route53-recovery-readiness:GetReadinessCheckStatus",
                "route53-recovery-readiness:GetResourceSet",
                "route53-recovery-readiness:ListReadinessChecks",
                "route53:GetHealthCheck",
                "route53:ListHealthChecks",
                "route53:ListHostedZones",
                "route53:ListResourceRecordSets",
                "route53resolver:ListResolverEndpoints",
                "route53resolver:ListResolverEndpointIpAddresses",
                "s3:ListBucket",
                "servicecatalog:GetApplication",
                "servicecatalog:ListAssociatedResources",
                "sns:GetSubscriptionAttributes",
                "sns:GetTopicAttributes",
                "sns:ListSubscriptionsByTopic",
                "sqs:GetQueueAttributes",
                "sqs:GetQueueUrl",
                "ssm:DescribeAutomationExecutions",
                "states:DescribeStateMachine",
                "states:ListStateMachineVersions",
                "states:ListStateMachineAliases",
                "tag:GetResources"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AWSResilienceHubApiGatewayStatement",
            "Effect": "Allow",
            "Action": [
                "apigateway:GET"
```

```
            ],
            "Resource": [
                "arn:aws:apigateway:*::/apis/*",
                "arn:aws:apigateway:*::/restapis/*",
                "arn:aws:apigateway:*::/usageplans"
            ]
        },
        {
            "Sid": "AWSResilienceHubS3ArtifactStatement",
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:PutObject",
                "s3:GetObject"
            ],
            "Resource": "arn:aws:s3:::aws-resilience-hub-artifacts-*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
        },
        {
            "Sid": "AWSResilienceHubS3AccessStatement",
            "Effect": "Allow",
            "Action": [
                "s3:GetBucketLocation",
                "s3:GetBucketLogging",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketTagging",
                "s3:GetBucketVersioning",
                "s3:GetMultiRegionAccessPointRoutes",
                "s3:GetReplicationConfiguration",
                "s3:ListAllMyBuckets",
                "s3:ListMultiRegionAccessPoints"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
        },
```

```
        {
            "Sid": "AWSResilienceHubCloudWatchStatement",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": "ResilienceHub"
                }
            }
        },
        {
            "Sid": "AWSResilienceHubSSMStatement",
            "Effect": "Allow",
            "Action": [
                "ssm:GetParametersByPath"
            ],
            "Resource": "arn:aws:ssm:*:*:parameter/ResilienceHub/*"
        }
    ]
}
```

AWS Resilience Hub 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 feed RSS nella pagina della cronologia dei AWS Resilience Hub documenti.

Modifica	Descrizione	Data
AWSResilienceHubAssessmentExecutionPolicy— Modifica	AWS Resilience Hub ha aggiornato `AWSResilienceHubAsssessmentExecutionPolicy` la concessione `List` e `Get` le autorizzazioni per consentir	17 dicembre 2024

Modifica	Descrizione	Data
	e l'accesso agli esperimenti AWS FIS durante l'esecuzione delle valutazioni.	
AWSResilienceHubAssessmentExecutionPolicy— Modifica	AWS Resilience Hub è stato aggiornato `AWSResilienceHubAsssessmentExecutionPolicy` per concedere `Describe` le autorizzazioni per consentire l'accesso a risorse e configurazioni su Amazon ElastiCache (Redis OSS) Serverless durante l'esecuzione delle valutazioni.	25 settembre 2024
AWSResilienceHubAssessmentExecutionPolicy— Modifica	AWS Resilience Hub è stato aggiornato `AWSResilienceHubAsssessmentExecutionPolicy` per concedere `Describe` le autorizzazioni necessarie 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

Modifica	Descrizione	Data
AWSResilienceHubAssessmentExecutionPolicy— Cambia	AWS Resilience Hub l'ho 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— Modifica	AWS Resilience Hub aggiornato `AWSResilienceHubAsssessmentExecutionPolicy` per concedere `Describe` le autorizzazioni per consentire la lettura della AWS Step Functions configurazione durante l'esecuzione delle valutazioni.	30 ottobre 2023
AWSResilienceHubAssessmentExecutionPolicy— Modifica	AWS Resilience Hub l'ho aggiornato `AWSResilienceHubAsssessmentExecutionPolicy` per concedere `Describe` le autorizzazioni per consentirti di accedere alle risorse su Amazon RDS durante l'esecuzione delle valutazioni.	5 ottobre 2023

Modifica	Descrizione	Data
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 alle persone e alle autorizzazioni IAM

Puoi concedere le autorizzazioni IAM ai personaggi con cui è necessario lavorare AWS Resilience Hub utilizzando policy `AWSResilienceHubAsssessmentExecutionPolicy` AWS gestite e una delle seguenti policy specifiche per ogni persona. Per ulteriori informazioni sulla policy AWS gestita, consulta. the section called “AWSResilienceHubAsssessmentExecutionPolicy”

Politiche per i personaggi suggerite da AWS Resilience Hub:

- Autorizzazioni IAM per la persona del gestore delle applicazioni dell'infrastruttura
- Autorizzazioni IAM per la persona del responsabile della continuità operativa
- Autorizzazioni IAM per la persona del proprietario dell'applicazione
- Autorizzazioni IAM per la concessione dell'accesso in sola lettura

Autorizzazioni IAM per la persona del gestore delle applicazioni dell'infrastruttura

La seguente politica concede le autorizzazioni necessarie richieste per il personaggio del gestore delle applicazioni dell'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": "*"
    }
  ]
}
```

Autorizzazioni IAM per la persona del responsabile della continuità operativa

La seguente politica concede le autorizzazioni necessarie richieste per il ruolo 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": "*"
    }
  ]
}
```

Autorizzazioni IAM 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": "*"
    }
  ]
}
```

Autorizzazioni IAM per la concessione dell'accesso in sola lettura

La seguente policy 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 chiavi gestite (SSE-KMS). AWS Key Management Service 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 politiche IAM 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

La seguente policy sui bucket Amazon S3 e la policy IAM sono necessarie per consentire l'accesso in AWS Resilience Hub lettura ai file di stato Terraform situati 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 IAM AWS corrente 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 policy `AWSResilienceHubAsssessmentExecutionPolicy` gestita, l'`ListBucket`autorizzazione non è richiesta.

> **Note**
>
> Se i tuoi file di stato Terraform sono crittografati tramite KMS, 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 tramite KMS, 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 (Amazon EKS) analizzando l'infrastruttura del cluster Amazon EKS. AWS Resilience Hub utilizza la configurazione RBAC (role-based access control) 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 cluster Amazon EKS per l'analisi e la valutazione del carico di lavoro, devi completare quanto segue:

- Crea o usa un ruolo esistente AWS Identity and Access Management (IAM) nello stesso account del cluster Amazon EKS.
- Abilita l'accesso di utenti e ruoli IAM al tuo cluster Amazon EKS e concedi autorizzazioni di sola lettura aggiuntive alle risorse K8s all'interno del cluster Amazon EKS. Per ulteriori informazioni sull'abilitazione dell'accesso di utenti e ruoli IAM al tuo cluster Amazon EKS, consulta Abilitare l'accesso di utenti e ruoli IAM al tuo cluster - Amazon EKS.

L'accesso al tuo cluster Amazon EKS tramite entità IAM è abilitato da AWS IAM Authenticator for Kubernetes, che viene eseguito sul piano di controllo di Amazon EKS. L'Authenticator ottiene le informazioni di configurazione da. `aws-auth ConfigMap`

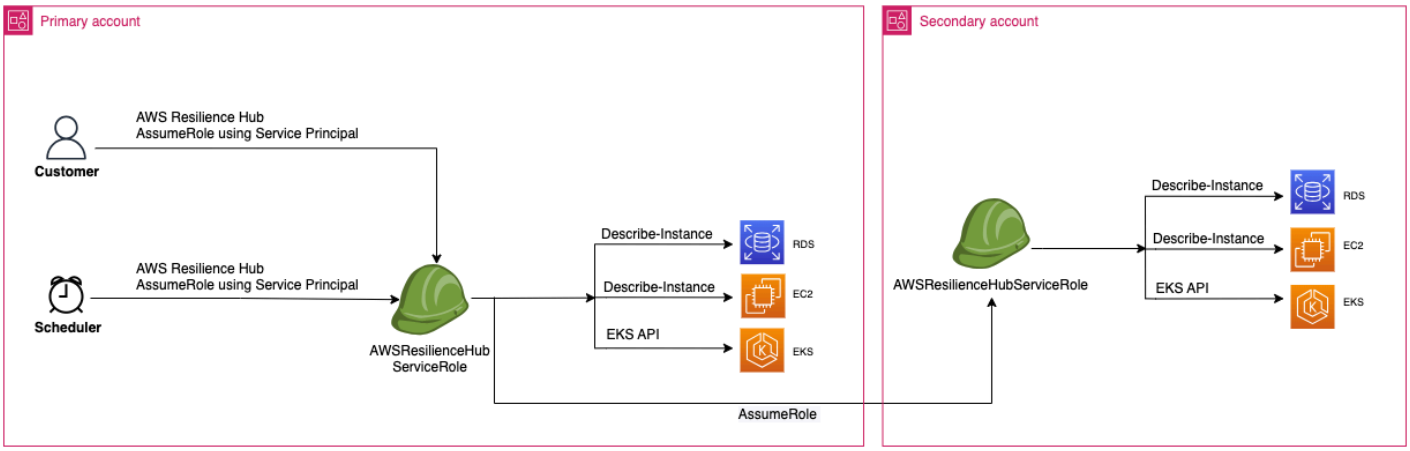
> **Note**
>
> - Per ulteriori informazioni su tutte le `aws-auth ConfigMap` impostazioni, consulta Full Configuration Format on. GitHub
> - Per ulteriori informazioni sulle diverse identità IAM, consulta Identità (utenti, gruppi e ruoli) nella Guida per l'utente IAM.
> - Per ulteriori informazioni sulla configurazione del controllo degli accessi basato sui ruoli (RBAC) di Kubernetes, consulta Using RBAC Authorization.

AWS Resilience Hub interroga le risorse all'interno del tuo cluster Amazon EKS utilizzando un ruolo IAM nel tuo account. Per accedere AWS Resilience Hub alle risorse all'interno del cluster Amazon EKS, il ruolo IAM utilizzato da AWS Resilience Hub deve essere mappato su un gruppo Kubernetes con autorizzazioni di sola lettura sufficienti per le risorse all'interno del cluster Amazon EKS.

AWS Resilience Hub consente di accedere alle risorse del cluster Amazon EKS utilizzando una delle seguenti opzioni di ruolo IAM:

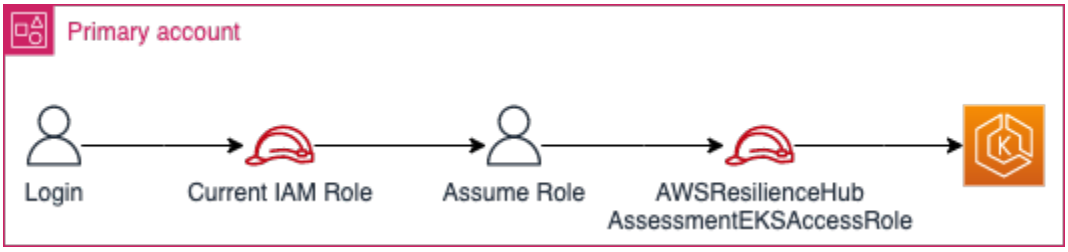
- Se l'applicazione è configurata per utilizzare l'accesso basato sui ruoli per accedere alle risorse, il ruolo invoker o il ruolo di account secondario assegnato AWS Resilience Hub durante la creazione di un'applicazione verrà utilizzato per accedere al cluster Amazon EKS durante la valutazione.

  Il seguente diagramma concettuale mostra come accedere AWS Resilience Hub ai cluster Amazon EKS quando l'applicazione è configurata come applicazione basata sui ruoli.

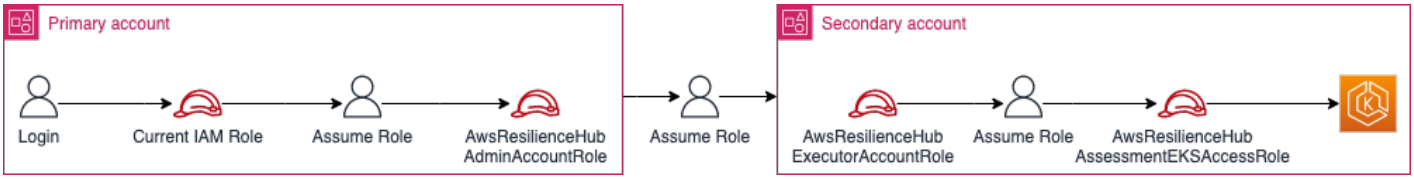


- Se la tua applicazione è configurata per utilizzare l'utente IAM corrente per accedere alle risorse, devi creare un nuovo ruolo IAM con il nome `AwsResilienceHubAssessmentEKSAccessRole` nello stesso account del cluster Amazon EKS. Questo ruolo IAM verrà quindi utilizzato per accedere al tuo cluster Amazon EKS.

  Il seguente diagramma concettuale mostra come AWS Resilience Hub accedere ai cluster Amazon EKS distribuiti nel tuo account principale quando l'applicazione è configurata per utilizzare le attuali autorizzazioni utente IAM.



  Il seguente diagramma concettuale mostra come AWS Resilience Hub accede ai cluster Amazon EKS distribuiti su un account secondario quando l'applicazione è configurata per utilizzare le attuali autorizzazioni utente IAM.



Concessione dell' AWS Resilience Hub accesso alle risorse nel cluster Amazon EKS

AWS Resilience Hub consente di accedere alle risorse situate nei cluster Amazon EKS a condizione che siano state configurate 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 ruolo IAM per accedere al cluster Amazon EKS.

   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 su come vengono AWS Resilience Hub utilizzati i ruoli IAM, consulta. the section called “Come funziona AWS Resilience Hub con IAM”

   Se hai configurato la tua applicazione utilizzando le attuali autorizzazioni utente `AwsResilienceHubAssessmentEKSAccessRole` IAM, devi creare il ruolo IAM nello stesso account del cluster Amazon EKS. Questo ruolo IAM verrà quindi utilizzato durante l'accesso al cluster Amazon EKS.

   Durante l'importazione e la valutazione dell'applicazione, AWS Resilience Hub utilizza un ruolo IAM per accedere alle risorse nel cluster Amazon EKS. Questo ruolo deve essere creato nello stesso account del cluster Amazon EKS e verrà mappato con un gruppo Kubernetes che include le autorizzazioni richieste per AWS Resilience Hub valutare il cluster Amazon EKS.

   Se il tuo cluster Amazon EKS si trova nello stesso account dell'account AWS Resilience Hub chiamante, il ruolo deve essere creato utilizzando la seguente policy di fiducia IAM. In questa policy di fiducia IAM, `caller_IAM_role` viene utilizzato nell'account corrente APIs per chiamare il AWS Resilience Hub.

   > **Note**
   >
   > `caller_IAM_role`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 cluster Amazon EKS si trova in un account incrociato (un account diverso dall'account AWS Resilience Hub chiamante), devi creare il ruolo `AwsResilienceHubAssessmentEKSAccessRole` IAM utilizzando la seguente politica di fiducia IAM:

> **Note**
>
> Come prerequisito, per accedere al cluster Amazon EKS 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

   Stai 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 cluster Amazon EKS, 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 cluster Amazon EKS.
      - `resilience-hub-eks-access-cluster-role-binding`(`ClusterRoleBinding`) — Definisce un gruppo denominato `resilience-hub-eks-access-group` nel cluster Amazon EKS 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 cluster Amazon EKS 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 cluster Amazon EKS per valutare la resilienza dell'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 mappare il `resilience-hub-eks-access-group` ruolo IAM utilizzato per accedere al cluster Amazon EKS.

   Questo passaggio crea una mappatura tra il ruolo IAM utilizzato nella fase 1 e il gruppo Kubernetes creato nella fase 2. Questa mappatura concede le autorizzazioni ai ruoli IAM per l'accesso alle risorse all'interno del cluster Amazon EKS.

   > **Note**
   >
   > - `ROLE-NAME`si riferisce al ruolo IAM utilizzato per accedere al cluster Amazon EKS.
   >   - 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'utente IAM corrente per accedere alle risorse, deve essere il. `AwsResilienceHubAssessmentEKSAccessRole`
   > - `ACCOUNT-ID`dovrebbe essere l'ID dell' AWS account del cluster Amazon EKS.

   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
```

- Puoi modificare manualmente `aws-auth ConfigMap` aggiungendo i dettagli del ruolo IAM alla `mapRoles ConfigMap` sezione dei dati sottostanti. Usa 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 ruolo IAM da aggiungere.
    - Sintassi ARN —. `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 ruolo IAM 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 AWS Resilience Hub abilitare la pubblicazione di notifiche sull'applicazione negli argomenti di Amazon Simple Notification Service (Amazon SNS). Per inviare notifiche push a un argomento di Amazon SNS, assicurati di disporre di quanto segue:

- Un' AWS Resilience Hub applicazione attiva.

- Un argomento Amazon SNS esistente a cui inviare AWS Resilience Hub notifiche. Per ulteriori informazioni sulla creazione di un argomento Amazon SNS, consulta Creazione di un argomento Amazon SNS.

AWS Resilience Hub Per abilitare la pubblicazione di notifiche sul tuo argomento Amazon SNS, devi aggiornare la politica di accesso dell'argomento Amazon SNS 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 pubblichi 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'argomento Amazon SNS. AWS Resilience Hub Modifica il valore del principale da `aresiliencehub.amazonaws.com`. `resiliencehub.<opt-in-region>.amazonaws.com`

Se stai utilizzando un argomento Amazon SNS Server Side Encrypted (SSE), devi assicurarti AWS Resilience Hub che disponga `Decrypt` dell'accesso `GenerateDataKey` e * alla chiave di crittografia Amazon SNS.

Per fornire `Decrypt` e `GenerateDataKey*` accedere a AWS Resilience Hub, devi includere le seguenti autorizzazioni per la politica di accesso. AWS Key Management Service

```
{
```

```
  "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. Puoi limitare le autorizzazioni per includere o escludere i consigli per applicazione utilizzando la seguente policy di fiducia IAM. In questa policy di fiducia IAM, `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 chiamate API AWS pubblicate per accedere AWS Resilience Hub attraverso la rete. I client devono supportare Transport Layer Security (TLS) 1.2 o versioni successive. È consigliabile TLS 1.3 o versioni successive. I client devono, inoltre, supportare le suite di crittografia con PFS (Perfect Forward Secrecy), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (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 i livelli di resilienza delle applicazioni non siano influenzati. Questi controlli stimano il Recovery Time Objective (RTO) e il Recovery Point Objective (RPO) rispetto ai valori definiti nella politica di resilienza per ogni 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 devi fornire le autorizzazioni IAM pertinenti per consentirgli di accedere alle AWS Resilience Hub tue risorse. Per ulteriori informazioni sulle autorizzazioni IAM richieste 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
- Gateway NAT
- Amazon Route 53
- Amazon Application Recovery Controller (ARC)

- File server Amazon FSx per Windows
- AWS Step Functions
- Amazon ElastiCache (sistema operativo Redis)

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.

Replica dei dati

AWS Resilience Hub verifica se è definita una replica dei dati Amazon EFS a livello regionale o interregionale per il file system distribuito. La replica dei dati di Amazon EFS aiuta a migliorare l'RTO stimato e l'RPO stimato 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 tua politica
- Istantanee manuali per sistemi di backup di terze parti

Failover tra regioni

AWS Resilience Hub verifica gli obiettivi RTO e RPO definiti nella politica di resilienza per riprendersi dalle perturbazioni regionali. Inoltre, è in AWS Resilience Hub grado di identificare le seguenti architetture interregionali per far fronte alle interruzioni regionali:

- Un backup locale con una copia di un'istantanea interregionale
- Una replica letta 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 verifica gli obiettivi RTO e RPO 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 AZ 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.

Point-in-time ripristino

AWS Resilience Hub verifica se point-in-time il ripristino (PITR) è richiesto dall'obiettivo RPO della politica di 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.

Replica dei dati

AWS Resilience Hub verifica se per il bucket Amazon S3 distribuito sono state definite Same Region Replication (SRR) e Cross Region Replication (CRR). La replica dei dati di Amazon S3 migliora l'RTO

stimato del carico di lavoro e l'RPO stimato del carico di lavoro 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 agli obiettivi RTO definiti nella tua politica di resilienza, AWS Resilience Hub verifica se Amazon S3 Replication Time Control (S3 RTC) deve essere abilitato o meno. Questa funzionalità fatturabile replica il 99,99% 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 tua politica
- 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.

Point-in-time recupero

AWS Resilience Hub verifica se è necessario point-in-time il ripristino (PITR) in base all'obiettivo RPO della politica di 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

AWS Resilience Hub verifica se la tabella Amazon DynamoDB distribuita è definita come tabella globale con una o più repliche in altre regioni. La configurazione di Global Table migliora l'RTO del carico di lavoro stimato e l'RPO del carico di lavoro stimato a livello di regione e offre anche la possibilità di lavorare in modalità attiva-attiva o attiva-passiva multiregione. AWS Backup oppure Amazon DynamoDB PITR può essere utilizzato in una delle regioni per gestire le interruzioni delle applicazioni.

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' EC2 istanza Amazon come istanza con stato se viene soddisfatto uno dei seguenti criteri:

- Se `DeleteOnTermination` l'attributo è impostato su false per almeno un volume Amazon Elastic Block Store (Amazon EBS) collegato a questa istanza.
- Se Amazon Data Lifecycle Manager o un AWS Backup piano sono collegati all' EC2 istanza 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' EC2 istanza 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 gruppi di Auto Scaling (ASG) con configurazione Multi-AZ. Se viene identificato un ASG esistente, ARH verificherà se è configurato su più zone di disponibilità. Se ASG viene definito anche utilizzando solo EC2 istanze Amazon spot, si consiglia di aumentarne la capacità con istanze Amazon on-demand per migliorare la resilienza quando EC2 le istanze Amazon spot non sono disponibili. EC2

EC2 Flotta 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 di resilienza specifici per Amazon EBS. Per ulteriori informazioni su Amazon EBS, consulta la documentazione di Amazon EBS.

Backup pianificato

AWS Resilience Hub verifica se uno o entrambi i seguenti elementi sono definiti per i tuoi volumi Amazon EBS.

- Una regola di backup per un volume Amazon EBS specifico collegato alla tua EC2 istanza Amazon.
- Una regola di backup per creare AMI supportate da Amazon EBS sulla tua istanza Amazon. EC2
- 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 volume Amazon EBS è considerato un volume con stato se viene soddisfatto uno dei seguenti criteri:

- Se `DeleteOnTermination` l'attributo è impostato su false per questo volume Amazon EBS.
- Se Amazon Data Lifecycle Manager o un AWS Backup piano è associato a questo volume Amazon EBS o all' EC2 istanza 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 le raccomandazioni 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 connessa al VPC. La connessione AWS Lambda a sottoreti in diversi Amazon VPC consente la resilienza AZs delle funzioni in caso di interruzione della zona di disponibilità.

Coda di lettere morte

AWS Resilience Hub verifica se a una AWS Lambda funzione è associata una coda di lettere morte (DLQ) per archiviare le richieste non riuscite. Il collegamento di un DLQ alla AWS Lambda funzione 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 Amazon EKS, consulta la documentazione di Amazon EKS.

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 cluster Amazon EKS aggiuntivo in un'altra regione se la politica di resilienza richiede una copertura in caso di interruzione regionale. Questo cluster Amazon EKS aggiuntivo è inoltre verificato per le implementazioni 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): l'utilizzo di 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 gestiti da Amazon EKS: questa sostituzione semplifica gli aggiornamenti delle immagini dei nodi di lavoro durante la manutenzione.
- Supporto di richieste dinamiche di CPU e 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 vivibilità 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 del cluster Amazon EKS di crescere e soddisfare le richieste di carico di lavoro.
- Configurazione di Horizontal Pod Autoscaler: questa configurazione aiuta il cluster Amazon EKS 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 per Amazon Simple Notification Service (Amazon SNS). Per ulteriori informazioni su Amazon SNS, consulta la documentazione di Amazon SNS.

Abbonamenti tematici

AWS Resilience Hub verifica se all'argomento Amazon SNS è associato almeno un abbonamento 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 (Amazon SQS). Per ulteriori informazioni su Amazon SQS, consulta la documentazione di Amazon SQS.

Coda di lettere morte

AWS Resilience Hub verifica se alla coda Amazon SQS è associato un DLQ 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 (Amazon ECS). Per ulteriori informazioni su Amazon ECS, consulta la documentazione di Amazon ECS.

Multi-AZ deployment (Implementazione Multi-AZ)

AWS Resilience Hub verifica se le attività o i servizi di Amazon ECS vengono eseguiti in più parti in AZs base ad Amazon EC2 o ai tipi di AWS Fargate avvio. È necessario un cluster Amazon ECS 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 parti. AZs

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 l'interruzione regionale, AWS Resilience Hub verificherà se è presente un'ulteriore distribuzione della risorsa API Amazon API Gateway in un'altra regione.

Implementazione di API private Multi-AZ

AWS Resilience Hub verifica se la tua API è definita come privata all'interno di Amazon API Gateway. Private APIs dovrebbe ricevere traffico tramite un endpoint di interfaccia Amazon VPC distribuito su più dispositivi. 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.

Gateway NAT

Questa sezione elenca tutti i controlli e i consigli specifici di NAT Gateway. Per ulteriori informazioni sui gateway NAT, vedere NAT Gateways.

Multi-AZ deployment (Implementazione Multi-AZ)

AWS Resilience Hub verifica se NAT Gateway è distribuito in più. AZs È necessaria un'ulteriore implementazione di NAT Gateway in una regione diversa se la politica richiede una copertura per le

interruzioni regionali. Il gateway NAT aggiuntivo, situato in una regione diversa, viene inoltre verificato per la sua implementazione in più aree. AZs

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 Application Recovery Controller (ARC)

Questa sezione elenca tutti i controlli e i consigli specifici di Amazon Application Recovery Controller (ARC) (ARC). Per ulteriori informazioni su ARC, consulta la documentazione di ARC.

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 controlli di preparazione all'ARC 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 file system, consulta Amazon EFS.

Backup del file system

AWS Resilience Hub controlla se AWS Backup è definito un file system per il file system 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 l'RTO stimato del carico di lavoro e l'RPO stimato del carico di lavoro a livello di infrastruttura, AZ e regione. Inoltre, potrebbe essere combinato con un'operazione In-Region 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.

Distribuzione tra 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.

Amazon ElastiCache (sistema operativo Redis)

Questa sezione elenca tutti i controlli e i consigli specifici di Amazon ElastiCache (Redis OSS).

Per ulteriori informazioni su Amazon ElastiCache (Redis OSS), consulta la ElastiCache documentazione di Amazon.

Implementazione Single-AZ

AWS Resilience Hub verifica se il cluster Amazon ElastiCache (Redis OSS) è distribuito come nodo singolo o con tutti i suoi nodi in un'unica zona di disponibilità.

Implementazione Single-AZ

AWS Resilience Hub verifica se il cluster Amazon ElastiCache (Redis OSS) è distribuito come gruppo di replica (sia per i cluster abilitati alla modalità cluster che per quelli con modalità cluster disabilitata) su più zone di disponibilità per consentire il failover in caso di interruzione della zona di disponibilità.

Failover tra regioni

AWS Resilience Hub verifica gli obiettivi RTO e RPO definiti nella politica di resilienza per riprendersi da un'interruzione regionale. Inoltre, è in AWS Resilience Hub grado di identificare i cluster di datastore globali di Amazon ElastiCache (Redis OSS) distribuiti in più regioni.

Backup

AWS Resilience Hub verifica se le seguenti funzionalità di backup sono applicate su un Amazon ElastiCache (Redis OSS) distribuito o su un cluster progettato autonomamente:

- Backup automatico
- Backup manuale per sistemi di backup di terze parti

AWS Resilience Hub non consiglierà il backup come metodo di ripristino se non si utilizza il backup. Tuttavia, è possibile ripristinare il livello di cache in caso di incoerenza dei dati e ricreare i dati dallo storage principale.

Failover più rapido a livello regionale

AWS Resilience Hub verifica gli obiettivi RTO e RPO definiti nella politica di resilienza durante le interruzioni dell'infrastruttura o della zona di disponibilità. Inoltre, è in AWS Resilience Hub grado di identificare le seguenti architetture regionali per il ripristino in caso di interruzioni dell'infrastruttura e della zona di disponibilità:

- Istanza del nodo di standby secondario in una zona di disponibilità diversa per il tipo di cluster Amazon ElastiCache (Redis OSS) disattivato in modalità cluster.

- Istanza del nodo di standby secondario in una zona di disponibilità diversa per ogni shard per il tipo di cluster Amazon ElastiCache (Redis OSS) abilitato alla modalità cluster.

Utilizzo di altri servizi

Questa sezione descrive AWS i servizi che interagiscono con AWS Resilience Hub.

Argomenti

- AWS CloudFormation
- AWS CloudTrail
- AWS Systems Manager
- AWS Trusted Advisor

AWS CloudFormation

AWS Resilience Hub è integrato con AWS CloudFormation, un servizio che consente di modellare e configurare le AWS risorse in modo da dedicare meno tempo alla creazione e alla gestione delle risorse e dell'infrastruttura. È necessario creare un modello che descrive tutte le AWS risorse desiderate (ad esempio AWS::ResilienceHub:::ResiliencyPolicy and AWS::ResilienceHub:::App) e fornisce e AWS CloudFormation configura tali risorse al posto dell'utente.

Quando lo utilizzi AWS CloudFormation, puoi riutilizzare il modello per configurare le AWS Resilience Hub risorse in modo coerente e ripetuto. Descrivi le tue risorse una sola volta, quindi fornisci ripetutamente le stesse risorse in più AWS account e aree geografiche.

AWS Resilience Hub e AWS CloudFormation modelli

Per fornire e configurare le risorse AWS Resilience Hub e i servizi correlati, è necessario conoscere AWS CloudFormation i modelli. I modelli sono file di testo formattati in JSON o YAML. Questi modelli descrivono le risorse che desideri fornire negli AWS CloudFormation stack. Se non conosci JSON o YAML, puoi usare AWS CloudFormation Designer per iniziare a usare i modelli. AWS CloudFormation Per ulteriori informazioni, consulta Che cos'è AWS CloudFormation Designer? nella Guida per l'utente di AWS CloudFormation .

AWS Resilience Hub supporta la creazione e l'inserimento. AWS::ResilienceHub:::ResiliencyPolicy AWS::ResilienceHub:::App AWS CloudFormationPer 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 CloudFormation utente.

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.

Scopri di più su AWS CloudFormation

Per ulteriori informazioni su AWS CloudFormation, consulta le seguenti risorse:

- AWS CloudFormation
- AWS CloudFormation Guida per l'utente
- AWS CloudFormation Documentazione di riferimento API
- 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 le fasi del processo SOPs fornendo una serie di documenti SSM che è possibile utilizzare come base per tali operazioni. SOPs

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 SOPs, 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'Supporto AWSutente.

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 più recente aggiornata 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 in AWS Resilience Hub”
- 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 ha 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 in AWS Resilience Hub”
  - 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 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'Supporto AWS 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

- Versione API: ultima
- Ultimo aggiornamento della documentazione: 17 dicembre 2024

Modifica	Descrizione	Data
AWS Resilience Hub integra gli allarmi Amazon CloudWatch già implementati	AWS Resilience Hub ora rileva e integra automaticamente gli CloudWatch allarmi Amazon già configurati nelle sue valutazioni della resilienza, fornendo una visione più completa dello stato di resilienza dell'applicazione. Questa nuova funzionalità combina AWS Resilience Hub le raccomandazioni con l'attuale configurazione di monitoraggio per semplificare la gestione degli allarmi e migliorare l'accuratezza della valutazione. Per ulteriori informazioni, consulta Gestione degli allarmi.	17 dicembre 2024
AWS Resilience Hub ha abilitato funzionalità aggiuntive per fornire test di resilienza semplificati con esperimen	AWS Resilience Hub ora supporta una maggiore integrazione con AWS Fault Injection Service (AWS FIS)	17 dicembre 2024

ti personalizzati AWS Fault Injection Service	per offrire consigli personalizzati utilizzando AWS FIS azioni e scenari basati sul contesto applicativo specifico per migliorare il livello di resilienza. L'esecuzione degli esperimenti consigliati o dei test personalizzati migliorerà il punteggio di resilienza, consentendoti di tenere traccia delle modifiche nel tempo. Per ulteriori informazioni, consulta i seguenti argomenti: • AWSResilienceHubAssessmentExecutionPolicy • Gestione degli AWS Fault Injection Service esperimenti • AWS Resilience Hub — Test di resilienza

AWS Resilience Hub introduce una visualizzazione riassuntiva	AWS Resilience Hub offre una rappresentazione visiva di alto livello della resilienza delle applicazioni attraverso tabelle e grafici chiari, che consentono di visualizzare lo stato del portafoglio di applicazioni e di gestire e migliorare in modo efficiente la capacità delle applicazioni di resistere e riprendersi dalle interruzioni. Oltre alla nuova visualizzazione di riepilogo, è possibile esportare i dati che alimentano la visualizzazione di riepilogo per creare report personalizzati per la comunicazione con le parti interessate. Per ulteriori informazioni, consulta the section called “AWS Resilience Hub sommario”.	21 novembre 2024

AWS Resilience Hub introduce il widget Resiliency nella dashboard di MyApplications	Il nuovo widget Resiliency nella dashboard di myApplications semplifica la valutazione e il monitoraggio del livello di resilienza delle applicazioni. Consente di valutare rapidamente la resilienza delle applicazioni definite in myApplications senza doverle replicare manualmente in. AWS Resilience Hub Per ulteriori informazioni, consulta i seguenti argomenti: • the section called “AWS Resilience Hub e MyApplications” • the section called “Gestione delle valutazioni della resilienza dal widget Resiliency”	22 ottobre 2024

AWS Resilience Hub estende il supporto per Amazon ElastiCache (Redis OSS) Serverless	AWS Resilience Hub ora valuta le applicazioni che utilizzano Amazon ElastiCache (Redis OSS), inclusi Amazon ElastiCache (Redis OSS) Serverless e Global Datastores, e fornisce consigli di resilienza avanzati. Queste includono linee guida per le configurazioni regionali e multiregionali, nonché strategie per le implementazioni Multi-AZ, il raggruppamento delle risorse e il backup. Inoltre, per fornire un migliore controllo sulla posizione di resilienza delle applicazioni, offre CloudWatch allarmi AWS Resilience Hub Amazon personalizzati per Amazon ElastiCache (Redis OSS). Per ulteriori informazioni, consulta i seguenti argomenti: • the section called “Gestione dei componenti dell'applicazione” • the section called “ AWS Resilience Hub risorse supportate” • the section called “AWSResilienceHubAssessmentExecutionPolicy”	25 settembre 2024

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. 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”	1° agosto 2024

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 intellige nza artificiale generativa di Amazon Bedrock per trasformare dati di resilienz a 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 funzionalità 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 “Imposta la valutazione programmata e la notifica di deriva”	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 risorse Amazon EKS per includere nuove raccomandazioni operative. Durante l'esecuzione di una valutazione che include risorse dai cluster Amazon EKS, 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 AWS Fault Injection Service esperimenti”.	9 novembre 2023

AWS Resilience Hub fornisce informazioni aggiuntive a livello di applicazione	AWS Resilience Hub fornisce informazioni aggiuntive a livello di applicazione sull'RTO stimato del carico di lavoro e sull'RPO stimato del carico di lavoro. Queste informazioni aggiuntive indicano il carico di lavoro massimo possibile stimato (RTO) e l'RPO (carico di lavoro) stimato dell'applicazione in base all'ultima valutazione positiva. Questo valore è l'RTO del carico di lavoro massimo stimato e l'RPO del carico di lavoro stimato per tutti i tipi 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 RTO (Recovery Time Objectives) stimati del carico di lavoro e gli obiettivi RPO (Recovery Point Objectives) del carico di lavoro stimato. 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 “AWSResilienceHubAsssessmentExecutionPolicy”	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 AWS Fault Injection Service (AWS FIS) test. Durante l'esecuzione di una valutazione AWS Resilience Hub, 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 (Amazon SNS) di ricevere notifiche quando l'obiettivo del tempo di ripristino del carico di lavoro (RTO) stimato o l'obiettivo stimato del punto di ripristino del carico di lavoro (RPO) è passato dal raggiungimento dell'obiettivo a non soddisfar e 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 argomenti di Amazon SNS ti consentirà di anticipar e 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 “Imposta la valutazione programmata e la notifica di deriva”	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 applicazi oni che includono Amazon RDS, ora distingueremo tra diversi motori di database per fornire obiettivi di tempo di ripristino del carico di lavoro stimati più precisi (). RTOs AWS Resilience Hub fornirà inoltre azioni aggiuntive per implementare le migliori pratiche di resilienza all'inter no del tuo ambiente. AWS Le best practice possono includere approfondimenti sulle prestazioni con DevOps Guru for Amazon RDS, monitoraggio avanzato e automazione della distribuz ione blu/verde 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 (Amazon EBS) per riconoscere gli snapshot di Amazon EBS, che vengono acquisiti all'interno della stessa regione Amazon EBS tramite direct. APIs Il supporto esteso si aggiunge al supporto attuale per i clienti che utilizzano Amazon Data Lifecycle Manager (Amazon Data Lifecycle Manager) o Backup. AWS Per ulteriori informazioni, consulta la sezione relativa ad Amazon Elastic Block Store (Amazon EBS).	2 agosto 2023

Miglioramenti di Amazon Elastic Compute Cloud	AWS Resilience Hub ha esteso il supporto per Amazon Elastic Compute Cloud (Amazon EC2). 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 • Support per gruppi con auto-scaling con Amazon Application Recovery Controller (ARC) (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 gestite	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 CRR) /Amazon S3 Same-Region Replication (SRR), il controllo delle versioni e il backup ora AWS Resilienc e Hub valuteranno Amazon S3 per il punto di accesso multiregionale, Amazon S3 Replication Time Control (Amazon S3) RTC) AWS e configurazione di Backup Recovery (PITR). AWS point-in-time Per ulteriori informazioni, consulta i seguenti argomenti: • the section called “AWS Resilience Hub riferimen to alle autorizzazioni di accesso” • Gestione dello storage Amazon S3	21 marzo 2023

Supporto aggiuntivo per Amazon Elastic Kubernetes Service	AWS Resilience Hub ha aggiunto il cluster Amazon EKS come risorsa supportata per la definizione, la convalida e il monitoraggio della resilienza delle applicazioni. I clienti possono aggiungere cluster Amazon EKS ad applicazioni nuove o esistenti e ricevere valutazioni e consigli per migliorare la resilienza. I clienti possono aggiungere risorse applicative utilizzando Terraform AWS CloudFormation e MyApplications. AWS Resource Groups Inoltre, i clienti possono aggiungere uno o più cluster Amazon EKS direttamente in una o più regioni con uno o più namespace in ogni cluster. Ciò consente di AWS Resilience Hub fornire valutazioni e raccomandazioni singole e interregionali. Oltre a esaminare le implementazioni, le repliche e i pod, analizzare à la ReplicationControllers resilienza complessiva del cluster. AWS Resilience Hub AWS Resilience Hub supporta carichi di lavoro di cluster Amazon EKS stateless. Le nuove funzionalità sono disponibili in tutte le AWS	21 marzo 2023

	regioni in cui AWS Resilience Hub è supportata. Per ulteriori informazioni, consulta i seguenti argomenti: • the section called “Gestisci le risorse delle tue applicazioni” • 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 (Amazon EFS), ora AWS Resilience Hub valuterà Amazon EFS per la replica e la configurazione AZ di Amazon EFS. Per ulteriori informazioni, consulta i seguenti argomenti: • the section called “ AWS Resilience Hub risorse supportate” • What is 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 “Configurare i 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 (Amazon EBS) AWS Resilience Hub , ora valuterà gli snapshot di Amazon EBS tramite Amazon Data Lifecycle Manager e Amazon EBS 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 (Amazon EBS)	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 (RTO e RPO) è stata soddisfatta o meno. Ogni volta che viene eseguita una valutazione, 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 (Amazon SNS)	AWS Resilience Hub ora valuta le applicazioni che utilizzano Amazon SNS analizzando la configurazione di Amazon SNS, inclusi gli abbonati, e fornisce consigli per soddisfare gli obiettivi di ripristino del carico di lavoro stimati dell'organizzazione (RTO del carico di lavoro stimato e RPO del carico di lavoro stimato) per le applicazioni. 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 “Raggruppamento di risorse in un componente applicativo”	16 novembre 2022

Supporto aggiuntivo per Amazon Application Recovery Controller (ARC) (Amazon ARC)	AWS Resilience Hub ora valuta Amazon ARC for Elastic Load Balancing e Amazon Relational Database Service (Amazon RDS), che include consigli sui vantaggi di Amazon ARC. Estensione del supporto per AWS Resilience Hub la valutazione di Amazon ARC oltre AWS Auto Scaling Group AWS (ASG) e Amazon DynamoDB. Amazon ARC offre un'elevata disponibilità per la tua 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 ARC for Elastic Load Balancing e Amazon Relational Database Service (Amazon RDS), che include consigli sui vantaggi di Amazon ARC. Estensione del supporto per AWS Resilience Hub la valutazione di Amazon ARC oltre AWS Auto Scaling Group AWS (ASG) e Amazon DynamoDB. Amazon ARC offre un'elevata disponibi lità per la tua applicazione, consentendoti di eseguire rapidamente il failover dell'inte ra 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 applicati vi	Aggiunti Route53 e AWS Backup all'elenco delle risorse dei componenti applicativi supportate nella sezione di AppComponent raggruppa mento.	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 Resilience Hub	AWS Resilience Hub è ora disponibile. Questa guida descrive come utilizzarla AWS Resilience Hub per analizzare l'infrastruttura, ottenere consigli per migliorare la resilienza delle AWS app, esaminare i punteggi di resilienza e altro ancora.	10 novembre 2021

AWS Glossario

Per la AWS terminologia più recente, consultate il AWS glossario nella sezione Reference.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.