aws

Guida per gli sviluppatori

Amazon Application Recovery Controller (ARC)

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon Application Recovery Controller (ARC): Guida per gli sviluppatori

Copyright © 2026 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 dei rispettivi proprietari, che possono o meno essere affiliati, collegati o sponsorizzati da Amazon.

Table of Contents

Che cos'è ARC? 1
Ripristino della zona di disponibilità multipla 1
Ripristino in più regioni 2
Modifica della disponibilità per la verifica della disponibilità di Amazon Application Recovery Controller (ARC) 4
Opzioni di migrazione 4
Confronta le funzionalità Multi-AZ e Multi-region 5
Ripristino Multi-AZ 8
Spostamento zonale 8
Come funziona uno spostamento zonale 9
Regioni AWS 10
Zonal shift components 15
Piani di dati e controllo 18
Prezzi 18
Best practice 19
operazioni API 21
Esempi di utilizzo delle operazioni CLI 21
Risorse supportate 26
Avvio, aggiornamento o annullamento di un turno zonale 38
Registrazione di log e monitoraggio 40
IAM per il cambiamento zonale 44
Spostamento zonale automatico 55
Come funziona l'autoshift zonale 57
Regioni AWS 67
Zonal autoshift components 68
Piani di dati e controllo 71
Prezzi 71
Best practice 71
operazioni API 76
Esempi di utilizzo delle operazioni CLI 77
Abilitazione e utilizzo dell'autoshift zonale 84
Test dell'autoshift zonale con AWS FIS 89
Registrazione di log e monitoraggio 90
Identity and Access Management 102

Quote 116
Ripristino in più regioni 117
Controllo del routing 117
Informazioni sul controllo del routing 118
AWS Regioni 121
Componenti 122
Piani di dati e controllo 124
Assegnazione di tag 126
Prezzi 126
Guida introduttiva al ripristino in più regioni 127
Best practice 129
operazioni API 132
Esempi di utilizzo delle operazioni CLI 136
Utilizzo dei componenti di controllo del routing 153
Registrazione di log e monitoraggio 172
Identity and Access Management 177
Quote 192
Controllo di prontezza 193
Che cos'è il controllo di prontezza? 194
AWS Regioni 203
Componenti 203
Piani di dati e controllo 206
Assegnazione di tag 207
Prezzi 208
Configura un'applicazione resiliente 208
Best practice 209
operazioni API 210
Esempi di utilizzo delle operazioni CLI 213
Utilizzo dei gruppi di ripristino e dei controlli di fattibilità 224
Monitoraggio dello stato di preparazione 230
Ottenere consigli sull'architettura 232
Creazione di autorizzazioni per più account 234
Regole di preparazione, tipi di risorse e ARNS 236
Registrazione di log e monitoraggio 257
Identity and Access Management 272
Quote 287

Interruttore di regione 287
Informazioni su Region Switch 288
Best practice 303
Tutorial: active/passive piano 305
Tutorial: generazione automatica dei report 312
Tutorial: Esegui un flusso di lavoro post-ripristino RDS 315
operazioni API 317
Lavorare con l'interruttore di regione 319
Pannelli di controllo 359
Supporto multi-account 359
Identity and Access Management 365
Registrazione di log e monitoraggio 388
Quote 397
Esempi di codice 398
Nozioni di base 398
Azioni 399
Sicurezza 410
Protezione dei dati 411
Crittografia dei dati a riposo 412
Crittografia dei dati in transito 412
Identity and Access Management 412
Destinatari 412
Autenticazione con identità 413
Gestione dell’accesso tramite policy 414
In che modo le funzionalità di Amazon Application Recovery Controller (ARC) funzionano con IAM 416
Esempi di policy basate su identità 416
AWS politiche gestite 416
Risoluzione dei problemi 424
AWS PrivateLink 426
Registrazione di log e monitoraggio 428
Convalida della conformità 429
Resilienza 429
Sicurezza dell’infrastruttura 429
Cronologia dei documenti 431
..... cdxlix

Che cos'è ARC?

Amazon Application Recovery Controller (ARC) ti aiuta a prepararti e completare un ripristino più rapido per le applicazioni in esecuzione sull'infrastruttura cloud AWS globale.

ARC offre le seguenti funzionalità:

- Ripristino della zona di disponibilità multipla (AZ), che include lo spostamento di zona e lo spostamento automatico di zona, che consente di ripristinare i problemi relativi a una singola zona di disponibilità spostando temporaneamente il traffico da una zona di zona A compromessa a una zona di zona sana.
- Ripristino multiregionale, che include il controllo del routing e il cambio di regione per il ripristino delle applicazioni a livello regionale, e il controllo della disponibilità per il monitoraggio delle applicazioni.

Ripristino della zona di disponibilità multipla

Spostamento zonale

È possibile utilizzare ARC zonal shift per isolare e ripristinare rapidamente i problemi relativi a una singola zona di disponibilità (AZ). Lo spostamento zonale sposta temporaneamente il traffico di una risorsa supportata da una zona AZ compromessa verso una risorsa funzionante nella stessa regione. AZs AWS L'avvio di uno spostamento zonale consente di ripristinare rapidamente l'applicazione, ad esempio in seguito all'implementazione di codice errato da parte di uno sviluppatore o a seguito di un AWS danneggiamento in una singola zona di zona. L'allontanamento del traffico dalla zona AZ compromessa riduce l'impatto per i clienti che utilizzano l'applicazione nella zona AZ compromessa.

Puoi avviare uno spostamento di zona per qualsiasi risorsa supportata nel tuo account in una regione. AWS I turni zonali sono manuali e temporanei. Quando si avvia un turno zonale, è necessario specificare una scadenza (estendibile) fino a tre giorni. Per abilitare lo spostamento zonale per le risorse supportate, fare riferimento a. Risorse supportate

Cambio automatico zonale

L'autoshift zonale ARC AWS autorizza a spostare il traffico da una zona di zona compromessa a favore delle risorse supportate, per conto dell'utente, a favore di risorse sane nella stessa regione. AZs AWS AWS avvia uno spostamento automatico zonale quando la telemetria interna indica che in una zona AZ in una regione si è verificata una compromissione che potrebbe avere un impatto sui

clienti. AWS La telemetria interna incorpora metriche provenienti da più fonti, tra cui la rete e i servizi AWS Amazon ed Elastic Load EC2 Balancing.

Gli spostamenti automatici zonali sono temporanei. AWS termina uno spostamento automatico zonale quando gli indicatori di telemetria interni indicano che non esiste più un problema o un problema potenziale.

Per ulteriori informazioni su queste funzionalità, consulta i seguenti capitoli:

- Zonal shift in ARC
- Zonal autoshift in ARC

Ripristino in più regioni

Cambio di regione

Lo switch di regione in ARC offre una soluzione centralizzata, automatizzata e osservabile per il ripristino di applicazioni in più regioni. Il cambio di regione consente di pianificare e coordinare il ripristino per le applicazioni in modo da garantire Regioni AWS la continuità aziendale e ridurre il sovraccarico operativo.

È possibile utilizzare Region switch per orchestrare attività di ripristino complesse e su larga scala per le risorse applicative, su più account. AWS In caso Regione AWS di problemi, i piani creati utilizzando Region Switch possono eseguire il failover o trasferire le risorse in un'altra regione, in modo che l'applicazione possa continuare a funzionare in condizioni ottimali. Regione AWS

Controllo del routing

I controlli di routing estremamente affidabili di ARC consentono il ripristino in più regioni in modo che le applicazioni possano effettuare il failover del traffico DNS del Domain Name System tra le regioni. AWS

Se l'applicazione è progettata per funzionare in più AWS regioni, è possibile utilizzare il controllo del routing ARC per eseguire il failover tra le regioni. Il controllo del routing consente di effettuare il failover del traffico da una AWS regione compromessa a una AWS regione integra, in modo da garantire che l'applicazione mantenga la disponibilità. Il controllo del routing include regole di sicurezza che aiutano a proteggervi da esiti indesiderati imponendo barriere definite dall'utente. Ad esempio, è possibile imporre una regola di sicurezza in base alla quale solo una delle repliche dell'applicazione, attiva o in standby, è abilitata e in uso.

Controllo di prontezza

ARC Readiness Check monitora continuamente le quote di AWS risorse, la capacità e le politiche di routing di rete e può notificare all'utente le modifiche che potrebbero influire sulla capacità di eseguire il failover su un'applicazione di replica e di ripristinare i dati in caso di problemi regionali. I continui controlli di fattibilità garantiscono la possibilità di mantenere le applicazioni multiregionali in uno stato scalabile e configurato per gestire il traffico di failover. Il controllo di fattibilità è utile quando si configura ARC per la prima volta e durante il normale funzionamento dell'applicazione. Il controllo di fattibilità non è destinato all'uso nel percorso critico per il failover durante un evento.

Per ulteriori informazioni su queste funzionalità, consulta i seguenti capitoli:

- Cambio di regione in ARC
- Controllo del routing in ARC
- Controllo di prontezza in ARC

Modifica della disponibilità per la verifica della disponibilità di Amazon Application Recovery Controller (ARC)

> **Note**
>
> La funzionalità di controllo della disponibilità in Amazon Application Recovery Controller (ARC) non sarà più aperta ai nuovi clienti a partire dal 30 aprile 2026. I clienti esistenti possono continuare a utilizzare il servizio normalmente.

Dopo un'attenta valutazione, abbiamo deciso di chiudere la funzionalità di verifica della disponibilità in Amazon Application Recovery Controller (ARC) ai nuovi clienti a partire dal 30 aprile 2026. I clienti esistenti possono continuare a utilizzare il servizio normalmente.

Il controllo della disponibilità di ARC è una funzionalità che consente di monitorare la preparazione delle risorse per il disaster recovery. ARC continua a essere disponibile, ma la funzione di verifica della disponibilità non sarà più aperta ai nuovi clienti a partire dal 30 aprile 2026.

> **Note**
>
> Gli switch ARC e ARC Region continuano a essere pienamente supportati. Questa modifica riguarda solo la funzione di controllo della fattibilità. Non sono state apportate modifiche al cambio di regione, ai controlli di routing, allo spostamento di zona e allo spostamento automatico di zona.

Opzioni di migrazione

Per funzionalità simili al Readiness Check, consigliamo di eseguire l'onboarding dell'applicazione multiregionale su ARC Region Switch.

ARC Region Switch è un servizio completamente gestito che fornisce un'orchestrazione completa del ripristino multiregionale. Include una funzionalità chiamata valutazione del piano, che monitora regolarmente lo stato del piano di switch regionale per garantire la disponibilità all'esecuzione.

Per iniziare a usare ARC Region Switch, vedi. Cambio di regione in ARC

Confronta le funzionalità di ripristino Multi-AZ e Multi-region in ARC

Lo spostamento di zona, lo spostamento automatico di zona, il controllo del routing e lo switch di regione in Amazon Application Recovery Controller (ARC) possono tutti garantire un ripristino rapido e aiutarti a garantire la resilienza delle tue applicazioni. AWS Queste funzionalità sono altamente disponibili e aiutano a supportare il ripristino in scenari in cui l'applicazione presenta una maggiore latenza o una disponibilità ridotta. Queste funzionalità aiutano anche a ripristinare rapidamente le applicazioni spostando il traffico lontano da problemi isolati, il che limita l'impatto e il tempo perso a causa di tali problemi.

Il controllo del routing e il cambio di regione si concentrano sulle AWS applicazioni che si trovano in più aree Regioni AWS (multiregione), mentre lo spostamento zonale e lo spostamento automatico di zona supportano solo lo spostamento del traffico per le risorse supportate con applicazioni Multi-AZ.

Le informazioni contenute nella tabella seguente includono alcune delle caratteristiche chiave delle funzionalità di resilienza ARC. Queste descrizioni possono aiutarti a capire meglio come un'opzione specifica possa essere la scelta migliore per le esigenze della tua applicazione.

Controllo del routing	Interruttore di regione	Spostamento zonale	Cambio automatico zonale
Regionale Reindirizza il traffico da una regione all'altra (principa lmente) AWS	Regionale Reindirizza il traffico da una regione all'altra AWS (principa lmente)	Zonale Sposta il traffico lontano da una zona di disponibilità Il traffico viene indirizzato verso altre zone di disponibilità della regione, non verso un obiettivo specifico	Zonale Sposta il traffico lontano da una zona di disponibilità Il traffico viene indirizzato verso altre zone di disponibilità della regione, non verso un obiettivo specifico
Richiede una configurazione	Richiede configura zione	Potrebbe richiedere una configurazione	Richiede una configurazione

Controllo del routing	Interruttore di regione	Spostamento zonale	Cambio automatico zonale
Richiede configurazione e configurazione	Richiede configurazione e configurazione	Richiede l'attivazione di alcune risorse supportate Per ulteriori informazioni, fare riferimento a Risorse supportate	Deve essere abilitato per una risorsa supportata Per ulteriori informazioni, fare riferimento a Risorse supportate
Avviato dal cliente Il cliente decide quando reindirizzare il traffico	Avviato dal cliente Il cliente decide quando reindirizzare il traffico	Avviato dal cliente Il cliente determina quando iniziare un cambiamento di zona	AWS-avviato AWS sposta il traffico delle applicazioni da una AZ per conto dell'utente
A pagamento Richiede costi separati per il controllo del routing	A pagamento Richiede costi separati per i piani di cambio di regione	Incluso nei servizi (senza costi aggiuntivi) La creazione di turni zonali per allontanare il traffico AZs è inclusa nelle risorse supportate	Incluso nei servizi (senza costi aggiuntivi) L'avvio degli spostamenti automatici per allontanare il traffico per conto dell'utente è AZs incluso nelle risorse supportate
Non ha scadenza Il traffico può essere reindirizzato a una replica a tempo indeterminato	Non ha scadenza L'applicazione può essere spostata su una replica a tempo indeterminato	Temporaneo Tutti i turni zonali devono essere impostati come scaduti	Temporaneo AWS avvia e termina i turni automatici

Per ulteriori informazioni su ciascuna di queste funzionalità, consulta i seguenti capitoli:

- Zonal shift in ARC
- Zonal autoshift in ARC
- Controllo del routing in ARC
- Cambio di regione in ARC

Usa lo spostamento zonale e lo spostamento automatico di zona per ripristinare le applicazioni in ARC

Questa sezione spiega come utilizzare le funzionalità di Amazon Application Recovery Controller (ARC) per recuperare in modo affidabile una AWS risorsa da un problema in una zona di disponibilità (AZ) compromessa. Lo spostamento zonale e lo spostamento automatico di zona spostano temporaneamente il traffico di una risorsa supportata da una zona di zona compromessa, riducendo così i tempi di ripristino delle applicazioni.

La differenza principale tra lo spostamento zonale e lo spostamento automatico zonale è che uno è uno spostamento manuale del traffico controllato dall'utente, mentre l'altro allontana automaticamente il traffico da eventuali problemi.

- Con lo spostamento zonale, sposti manualmente il traffico verso una risorsa supportata allontanandolo da una zona di disponibilità. Regione AWS
- Con lo spostamento automatico zonale, il traffico relativo a una risorsa supportata viene automaticamente spostato da una zona di zona compromessa e reindirizzato a una risorsa integra nella stessa regione. AZs AWS

I seguenti argomenti descrivono le funzionalità di spostamento zonale e spostamento automatico di zona e come utilizzarle.

Argomenti

- Zonal shift in ARC
- Zonal autoshift in ARC

Zonal shift in ARC

Lo spostamento di zona di Amazon Application Recovery Controller (ARC) consente di spostare il traffico di una risorsa supportata da una zona di disponibilità (AZ) compromessa Regione AWS a uno integro AZs nella stessa regione. Lo spostamento del traffico delle risorse da una zona di disponibilità ridotta riduce la durata e la gravità dell'impatto causato da interruzioni di corrente o da problemi hardware o software in una zona di zona e aiuta a mitigare i problemi e ripristinare rapidamente l'applicazione. È possibile scegliere di spostare il traffico, per esempio, perché una cattiva implementazione causa problemi di latenza o perché la zona di disponibilità è compromessa.

È necessario attivare le risorse per utilizzare Zonal Shift. Per ulteriori informazioni, vedi Risorse supportate.

Prima di iniziare uno spostamento zonale, è necessario pre-scalare l'applicazione e assicurarsi di disporre di una capacità sufficiente per spostare il traffico lontano da una zona di disponibilità. Dopo la prescalabilità, puoi scegliere la zona di disponibilità da cui allontanarti e la risorsa verso cui spostare il traffico, quindi avviare lo spostamento zonale. Puoi annullare il turno in qualsiasi momento per far sì che il traffico inizi a tornare alla zona di disponibilità originale. Per ulteriori informazioni, consulta Best practice per spostamenti zonali in ARC

Tutti gli spostamenti zonali sono mitigazioni temporanee. Quando si avvia uno spostamento zonale, si imposta una scadenza iniziale, da un minuto a tre giorni (72 ore), che è possibile estendere, se è necessario continuare lo spostamento del traffico.

In scenari specifici, lo spostamento zonale non allontana il traffico dalla AZ. Per ulteriori informazioni, consulta Risorse supportate.

Come funziona uno spostamento zonale

Quando si avvia uno spostamento zonale per una risorsa supportata, il traffico relativo alla risorsa viene allontanato dalla zona di disponibilità (AZ) specificata. Le risorse supportate da ARC forniscono integrazioni che contrassegnano la zona Z specificata come non integra, il che si traduce in uno spostamento del traffico dalla zona AZ compromessa.

Il traffico inizia a cambiare: quando inizi uno spostamento di zona in ARC, potresti non vedere immediatamente il traffico uscire dalla zona di disponibilità. Il completamento delle connessioni esistenti e in corso nella Zona di Disponibilità può richiedere poco tempo, a seconda del comportamento del client e del riutilizzo della connessione. Le impostazioni DNS e altri fattori, tra cui le connessioni esistenti, possono essere completate in pochi minuti, ma potrebbero richiedere più tempo. Per ulteriori informazioni, consulta Garantire che i cambiamenti di traffico finiscano rapidamente.

Termina lo spostamento del traffico: quando scade un cambio di zona o lo annulli, ARC interviene per interrompere lo spostamento del traffico e inverte la procedura di avvio di un cambio di traffico. Ora, l'AZ recuperata viene riconosciuta come disponibile per la risorsa e il traffico riprende a fluire verso la AZ.

È necessario impostare tutti i turni zonali in modo che scadano all'inizio dei turni. Inizialmente puoi impostare la scadenza di un turno zonale dopo un massimo di tre giorni (72 ore). Tuttavia, puoi aggiornare un turno zonale per impostare una nuova scadenza in qualsiasi momento. Puoi anche

annullare uno spostamento zonale prima della scadenza, se sei pronto a ripristinare il traffico verso la zona di disponibilità.

Quando il traffico non si sposta: in scenari specifici, uno spostamento zonale non sposta il traffico dalla zona di disponibilità. Ad esempio, supponiamo di iniziare uno spostamento zonale per un sistema di bilanciamento del carico quando i gruppi target del sistema di bilanciamento del carico AZs non dispongono di istanze o se tutte le istanze non sono integre. In questo scenario, il load balancer si trova in uno stato di fail-open e l'avvio di uno spostamento di zona non comporta lo spostamento del traffico.

Prima di iniziare un cambiamento di zona per una risorsa, assicurati che siano soddisfatte tutte le condizioni per un cambiamento zonale efficace. AWS le risorse gestiscono i turni zonali in modo diverso. Per ulteriori informazioni sul supporto dei turni zonali, vedere. Risorse supportate

Regione AWS disponibilità per lo spostamento zonale

Per informazioni dettagliate sul supporto regionale e sugli endpoint di servizio per Amazon Application Recovery Controller (ARC), consulta gli endpoint e le quote di Amazon Application Recovery Controller (ARC) nel riferimento generale di Amazon Web Services.

Lo spostamento zonale e lo spostamento automatico di zona sono attualmente disponibili nelle versioni elencate qui. Regioni AWS Lo spostamento di zona e lo spostamento automatico di zona sono disponibili anche nelle regioni della Cina, ovvero la regione Cina (Pechino) e la regione Cina (Ningxia). Le risorse che utilizzano Amazon Application Recovery Controller (ARC) possono avere ulteriori considerazioni. Per ulteriori informazioni, vedi Risorse supportate.

Nome della regione	Regione	Endpoint	Protocollo	
US East (Ohio)	us-east-2	arc-zonal-shift.us-east-2.amazonaws.com	HTTPS	
		arc-zonal-shift-fips.us-east-2.api.aws	HTTPS	
		arc-zonal-shift.us-east-2.api.aws	HTTPS	
US East (N. Virginia)	us-east-1	arc-zonal-shift.us-east-1.amazonaws.com	HTTPS	
		arc-zonal-shift-fips.us-east-1.api.aws	HTTPS	

Nome della regione	Regione	Endpoint	Protocollo
		arc-zonal-shift.us-east-1.api.aws	HTTPS
Stati Uniti occidentali (California settentrionale)	us-west-1	arc-zonal-shift.us-west-1.amazonaws.com	HTTPS
		arc-zonal-shift-fips.us-west-1.api.aws	HTTPS
		arc-zonal-shift.us-west-1.api.aws	HTTPS
US West (Oregon)	us-west-2	arc-zonal-shift.us-west-2.amazonaws.com	HTTPS
		arc-zonal-shift-fips.us-west-2.api.aws	HTTPS
		arc-zonal-shift.us-west-2.api.aws	HTTPS
Africa (Città del Capo)	af-south-1	arc-zonal-shift.af-south-1.amazonaws.com	HTTPS
		arc-zonal-shift.af-south-1.api.aws	HTTPS
Asia Pacifico (Hong Kong)	ap-east-1	arc-zonal-shift.ap-east-1.amazonaws.com	HTTPS
		arc-zonal-shift.ap-east-1.api.aws	HTTPS
Asia Pacific (Hyderabad)	ap-south-2	arc-zonal-shift.ap-south-2.amazonaws.com	HTTPS
		arc-zonal-shift.ap-south-2.api.aws	HTTPS
Asia Pacifico (Giacarta)	ap-southeast-3	arc-zonal-shift.ap-southeast-3.amazonaws.com	HTTPS
		arc-zonal-shift.ap-southeast-3.api.aws	HTTPS

Nome della regione	Regione	Endpoint	Protocollo	
Asia Pacifico (Malesia)	ap-southeast-5	arc-zonal-shift.ap-southeast-5.amazonaws.com arc-zonal-shift.ap-southeast-5.api.aws	HTTPS HTTPS	
Asia Pacifico (Melbourne)	ap-southeast-4	arc-zonal-shift.ap-southeast-4.amazonaws.com arc-zonal-shift.ap-southeast-4.api.aws	HTTPS HTTPS	
Asia Pacifico (Mumbai)	ap-south-1	arc-zonal-shift.ap-south-1.amazonaws.com arc-zonal-shift.ap-south-1.api.aws	HTTPS HTTPS	
Asia Pacifico (Nuova Zelanda)	ap-southeast-6	arc-zonal-shift.ap-southeast-6.amazonaws.com arc-zonal-shift.ap-southeast-6.api.aws	HTTPS HTTPS	
Asia Pacifico (Osaka-Locale)	ap-northeast-3	arc-zonal-shift.ap-northeast-3.amazonaws.com arc-zonal-shift.ap-northeast-3.api.aws	HTTPS HTTPS	
Asia Pacifico (Seoul)	ap-northeast-2	arc-zonal-shift.ap-northeast-2.amazonaws.com arc-zonal-shift.ap-northeast-2.api.aws	HTTPS HTTPS	
Asia Pacifico (Singapore)	ap-southeast-1	arc-zonal-shift.ap-southeast-1.amazonaws.com arc-zonal-shift.ap-southeast-1.api.aws	HTTPS HTTPS	

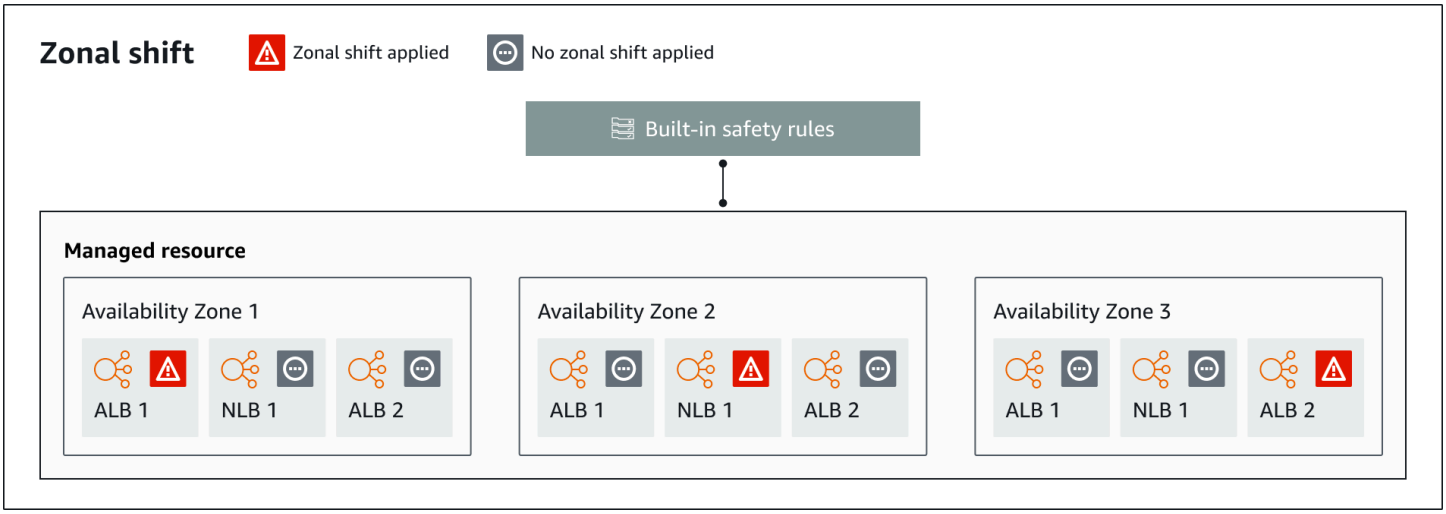
Nome della regione	Regione	Endpoint	Protocollo
Asia Pacifico (Sydney)	ap-southeast-2	arc-zonal-shift.ap-southeast-2.amazonaws.com	HTTPS
		arc-zonal-shift.ap-southeast-2.api.aws	HTTPS
Asia Pacifico (Taipei)	ap-east-2	arc-zonal-shift.ap-east-2.amazonaws.com	HTTPS
		arc-zonal-shift.ap-east-2.api.aws	HTTPS
Asia Pacifico (Thailandia)	ap-southeast-7	arc-zonal-shift.ap-southeast-7.amazonaws.com	HTTPS
		arc-zonal-shift.ap-southeast-7.api.aws	HTTPS
Asia Pacifico (Tokyo)	ap-northeast-1	arc-zonal-shift.ap-northeast-1.amazonaws.com	HTTPS
		arc-zonal-shift.ap-northeast-1.api.aws	HTTPS
Canada (Centrale)	ca-central-1	arc-zonal-shift.ca-central-1.amazonaws.com	HTTPS
		arc-zonal-shift-fips.ca-central-1.api.aws	HTTPS
		arc-zonal-shift.ca-central-1.api.aws	HTTPS
Canada occidentale (Calgary)	ca-west-1	arc-zonal-shift.ca-west-1.amazonaws.com	HTTPS
		arc-zonal-shift-fips.ca-west-1.api.aws	HTTPS
		arc-zonal-shift.ca-west-1.api.aws	HTTPS
Europa (Francoforte)	eu-central-1	arc-zonal-shift.eu-central-1.amazonaws.com	HTTPS
		arc-zonal-shift.eu-central-1.api.aws	HTTPS
Europa (Irlanda)	eu-west-1	arc-zonal-shift.eu-west-1.amazonaws.com	HTTPS
		arc-zonal-shift.eu-west-1.api.aws	HTTPS

Nome della regione	Regione	Endpoint	Protocollo
Europa (Londra)	eu-west-2	arc-zonal-shift.eu-west-2.amazonaws.com arc-zonal-shift.eu-west-2.api.aws	HTTPS HTTPS
Europa (Milano)	eu-south-1	arc-zonal-shift.eu-south-1.amazonaws.com arc-zonal-shift.eu-south-1.api.aws	HTTPS HTTPS
Europa (Parigi)	eu-west-3	arc-zonal-shift.eu-west-3.amazonaws.com arc-zonal-shift.eu-west-3.api.aws	HTTPS HTTPS
Europa (Spagna)	eu-south-2	arc-zonal-shift.eu-south-2.amazonaws.com arc-zonal-shift.eu-south-2.api.aws	HTTPS HTTPS
Europa (Stoccolma)	eu-north-1	arc-zonal-shift.eu-north-1.amazonaws.com arc-zonal-shift.eu-north-1.api.aws	HTTPS HTTPS
Europa (Zurigo)	eu-central-2	arc-zonal-shift.eu-central-2.amazonaws.com arc-zonal-shift.eu-central-2.api.aws	HTTPS HTTPS
Israele (Tel Aviv)	il-central-1	arc-zonal-shift.il-central-1.amazonaws.com arc-zonal-shift.il-central-1.api.aws	HTTPS HTTPS
Messico (Centrale)	mx-central-1	arc-zonal-shift.mx-central-1.amazonaws.com arc-zonal-shift.mx-central-1.api.aws	HTTPS HTTPS
Medio Oriente (Bahrein)	me-south-1	arc-zonal-shift.me-south-1.amazonaws.com arc-zonal-shift.me-south-1.api.aws	HTTPS HTTPS

Nome della regione	Regione	Endpoint	Protocollo
Medio Oriente (Emirati Arabi Uniti)	me-central-1	arc-zonal-shift.me-central-1.amazonaws.com arc-zonal-shift.me-central-1.api.aws	HTTPS HTTPS
Sud America (São Paulo)	sa-east-1	arc-zonal-shift.sa-east-1.amazonaws.com arc-zonal-shift.sa-east-1.api.aws	HTTPS HTTPS
AWS GovCloud (Stati Uniti orientali)	us-gov-east-1	arc-zonal-shift.us-gov-east-1.amazonaws.com arc-zonal-shift-fips.us-gov-east-1.api.aws arc-zonal-shift.us-gov-east-1.api.aws	HTTPS HTTPS HTTPS
AWS GovCloud (Stati Uniti occidentali)	us-gov-west-1	arc-zonal-shift.us-gov-west-1.amazonaws.com arc-zonal-shift-fips.us-gov-west-1.api.aws arc-zonal-shift.us-gov-west-1.api.aws	HTTPS HTTPS HTTPS

Zonal shift components

Il diagramma seguente illustra un esempio di spostamento zonale che sposta il traffico lontano da una zona di disponibilità in un. Regione AWS I controlli incorporati nello spostamento zonale impediscono di iniziare un altro turno zonale per una risorsa quando ha già un turno attivo.



Di seguito sono riportati i componenti della funzionalità di spostamento zonale in ARC.

Spostamento zonale

Si avvia uno spostamento di zona per una risorsa gestita nel proprio AWS account per spostare temporaneamente il traffico da una zona di disponibilità in una Regione AWS zona a uno AZs attivo nella regione, per ripristinare rapidamente un problema in una zona. Per ulteriori informazioni sulle risorse supportate per lo spostamento zonale, fare riferimento a. Risorse supportate

Controlli di sicurezza integrati

I controlli integrati in ARC impediscono che si verifichi più di uno spostamento di traffico per una risorsa alla volta. In altre parole, è possibile spostare attivamente il traffico lontano da una zona di disponibilità solo con un cambio di zona, un esercizio o uno spostamento automatico della risorsa su iniziativa del cliente. Ad esempio, se si avvia uno spostamento di zona per una risorsa quando è attualmente spostata via con lo spostamento automatico, il cambiamento di zona ha la precedenza. Per ulteriori informazioni, consulta e Risultati per le prove pratiche. Zonal autoshift in ARC

Identificatore di risorsa

L'identificatore di una risorsa da includere in uno spostamento zonale. L'identificatore è l'Amazon Resource Name (ARN) della risorsa.

Per un cambio di zona, puoi scegliere le risorse del tuo account solo per un AWS servizio supportato da ARC. Per ulteriori informazioni sulle risorse supportate per lo spostamento zonale, fare riferimento a. Risorse supportate

Risorsa gestita

Alcune AWS risorse devono attivare manualmente lo spostamento di zona, mentre altre vengono abilitate automaticamente. Per ulteriori informazioni sulle risorse supportate per lo spostamento zonale, fare riferimento a. Risorse supportate

Nome risorsa

Il nome di una risorsa in ARC che è possibile specificare per uno spostamento di zona.

Stato (stato del turno zonale)

Uno status per un cambiamento zonale. Lo `Status` per uno spostamento zonale può avere uno dei seguenti valori:

- ATTIVO: Lo spostamento zonale viene avviato e attivo.
- SCADUTO: Lo spostamento zonale è scaduto (il tempo di scadenza è stato superato).
- ANNULLATO: Il turno zonale è stato annullato.

Stato applicato

Lo stato applicato indica se per una risorsa è in corso un cambiamento. Lo spostamento con lo stato `APPLIED` determina la zona di disponibilità in cui il traffico dell'applicazione è stato spostato verso una risorsa e quando termina tale turno.

Tipo di turno

Definisce il tipo di spostamento zonale. `shiftType`Possono avere i seguenti valori:

- ZONAL_SHIFT
- ZONAL_AUTOSHIFT
- ESERCITAZIONE_CORRI
- FIS EXPERIMENT

Ora di scadenza (ora di scadenza)

L'ora di scadenza (ora di scadenza) di un cambiamento di zona. Gli spostamenti zonali sono temporanei. Per un turno zonale, puoi inizialmente impostare un turno zonale in modo che rimanga attivo per un massimo di tre giorni (72 ore).

Quando si avvia uno spostamento zonale, si specifica per quanto tempo si desidera che rimanga attivo, che ARC converte in un'ora di scadenza (ora di scadenza). Puoi annullare

uno spostamento zonale, ad esempio, se sei pronto a ripristinare il traffico verso la zona di disponibilità. Oppure puoi estendere un cambiamento zonale avviato dal cliente aggiornandolo per specificare un altro periodo di scadenza.

È possibile annullare le esercitazioni a turni zonali che fanno parte del cambio automatico zonale.

Piani di dati e controllo per lo spostamento zonale

Quando pianifichi il failover e il disaster recovery, considera la resilienza dei tuoi meccanismi di failover. Ti consigliamo di assicurarti che i meccanismi da cui dipendi durante il failover siano altamente disponibili, in modo da poterli utilizzare quando ne hai bisogno in uno scenario di emergenza. In genere, è consigliabile utilizzare le funzioni del piano dati per i meccanismi ogni volta che è possibile, per la massima affidabilità e tolleranza ai guasti. In quest'ottica, è importante capire in che modo la funzionalità di un servizio è suddivisa tra piani di controllo e piani dati e quando è possibile contare su un'aspettativa di estrema affidabilità con il piano dati di un servizio.

Come per la maggior parte dei AWS servizi, la funzionalità per la funzionalità di spostamento zonale è supportata dai piani di controllo e dai piani dati. Sebbene entrambi siano progettati per essere affidabili, un piano di controllo è ottimizzato per la coerenza dei dati, mentre un piano dati è ottimizzato per la disponibilità. Un piano dati è progettato per la resilienza in modo da poter mantenere la disponibilità anche durante eventi di interruzione, quando un piano di controllo potrebbe non essere disponibile.

In generale, un piano di controllo consente di eseguire funzioni di gestione di base, come creare, aggiornare ed eliminare risorse nel servizio. Un piano dati fornisce le funzionalità principali di un servizio.

Per ulteriori informazioni sui piani dati, sui piani di controllo e su come AWS crea servizi per soddisfare gli obiettivi di alta disponibilità, consulta il paper Static stability using Availability Zones in Amazon Builders' Library.

Prezzi per il cambio di zona in ARC

Per quanto riguarda lo spostamento di zona, puoi avviare uno spostamento di zona per le risorse supportate, per ripristinare l'applicazione da un problema in una zona di disponibilità. Non sono previsti costi aggiuntivi per l'utilizzo dello spostamento zonale.

Per informazioni dettagliate sui prezzi di ARC ed esempi di prezzi, consulta ARC Pricing.

Best practice per spostamenti zonali in ARC

Consigliamo le seguenti best practice per l'utilizzo dei turni zonali per il ripristino Multi-AZ in ARC.

Argomenti

- Pianificazione e pre-scalabilità della capacità
- Limita il tempo in cui i clienti rimangono connessi ai tuoi endpoint
- Prova in anticipo l'inizio dei turni zonali
- Assicurati che tutte le zone di disponibilità siano funzionanti e che assorbano traffico
- Utilizza le operazioni dell'API Data Plane per il disaster recovery
- Sposta il traffico con uno spostamento di zona solo temporaneamente

Pianificazione e pre-scalabilità della capacità

Assicurati di aver pianificato e predimensionato o di poter scalare automaticamente una capacità sufficiente per far fronte al carico aggiuntivo imposto alle zone di disponibilità quando inizi un turno di zona. In un'architettura orientata al ripristino, in genere si consiglia di predimensionare la capacità di elaborazione in modo da includere un margine di crescita sufficiente per soddisfare i picchi di traffico quando una delle tre repliche (in genere) è offline.

Quando si avvia uno spostamento di zona per una risorsa supportata e il traffico viene spostato da una zona a zona, la capacità utilizzata dall'applicazione per le richieste di assistenza viene rimossa. È necessario assicurarsi di aver pianificato uno spostamento del traffico lontano da una zona di zona e di poter continuare a soddisfare le richieste nelle restanti aree. AZs

Limita il tempo in cui i client rimangono connessi ai tuoi endpoint

Quando Amazon Application Recovery Controller (ARC) allontana il traffico da un problema, ad esempio utilizzando lo spostamento zonale o lo spostamento automatico di zona, il meccanismo utilizzato da ARC per spostare il traffico dell'applicazione è un aggiornamento DNS. Un aggiornamento DNS fa sì che tutte le nuove connessioni vengano indirizzate lontano dalla posizione compromessa.

Tuttavia, i client con connessioni aperte preesistenti potrebbero continuare a effettuare richieste nei confronti della posizione compromessa fino alla riconnessione dei client. Per garantire un ripristino rapido, ti consigliamo di limitare il periodo di tempo in cui i client rimangono connessi ai tuoi endpoint.

Prova in anticipo l'inizio dei turni zonali

Prova regolarmente a spostare il traffico lontano dalle zone di disponibilità per la tua applicazione avviando i turni zonali. Pianifica ed esegui turni zonali iniziali, preferibilmente in ambienti di test e produzione, come parte dei regolari test di failover per il ripristino delle applicazioni in caso di emergenza. I test regolari sono fondamentali per garantire che siate pronti e abbiate la sicurezza necessaria per mitigare i problemi quando si verifica un evento operativo.

Assicurati che tutte le zone di disponibilità siano integre e che assorbano traffico

I turni zonali funzionano contrassegnando una risorsa, ovvero una replica dell'applicazione, come non integra in una zona di disponibilità. Ciò significa che è fondamentale garantire che le risorse delle applicazioni siano generalmente integre e che assorbano attivamente il traffico nelle zone di disponibilità di una regione. Ti consigliamo di disporre di dashboard per tenere traccia di ciò, tra cui, ad esempio, le metriche Elastic Load Balancing per destinazioni non integre e BytesProcessed per Availability Zone.

Prendi in considerazione la possibilità di monitorare lo stato delle tue risorse da una seconda regione adiacente. I vantaggi di questo approccio sono che può essere più rappresentativo dell'esperienza degli utenti finali e riduce anche il rischio che sia l'applicazione che il monitoraggio vengano colpiti dallo stesso problema contemporaneamente.

Utilizza le operazioni API del piano dati per il disaster recovery

Per avviare un cambiamento di zona quando è necessario ripristinare un'applicazione rapidamente e con poche dipendenze, consigliamo di utilizzare l'API AWS Command Line Interface or con azioni di spostamento zonale, con credenziali prememorizzate, se possibile. Puoi anche avviare turni zonali in, per facilità d'uso. Console di gestione AWS Ma quando un ripristino rapido e affidabile è fondamentale, le operazioni sul piano dati sono una scelta migliore. Per ulteriori informazioni, consulta la Zonal Shift API Reference Guide.

Sposta il traffico con uno spostamento di zona solo temporaneamente

Uno spostamento zonale allontana temporaneamente il traffico da una zona di disponibilità, per mitigare un danno. È necessario ripristinare la risorsa per l'applicazione in servizio non appena si interviene per correggere un problema. Ciò garantisce che l'intera applicazione venga ripristinata allo stato originale, completamente ridondante e resiliente.

Operazioni dell'API Zonal Shift

La tabella seguente elenca le operazioni dell'API ARC che è possibile utilizzare utilizzando lo spostamento zonale, che allontana il traffico da una zona di disponibilità per applicazioni Multi-AZ. La tabella include anche collegamenti alla documentazione pertinente.

Per esempi di come utilizzare le operazioni comuni dell'API Zonal Shift con, vedi. AWS Command Line InterfaceEsempi di utilizzo di AWS CLI with zonal shift

Azione	Utilizzo della console ARC	Utilizzando l'API ARC
Avviare uno spostamento zonale	Consulta Starting a zonal shift.	Consulta la sezione StartZonalShift
Aggiornare uno spostamento zonale	Consulta Updating or canceling a zonal shift.	Consulta la sezione UpdateZonalShift
Elenca i turni zonali	Consulta Zonal shift in ARC.	Consulta la sezione ListZonalShifts
Elenca le risorse gestite	Consulta Risorse supportate.	Consulta la sezione ListManagedResources
Ottieni risorse gestite	Consulta Risorse supportate.	Consulta la sezione GetManagedResource
Annullare uno spostamento zonale	Consulta Updating or canceling a zonal shift.	Consulta la sezione CancelZonalShift

Esempi di utilizzo di AWS CLI with zonal shift

Questa sezione fornisce esempi applicativi di utilizzo dello zonal shift, dell'utilizzo della AWS Command Line Interface funzionalità zonal shift in Amazon Application Recovery Controller (ARC) utilizzando le operazioni API. Gli esempi hanno lo scopo di aiutarti a sviluppare una comprensione di base su come lavorare con il cambiamento zonale utilizzando la CLI.

Lo spostamento zonale in ARC consente di spostare temporaneamente il traffico per le risorse supportate lontano da una zona di disponibilità in modo che l'applicazione possa continuare a funzionare normalmente con altre zone di disponibilità contemporaneamente. Regione AWS

Tutti i turni zonali sono temporanei e devono essere impostati inizialmente per scadere entro tre giorni. Tuttavia, puoi aggiornare un turno zonale in un secondo momento per impostare una nuova scadenza.

Per ulteriori informazioni sull'utilizzo di AWS CLI, vedere AWS CLI Command Reference. Per un elenco delle azioni dell'API Zonal Shift e i collegamenti a ulteriori informazioni, vedereOperazioni dell'API Zonal Shift.

Inizia lo spostamento zonale

È possibile avviare uno spostamento di zona con la CLI utilizzando `start-zonal-shift` il comando.

```
aws arc-zonal-shift start-zonal-shift \
       --resource-identifier arn:aws:elasticloadbalancing:us-
east-1:111122223333:loadbalancer/app/Testing/5a19403ecd42dc05 \
       --away-from use1-az1 \
       --expires-in 10m \
       --comment "Shifting traffic away from use1-az1"
```

```
{
    "awayFrom": "use1-az1",
    "comment": "Shifting traffic away from use1-az1",
    "expiryTime": "2024-12-17T21:37:26-08:00",
    "resourceIdentifier": "arn:aws:elasticloadbalancing:us-
east-1:111122223333:loadbalancer/app/Testing/5a19403ecd42dc05",
    "startTime": "2024-12-17T21:27:26-08:00",
    "status": "ACTIVE",
    "zonalShiftId": "9ac9ec1e-1df1-0755-3dc5-8cf573cd9c38"
}
```

Ottieni risorse gestite

È possibile ottenere informazioni su una risorsa gestita con la CLI utilizzando il `get-managed-resource` comando.

```
aws arc-zonal-shift get-managed-resource \
       --resource-identifier arn:aws:elasticloadbalancing:us-
east-1:111122223333:loadbalancer/app/Testing/5a19403ecd42dc05
```

```
{
```

```
    "appliedWeights": {
        "use1-az1": 0.0,
        "use1-az2": 1.0,
        "use1-az6": 1.0
    },
    "arn": "arn:aws:elasticloadbalancing:us-east-1:111122223333:loadbalancer/app/
Testing/5a19403ecd42dc05",
    "autoshifts": [],
    "name": "Testing",
    "zonalAutoshiftStatus": "DISABLED",
    "zonalShifts": [
        {
            "appliedStatus": "APPLIED",
            "awayFrom": "use1-az1",
            "comment": "Shifting traffic away from use1-az1",
            "expiryTime": "2024-12-17T21:37:26-08:00",
            "resourceIdentifier": "arn:aws:elasticloadbalancing:us-
east-1:111122223333:loadbalancer/app/Testing/5a19403ecd42dc05",
            "startTime": "2024-12-17T21:27:26-08:00",
            "zonalShiftId": "9ac9ec1e-1df1-0755-3dc5-8cf573cd9c38"
            "shiftType": "MANUAL"
        }
    ]
}
```

Elenca le risorse gestite

Puoi elencare le risorse gestite nel tuo account con la CLI utilizzando il `list-managed-resources` comando.

```
aws arc-zonal-shift list-managed-resources
```

```
{
    "items": [
        {
            "appliedWeights": {
                "use1-az1": 0.0,
                "use1-az2": 1.0,
                "use1-az6": 1.0
            },
            "arn": "arn:aws:elasticloadbalancing:us-east-1:111122223333:loadbalancer/
app/Testing/5a19403ecd42dc05",
            "autoshifts": [],
```

```
            "availabilityZones": [
                "use1-az1",
                "use1-az2",
                "use1-az6"
            ],
            "name": "Testing",
            "practiceRunStatus": "DISABLED",
            "zonalAutoshiftStatus": "DISABLED",
            "zonalShifts": [
                {
                    "appliedStatus": "APPLIED",
                    "awayFrom": "use1-az1",
                    "comment": "Shifting traffic away from use1-az1",
                    "expiryTime": "2024-12-17T21:37:26-08:00",
                    "resourceIdentifier": "arn:aws:elasticloadbalancing:us-
east-1:111122223333:loadbalancer/app/Testing/5a19403ecd42dc05",
                    "startTime": "2024-12-17T21:27:26-08:00",
                    "zonalShiftId": "9ac9ec1e-1df1-0755-3dc5-8cf573cd9c38"
                }
            ]
        }
    ]
}
```

Elenca i turni zonali

Puoi elencare i cambiamenti zonali nel tuo account con la CLI usando il comando. `list-zonal-shifts`

```
aws arc-zonal-shift list-zonal-shifts
```

```
{
    "items": [
        {
            "awayFrom": "use1-az1",
            "comment": "Shifting traffic away from use1-az1",
            "expiryTime": "2024-12-17T21:37:26-08:00",
            "resourceIdentifier": "arn:aws:elasticloadbalancing:us-
east-1:111122223333:loadbalancer/app/Testing/5a19403ecd42dc05",
            "startTime": "2024-12-17T21:27:26-08:00",
            "status": "ACTIVE",
            "zonalShiftId": "9ac9ec1e-1df1-0755-3dc5-8cf573cd9c38"
```

```
        }
    ]
}
```

Aggiorna lo spostamento zonale

È possibile aggiornare uno spostamento zonale con la CLI utilizzando `update-zonal-shift` il comando.

```
aws arc-zonal-shift update-zonal-shift \
       --zonal-shift-id 9ac9ec1e-1df1-0755-3dc5-8cf573cd9c38 \
       --expires-in 1h \
       --comment "Still shifting traffic away from use1-az1"
```

```
{
    "awayFrom": "use1-az1",
    "comment": "Still shifting traffic away from use1-az1",
    "expiryTime": "2024-12-17T22:29:38-08:00",
    "resourceIdentifier": "arn:aws:elasticloadbalancing:us-
east-1:111122223333:loadbalancer/app/Testing/5a19403ecd42dc05",
    "startTime": "2024-12-17T21:27:26-08:00",
    "status": "ACTIVE",
    "zonalShiftId": "9ac9ec1e-1df1-0755-3dc5-8cf573cd9c38"
}
```

Annulla lo spostamento zonale

È possibile annullare uno spostamento zonale con la CLI utilizzando `cancel-zonal-shift` il comando.

```
aws arc-zonal-shift cancel-zonal-shift \
       --zonal-shift-id 9ac9ec1e-1df1-0755-3dc5-8cf573cd9c38
```

```
{
    "awayFrom": "use1-az1",
    "comment": "Still shifting traffic away from use1-az1",
    "expiryTime": "2024-12-17T22:29:38-08:00",
    "resourceIdentifier": "arn:aws:elasticloadbalancing:us-
east-1:111122223333:loadbalancer/app/Testing/5a19403ecd42dc05",
    "startTime": "2024-12-17T21:27:26-08:00",
    "status": "CANCELED",
```

```
    "zonalShiftId": "9ac9ec1e-1df1-0755-3dc5-8cf573cd9c38"
}
```

Risorse supportate

Amazon Application Recovery Controller (ARC) attualmente supporta l'attivazione delle seguenti risorse per lo spostamento zonale e lo spostamento automatico di zona:

- Gruppi Amazon EC2 Auto Scaling
- Amazon Elastic Kubernetes Service
- Application Load Balancercon bilanciamento del carico tra zone abilitato o disabilitato
- Network Load Balancerscon il bilanciamento del carico tra zone abilitato o disabilitato

Per i requisiti specifici per Network Load Balancer e Application Load Balancer, consulta gli argomenti aggiuntivi di questa sezione.

Esamina le seguenti condizioni per lavorare con i turni zonali, lo spostamento automatico di zona e le risorse in ARC:

- Una risorsa deve essere attiva e dotata di tutte le risorse necessarie per spostarne il traffico. Prima di iniziare uno spostamento di zona per una risorsa, assicurati che si tratti di una risorsa gestita in ARC. Ad esempio, visualizza l'elenco delle risorse gestite in o utilizza l'`get-managed-resource`operazione con l'identificatore della risorsa. Console di gestione AWS
- Per iniziare un turno di zona con una risorsa, questa deve essere distribuita nella zona di disponibilità e nel luogo in Regione AWS cui si inizia il turno. Assicurati di avviare uno spostamento di zona nella stessa regione in cui si trova la zona di residenza da cui desideri allontanarti e che anche la risorsa per cui stai trasferendo il traffico si trovi nella stessa zona e regione.
- Assicurati di disporre delle autorizzazioni IAM corrette per utilizzare lo spostamento zonale con una risorsa. Per ulteriori informazioni, consulta IAM e autorizzazioni per lo spostamento zonale.
- Quando un Network Load Balancer o un Application Load Balancer si trova in uno stato di fail-open, uno spostamento di zona non avrà alcun effetto. Si tratta di un comportamento previsto, in quanto lo spostamento zonale non può forzare una AZ a non funzionare correttamente e quindi spostare il traffico verso l'altra AZs in una regione quando un sistema di bilanciamento del carico non riesce ad aprire. Per ulteriori informazioni, consulta Utilizzo del failover DNS di Route 53 per il sistema di bilanciamento del carico nella Guida dell'utente di Network Load Balancers e Utilizzo del failover DNS di Route 53 per il bilanciamento del carico nella Guida utente di Application Load Balancers.

- Se più sistemi di bilanciamento del carico inoltrano il traffico verso le stesse destinazioni, uno spostamento zonale su un sistema di bilanciamento del carico abilitato tra zone riduce la capacità target per tutti i sistemi di bilanciamento del carico, anche se il traffico non viene spostato da uno spostamento di zona.

Gruppi Amazon EC2 Auto Scaling

Un gruppo Amazon EC2 Auto Scaling contiene una raccolta di istanze Amazon EC2 che vengono trattate come un raggruppamento logico ai fini del ridimensionamento e della gestione automatici. I gruppi con scalabilità automatica consentono inoltre di utilizzare caratteristiche di Dimensionamento automatico Amazon EC2, quali le sostituzioni dei controlli di integrità e le policy di dimensionamento. Il mantenimento del numero di istanze in un gruppo con scalabilità automatica e la scalabilità automatica sono entrambe funzionalità di base del servizio Dimensionamento automatico Amazon EC2.

Utilizzo dello spostamento zonale per i gruppi di Auto Scaling

Per abilitare lo spostamento zonale, utilizzate uno dei seguenti metodi.

Console

Per abilitare lo spostamento zonale su un nuovo gruppo (console)

1. Segui le istruzioni riportate in Creare un gruppo di Auto Scaling utilizzando un modello di avvio e completa ogni passaggio della procedura, fino al passaggio 10.
2. Nella pagina Integra con altri servizi, per lo spostamento zonale ARC, seleziona la casella di controllo per abilitare lo spostamento zonale.
3. Per il comportamento del controllo sanitario, scegli Ignora non salutare o Sostituisci non salutare. Se impostato `sureplace-unhealthy`, le istanze non integre verranno sostituite nella Zona di disponibilità con lo spostamento zonale attivo. Se impostato `suignore-unhealthy`, le istanze non integre non verranno sostituite nella Zona di disponibilità con lo spostamento zonale attivo.
4. Continua con i passaggi descritti in Creare un gruppo di Auto Scaling utilizzando un modello di avvio.

AWS CLI

Per abilitare lo spostamento zonale su un nuovo gruppo ()AWS CLI

Aggiungi il parametro `--availability-zone-impairment-policy` al comando create-auto-scaling-group.

Il `--availability-zone-impairment-policy` parametro ha due opzioni:

- ZonalShiftEnabled— Se impostato su`true`, Auto Scaling registra il gruppo Auto Scaling con lo spostamento zonale ARC ed è possibile avviare, aggiornare o annullare uno spostamento zonale sulla console ARC. Se impostato su`false`, Auto Scaling annulla la registrazione del gruppo Auto Scaling dallo spostamento zonale ARC. È necessario che lo spostamento zonale sia già abilitato per impostarlo su. `false`
- ImpairedZoneHealthCheckBehavior— Se impostato su`replace-unhealthy`, le istanze non integre verranno sostituite nella zona di disponibilità con lo spostamento zonale attivo. Se impostato su`ignore-unhealthy`, le istanze non integre non verranno sostituite nella Zona di disponibilità con lo spostamento zonale attivo.

L'esempio seguente abilita lo spostamento zonale su un nuovo gruppo Auto Scaling denominato. *my-asg*

```
aws autoscaling create-auto-scaling-group \
  --launch-template LaunchTemplateName=my-launch-template,Version='1' \
  --auto-scaling-group-name my-asg \
  --min-size 1 \
  --max-size 10 \
  --desired-capacity 5 \
  --availability-zones us-east-1a us-east-1b us-east-1c \
  --availability-zone-impairment-policy '{
      "ZonalShiftEnabled": true,
      "ImpairedZoneHealthCheckBehavior": IgnoreUnhealthy
    }'
```

Console

Per abilitare lo spostamento zonale su un gruppo esistente (console)

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/e scegli Auto Scaling Groups dal pannello di navigazione.

2. Nella barra di navigazione nella parte superiore dello schermo, scegli il gruppo Auto Scaling in Regione AWS cui hai creato il tuo gruppo Auto Scaling.
3. Seleziona la casella di controllo accanto al gruppo Auto Scaling.

   Si aprirà un riquadro diviso nella parte inferiore della pagina.
4. Nella scheda Integrazioni, in ARC zonal shift, scegli Modifica.
5. Seleziona la casella di controllo per abilitare lo spostamento zonale.
6. Per il comportamento del controllo sanitario, scegli Ignora non salutare o Sostituisci non salutare.

   - Se il comportamento del controllo sanitario è impostato in modo da ignorare le istanze non integre, le istanze non integre non vengono sostituite nella zona di disponibilità con lo spostamento zonale attivo.
   - Se il comportamento del controllo dello stato è impostato per sostituire le istanze non integre, le istanze non integre vengono sostituite nella zona di disponibilità con lo spostamento zonale attivo.
7. Scegliere Aggiorna.

AWS CLI

Per abilitare lo spostamento zonale su un gruppo esistente ()AWS CLI

Aggiungi il parametro `--availability-zone-impairment-policy` al comando update-auto-scaling-group.

Il `--availability-zone-impairment-policy` parametro ha due opzioni:

- ZonalShiftEnabled— Se impostato su`TRUE`, Auto Scaling registra il gruppo Auto Scaling con lo spostamento zonale ARC ed è possibile avviare, aggiornare o annullare uno spostamento zonale sulla console ARC. Se impostato su`FALSE`, Auto Scaling annulla la registrazione del gruppo Auto Scaling dallo spostamento zonale ARC. È necessario che lo spostamento zonale sia già abilitato per impostarlo su. `FALSE`
- ImpairedZoneHealthCheckBehavior— Se impostato su`replace-unhealthy`, le istanze non integre verranno sostituite nella zona di disponibilità con lo spostamento zonale attivo. Se impostato su`ignore-unhealthy`, le istanze non integre non verranno sostituite nella Zona di disponibilità con lo spostamento zonale attivo.

L'esempio seguente abilita lo spostamento zonale sul gruppo Auto Scaling specificato.

```
aws autoscaling update-auto-scaling-group --auto-scaling-group-name my-asg \
  --availability-zone-impairment-policy '{
      "ZonalShiftEnabled": true,
      "ImpairedZoneHealthCheckBehavior": IgnoreUnhealthy
    }'
```

Per iniziare uno spostamento zonale, vedere. Avvio, aggiornamento o annullamento di un turno zonale

Come funziona lo spostamento zonale per i gruppi di Auto Scaling

Supponiamo di avere un gruppo Auto Scaling con le seguenti zone di disponibilità:

- `us-east-1a`
- `us-east-1b`
- `us-east-1c`

Notate dei guasti `us-east-1a` e iniziate un cambiamento di zona. I seguenti comportamenti si verificano quando viene avviato un cambiamento di zona in. `us-east-1a`

- Scalabilità orizzontale: Auto Scaling lancia tutte le nuove richieste di capacità nelle zone **`us-east-1b`** di disponibilità integre (e). `us-east-1c`
- Scaling dinamico: Auto Scaling impedisce alle politiche di scalabilità di ridurre la capacità desiderata. Auto Scaling non impedisce alle politiche di scalabilità di aumentare la capacità desiderata.
- Aggiornamento dell'istanza: l'Auto Scaling estende il timeout per qualsiasi processo di aggiornamento dell'istanza ritardato durante uno spostamento di zona attivo.

Controllo dello stato di salute della zona di disponibilità ridotta (selezione del comportamento)	Comportamento dell'Health check
Sostituisci malsano	Le istanze che sembrano non integre verranno sostituite in tutte le zone di disponibilità (`us-east-1a us-east-1b` , e). `us-east-1c`

Controllo dello stato di salute della zona di disponibilità ridotta (selezione del comportamento)	Comportamento dell'Health check
Ignora non salutari	Le istanze che sembrano non sane verranno sostituite in and. `us-east-1b` `us-east-1c` Le istanze non vengono sostituite nella zona di disponibilità con lo shift zonale attivo (). `us-east-1a`

Le migliori pratiche per l'utilizzo dello spostamento zonale

Per mantenere un'elevata disponibilità delle applicazioni quando si utilizza lo spostamento zonale, si consigliano le seguenti best practice.

- Monitora EventBridge le notifiche per determinare quando si verifica un evento di riduzione della zona di disponibilità in corso. Per ulteriori informazioni, consulta Automating Amazon EC2 Auto Scaling with. EventBridge
- Utilizza politiche di scalabilità con soglie appropriate per assicurarti di avere una capacità sufficiente a tollerare la perdita di una zona di disponibilità.
- Imposta una politica di manutenzione delle istanze con una percentuale minima di integrità di 100. Con questa impostazione, Auto Scaling attende che una nuova istanza sia pronta per l'uso prima di terminare un'istanza non integra.

Per i clienti prescalati, consigliamo inoltre quanto segue:

- Seleziona Ignore unhealthy come comportamento di controllo dello stato di salute per la zona di disponibilità ridotta perché non è necessario sostituire l'istanza non integra durante l'evento di compromissione.
- Usa lo spostamento automatico zonale in ARC per i tuoi gruppi di Auto Scaling. La funzionalità di trasferimento automatico zonale Amazon Application Recovery Controller (ARC) consente di spostare il traffico di una risorsa lontano AWS da una zona di disponibilità quando rileva una compromissione in una zona di disponibilità. AWS Per ulteriori informazioni, consulta Zonal autoshift in ARC.

Ai clienti con sistemi di bilanciamento del carico disattivati tra zone diverse, consigliamo inoltre:

- Utilizza balanced solo per la distribuzione delle zone di disponibilità.
- Se utilizzi lo spostamento zonale sia sul gruppo Auto Scaling che sui sistemi di bilanciamento del carico, assicurati di annullare prima lo spostamento zonale sul gruppo Auto Scaling. Quindi, attendi che la capacità sia bilanciata in tutte le zone di disponibilità prima di annullare lo spostamento zonale sul sistema di bilanciamento del carico.
- A causa della possibilità di uno squilibrio della capacità quando si abilita lo spostamento zonale e si utilizza un sistema di bilanciamento del carico disattivato tra zone, Auto Scaling dispone di una convalida aggiuntiva. Se stai seguendo le migliori pratiche, puoi riconoscere questa possibilità selezionando la casella di controllo in Console di gestione AWS o utilizzando il flag in, o. `skip-zonal-shift-validation` `CreateAutoScalingGroup` `UpdateAutoScalingGroup` `AttachTrafficSources`

Amazon Elastic Kubernetes Service

Amazon EKS offre funzionalità che consentono di rendere le applicazioni più resilienti a eventi come il deterioramento dello stato di salute o il danneggiamento di una zona di disponibilità. Quando esegui i carichi di lavoro in un cluster Amazon EKS, puoi migliorare ulteriormente la tolleranza agli errori e il ripristino delle applicazioni dell'ambiente applicativo utilizzando lo spostamento zonale o lo spostamento automatico di zona.

Utilizzo dello spostamento zonale con Amazon Elastic Kubernetes Service

Per abilitare lo spostamento zonale, utilizza uno dei seguenti metodi. Per ulteriori informazioni, consulta Informazioni sullo spostamento di zona ARC nella Guida per l'utente di Amazon Elastic Kubernetes Service.

Console

Per abilitare lo spostamento zonale su un nuovo cluster Amazon EKS (console)

1. Trova il nome e la regione del cluster Amazon EKS che desideri registrare con ARC.
2. Apri la console Amazon EKS a https://console.aws.amazon.com/eks/home#/clusters.
3. Selezionare il cluster.
4. Nella pagina delle Informazioni sul cluster, seleziona la scheda Panoramica.
5. In Zonal shift, scegli Gestisci.

6. Per EKS Zonal Shift, scegli Abilita o Disabilita.

AWS CLI

Per abilitare lo spostamento zonale su un nuovo cluster Amazon EKS ()AWS CLI

- Immetti il comando seguente:

```
aws eks create-cluster --name my-eks-cluster --role-
arn my-role-arn-to-create-cluster --resources-vpc-config
 subnetIds=string,string,securityGroupIds=string,string,endpointPublicAccess=boolean,end
 --zonal-shift-config enabled=true
```

Per abilitare lo spostamento zonale su un cluster Amazon EKS esistente ()AWS CLI

- Immetti il comando seguente:

```
aws eks update-cluster-config --name my-eks-cluster --zonal-shift-config
 enabled=true
```

Puoi avviare uno spostamento di zona per un cluster Amazon EKS oppure puoi consentire di farlo AWS per te abilitando lo spostamento automatico di zona. Dopo aver abilitato lo spostamento zonale del cluster Amazon EKS con ARC, puoi avviare uno spostamento zonale o abilitare lo spostamento automatico di zona utilizzando la console ARC, la AWS CLI o lo spostamento zonale e lo spostamento automatico zonale. APIs

Per ulteriori informazioni sull'avvio di un cambiamento zonale, consulta. Avvio, aggiornamento o annullamento di un turno zonale

Per ulteriori informazioni sull'abilitazione di Amazon EKS con zonal shift, consulta Informazioni su ARC Zonal Shift in Amazon EKS nella Amazon Elastic Kubernetes Service User Guide.

Come funziona il cambiamento di zona per Amazon Elastic Kubernetes Service

Durante un turno di zona di Amazon EKS, avviene automaticamente quanto segue:

- Tutti i nodi della zona AZ interessata sono isolati. Ciò impedisce a Kubernetes Scheduler di pianificare nuovi Pod sui nodi in una zona AZ non integra.

- Se utilizzi i gruppi di nodi gestiti, il ribilanciamento delle zone di disponibilità viene sospeso e il gruppo Auto Scaling viene aggiornato per garantire che i nuovi nodi del piano dati Amazon EKS vengano lanciati solo in condizioni ottimali. AZs
- I nodi della zona AZ non integra non vengono terminati e i Pod non vengono rimossi da questi nodi. Questo serve a garantire che, quando un turno di zona scade o viene annullato, il traffico possa essere reindirizzato in tutta sicurezza alla zona che ha ancora la piena capacità.
- Il EndpointSlice controller trova tutti gli endpoint Pod nella zona AZ compromessa e li rimuove dalla zona interessata. EndpointSlices Ciò garantisce che solo gli endpoint Pod integri AZs siano destinati a ricevere il traffico di rete. Quando uno spostamento di zona viene annullato o scade, il EndpointSlice controller lo aggiorna EndpointSlices per includere gli endpoint nella AZ ripristinata.

Per ulteriori informazioni, consulta il blog Containers.AWS

Application Load Balancer

Utilizzo dello spostamento zonale per Application Load Balancer

Per utilizzare Application Load Balancer con zonal shift, è necessario abilitare l'integrazione ARC zonal shift negli attributi di Application Load Balancer. Application Load Balancer supporta lo spostamento zonale con configurazioni abilitate o disattivate tra zone.

Prima di abilitare l'integrazione ARC e iniziare a utilizzare lo spostamento zonale, esaminate le seguenti informazioni:

- È possibile avviare uno spostamento zonale per uno specifico sistema di bilanciamento del carico solo per una singola zona di disponibilità. Non è possibile avviare uno spostamento zonale per più zone di disponibilità.
- AWS rimuove in modo proattivo gli indirizzi IP del sistema di bilanciamento del carico zonale dal DNS quando più problemi di infrastruttura influiscono sui servizi. Verificare sempre l'attuale capacità della zona di disponibilità prima di avviare uno spostamento zonale.
- Lo spostamento zonale non funzionerà per i gruppi target Single-AZ.
- Quando un Application Load Balancer è una destinazione di un Network Load Balancer, avviare sempre lo spostamento zonale dal Network Load Balancer. Se si avvia uno spostamento zonale dall'Application Load Balancer, il Network Load Balancer non riconoscerà lo spostamento e continuerà a inviare traffico all'Application Load Balancer.

Puoi avviare uno spostamento di zona per un sistema di bilanciamento del carico nella console Elastic Load Balancing (nella Regioni AWS maggior parte dei casi) o nella console ARC.

Console

Per abilitare lo spostamento zonale su un sistema di bilanciamento del carico (console)

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nella pagina di navigazione, in Load balancing, scegli Load balancers.
3. Seleziona il nome dell'Application Load Balancer.
4. Nella scheda Attributi, fate clic su Modifica.
5. Nella configurazione del routing della zona di disponibilità, per l'integrazione con >ARC zonal shift, scegli Abilita.
6. Scegli Save (Salva).

AWS CLI

Per abilitare lo spostamento zonale su un sistema di bilanciamento del carico ()AWS CLI

- Immetti il comando seguente:

```
aws elbv2 modify-load-balancer-attributes --load-balancer-arn my-alb-arn --
attributes Key=zonal_shift.config.enabled,Value=true
```

Per ulteriori informazioni sull'avvio di un cambiamento di zona, vedere. Avvio, aggiornamento o annullamento di un turno zonale

È possibile utilizzare l'`keepalive`opzione per configurare la durata delle connessioni. Per ulteriori informazioni, consulta la durata del client HTTP keepalive nella Guida per l'utente di Application Load Balancer. Per impostazione predefinita, Application Load Balancer impostano il valore di durata keepalive del client HTTP su 3600 secondi o 1 ora. Ti consigliamo di abbassare il valore in modo che sia in linea con l'obiettivo del tempo di ripristino per l'applicazione, ad esempio 300 secondi. Quando scegli la durata di keepalive di un client HTTP, considera che questo valore rappresenta un compromesso tra la riconnessione più frequente in generale, il che può influire sulla latenza, e lo spostamento più rapido di tutti i client da una zona o regione compromessa.

Come funziona lo spostamento zonale per Application Load Balancer

Quando viene avviato uno spostamento di zona su un Application Load Balancer con il bilanciamento del carico tra zone abilitato, tutto il traffico verso le destinazioni viene bloccato nella zona di disponibilità interessata e lo spostamento zonale rimuove l'indirizzo IP zonale dal DNS.

Per ulteriori informazioni, consulta Integrazioni per il tuo Application Load Balancer nella Application Load Balancer User Guide.

Network Load Balancers

Utilizzo dello spostamento zonale per Network Load Balancer

Per utilizzare Network Load Balancer con zonal shift, è necessario abilitare l'integrazione ARC zonal shift negli attributi Network Load Balancer. Network Load Balancer supporta lo spostamento zonale con configurazioni abilitate o disattivate tra zone.

Puoi scegliere quali risorse attivare per utilizzare lo spostamento zonale e lo spostamento automatico di zona e quando rinunciare a una zona di disponibilità ridotta. Sono supportati sia i Network Load Balancer con accesso a Internet che quelli interni.

Per abilitare lo spostamento zonale per il Network Load Balancer abilitato tra zone, tutti i gruppi target collegati al load balancer devono soddisfare i seguenti requisiti.

- Il bilanciamento del carico tra zone deve essere abilitato o impostato su. `use_load_balancer_configuration`
  - Per ulteriori informazioni sul bilanciamento del carico tra le zone del gruppo target, consulta Bilanciamento del carico tra zone per gruppi target.
- Il protocollo del gruppo target deve essere TCP o TLS.
  - Per ulteriori informazioni sui protocolli del gruppo target di Network Load Balancer, vedere Configurazione del routing.
- L'interruzione della connessione per destinazioni non integre deve essere disabilitata.
  - Per ulteriori informazioni sull'interruzione della connessione del gruppo target, vedere Interruzione della connessione per destinazioni non integre.
- Il gruppo target non deve avere come target alcun Application Load Balancer.
  - Per ulteriori informazioni sugli Application Load Balancer come destinazioni, consulta Utilizzare Application Load Balancer come destinazioni di un Network Load Balancer.

Puoi avviare uno spostamento di zona per un Network Load Balancer utilizzando AWS CLI il, il o Console di gestione AWS il widget Elastic Load Balancing. Quando un Application Load Balancer è l'obiettivo di un Network Load Balancer, è necessario avviare lo spostamento zonale dal Network Load Balancer. Se si avvia lo spostamento di zona dall'Application Load Balancer, il Network Load Balancer non interromperà l'invio di traffico all'Application Load Balancer e ai suoi obiettivi.

Console

Per abilitare lo spostamento zonale su un sistema di bilanciamento del carico (console)

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nella pagina di navigazione, in Load balancing, scegli Load balancers.
3. Seleziona il nome del Network Load Balancer.
4. Nella scheda Attributi, scegli Modifica.
5. Nella configurazione del routing della zona di disponibilità, per l'integrazione con ARC zonal shift, scegli Abilita.
6. Scegli Save (Salva).

AWS CLI

Per abilitare lo spostamento zonale su un sistema di bilanciamento del carico ()AWS CLI

- Immetti il comando seguente:

```
aws elbv2 modify-load-balancer-attributes --load-balancer-arn my-nlb-arn --
attributes Key=zonal_shift.config.enabled,Value=true
```

Per ulteriori informazioni sull'avvio di un cambiamento di zona, vedere. Avvio, aggiornamento o annullamento di un turno zonale

Come funziona lo spostamento zonale per Network Load Balancer

ARC crea un errore di controllo dello stato per il Network Load Balancer registrato in modo che il nodo Network Load Balancer nella zona AZ compromessa venga rimosso dal DNS quando si avvia uno spostamento di zona. Il Network Load Balancer disabilita le destinazioni nella zona interessata in modo che smettano di ricevere traffico, mentre Elastic Load Balancing considera queste destinazioni come destinazioni disabilitate per lo spostamento di zona. Gli obiettivi nello

stato disabilitato continuano a ricevere controlli di integrità. Quando gli obiettivi sono integri e lo spostamento zonale scade (o viene annullato), riprende il routing verso gli obiettivi nella zona precedentemente compromessa.

Durante lo spostamento zonale sui Network Load Balancer con bilanciamento del carico tra zone abilitato, gli indirizzi IP dei sistemi di bilanciamento del carico zonale vengono rimossi dal DNS. Le connessioni esistenti alle destinazioni nella zona di disponibilità ridotta persistono fino alla chiusura organica, mentre le nuove connessioni non vengono più instradate verso destinazioni nella zona di disponibilità ridotta.

Per ulteriori informazioni, consulta Zonal Shift for your Network Load Balancer nella Network Load Balancer User Guide.

Avvio, aggiornamento o annullamento di un turno zonale

Questa sezione fornisce le procedure per lavorare con i turni zonali, tra cui l'avvio di un turno zonale e l'annullamento di un turno zonale.

Starting a zonal shift

I passaggi di questa sezione spiegano come avviare un cambiamento di zona avviato dal cliente sulla console Amazon Application Recovery Controller (ARC). Per utilizzare lo spostamento zonale a livello di codice, consulta la Zonal Shift API Reference Guide.

Oltre ad avviare uno spostamento zonale in ARC, puoi anche avviare uno spostamento zonale per un sistema di bilanciamento del carico nella console Elastic Load Balancing (nelle regioni supportate). Per ulteriori informazioni, consulta Zonal shift nella Elastic Load Balancing User Guide.

Per iniziare un cambiamento zonale

1. Apri la console ARC all'indirizzohttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. In Multi-AZ, scegli Spostamento zonale.
3. Nella pagina Spostamento zonale, scegli Avvia spostamento zonale.
4. Seleziona la zona di disponibilità da cui desideri allontanare il traffico.
5. Seleziona una risorsa supportata dalla tabella Risorse per cui allontanare il traffico.
6. Per Imposta la scadenza del turno zonale, scegli o inserisci una scadenza per il turno zonale. Un turno zonale può essere impostato per essere attivo inizialmente per 1 minuto o fino a tre giorni (72 ore).

Tutti gli spostamenti zonali sono temporanei. È necessario impostare una scadenza, ma è possibile aggiornare i turni attivi in un secondo momento per impostare un nuovo periodo di scadenza fino a tre giorni.

7. Inserire un commento. Se lo si desidera, è possibile aggiornare lo spostamento zonale in un secondo momento e modificare il commento.
8. Seleziona la casella di controllo per confermare che l'avvio di un turno zonale ridurrà la capacità disponibile per l'applicazione, allontanando il traffico dalla zona di disponibilità.
9. Scegli Avvia.

Updating or canceling a zonal shift

I passaggi di questa sezione spiegano come aggiornare un cambiamento zonale avviato o annullare uno spostamento zonale sulla console Amazon Application Recovery Controller (ARC). Per utilizzare lo spostamento zonale a livello di codice, consulta la Zonal Shift API Reference Guide.

Puoi aggiornare un turno zonale per impostare una nuova scadenza oppure modificare o sostituire il commento per il turno zonale. Puoi annullare uno spostamento zonale in qualsiasi momento prima della scadenza.

È possibile annullare i turni zonali avviati dall'utente o i turni zonali iniziati per una risorsa per un'esercitazione relativa AWS allo spostamento automatico zonale. Per ulteriori informazioni sui turni di pratica in Zonal Autoshift, consulta. Come funzionano gli autoshift e le esecuzioni pratiche zonali

Per aggiornare uno spostamento zonale

1. Apri la console ARC all'indirizzohttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. In Multi-AZ, scegli Spostamento zonale.
3. Seleziona uno spostamento zonale che desideri aggiornare, quindi scegli Aggiorna spostamento zonale.
4. Per Imposta scadenza dello spostamento zonale, seleziona o inserire facoltativamente una scadenza.
5. Per Commento, modificare il commento esistente o inserire un nuovo commento facoltativamente.
6. Scegliere Aggiorna.

Per annullare uno spostamento zonale

1. Apri la console ARC all'indirizzohttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. In Multi-AZ, scegli Spostamento zonale.
3. Seleziona uno spostamento zonale che desideri annullare, quindi scegli Annulla spostamento zonale.
4. Nella finestra di dialogo modale di conferma, scegliete Conferma.

Registrazione e monitoraggio per lo spostamento di zona in Amazon Application Recovery Controller (ARC)

Puoi utilizzarlo AWS CloudTrail per monitorare lo spostamento di zona in Amazon Application Recovery Controller (ARC), per analizzare i modelli e aiutare a risolvere i problemi.

Argomenti

- Registrazione delle chiamate API zonal shift utilizzando AWS CloudTrail

Registrazione delle chiamate API zonal shift utilizzando AWS CloudTrail

Zonal shift for ARC è integrato con AWS CloudTrail, un servizio che fornisce una registrazione delle azioni intraprese da un utente, ruolo o AWS servizio in ARC. CloudTrail acquisisce tutte le chiamate API per lo spostamento di zona come eventi. Le chiamate acquisite includono chiamate dalla console ARC e chiamate in codice alle operazioni dell'API ARC per lo spostamento di zona.

Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per lo spostamento zonale. 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, è possibile determinare la richiesta di spostamento di zona inoltrata ad ARC, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e altri dettagli.

Per ulteriori informazioni CloudTrail, consulta la Guida per l'AWS CloudTrail utente.

Informazioni sullo spostamento zonale in CloudTrail

CloudTrail è abilitato sul tuo Account AWS quando crei l'account. Quando si verifica un'attività in ARC per uno spostamento di zona, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi di AWS servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare eventi recenti in. Account AWS Per ulteriori informazioni, consulta Lavorare con la cronologia CloudTrail degli eventi.

Per una registrazione continua degli eventi del tuo Account AWS, compresi gli eventi relativi al cambiamento di zona in ARC, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando si crea un percorso nella console, questo sarà valido in tutte le Regioni AWS. Il trail registra gli eventi di tutte le regioni della AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica della creazione di un percorso
- CloudTrail servizi e integrazioni supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di CloudTrail registro da più regioni e ricezione di file di CloudTrail registro da più account

Tutte le azioni ARC vengono registrate CloudTrail e documentate nella Routing Control API Reference Guide for Amazon Application Recovery Controller. Ad esempio, le chiamate alle `ListManagedResources` azioni `StartZonalShift` e generano voci nei file di registro. CloudTrail

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con credenziali utente root o AWS Identity and Access Management (IAM).
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro AWS servizio.

Per ulteriori informazioni, consulta Elemento CloudTrail userIdentity.

Visualizzazione degli eventi ARC nella cronologia degli eventi

CloudTrail consente di visualizzare gli eventi recenti nella cronologia degli eventi. Per ulteriori informazioni, consulta Lavorare con la cronologia degli CloudTrail eventi nella Guida AWS CloudTrail per l'utente.

Comprensione delle voci del file di registro dei turni zonali

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'`ListManagedResources`azione per lo spostamento zonale.


```
{
      "eventVersion": "1.08",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:role/admin",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "sessionIssuer": {
            "type": "Role",
            "principalId": "AROA33L3W36EXAMPLE",
            "arn": "arn:aws:iam::111122223333:role/admin",
            "accountId": "111122223333",
            "userName": "EXAMPLENAME"
          },
          "webIdFederationData": {},
          "attributes": {
            "creationDate": "2022-11-14T16:01:51Z",
            "mfaAuthenticated": "false"
          }
        }
      },
      "eventTime": "2022-11-14T16:14:41Z",
```

```
      "eventSource": "arc-zonal-shift.amazonaws.com",
      "eventName": "ListManagedResources",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.50",
      "userAgent": "Boto3/1.17.101 Python/3.8.10 Linux/4.14.231-180.360.amzn2.x86_64
 exec-env/AWS_Lambda_python3.8 Botocore/1.20.102",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "VGXG4ZUE7UZTVCMTJGIAF_EXAMPLE",
      "eventID": "4b5c42df-1174-46c8-be99-d67_EXAMPLE",
      "readOnly": true,
      "eventType": "AwsApiCall",
      "managementEvent": true,
      "recipientAccountId": "111122223333"
      "eventCategory": "Management"
      }
    }
```

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'`StartZonalShift`azione con un'eccezione di conflitto per lo spostamento zonale.

```
{
      "eventVersion": "1.08",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:role/admin",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "sessionIssuer": {
            "type": "Role",
            "principalId": "AROA33L3W36EXAMPLE",
            "arn": "arn:aws:iam::111122223333:role/admin",
            "accountId": "111122223333",
            "userName": "EXAMPLENAME"
          },
          "webIdFederationData": {},
          "attributes": {
            "creationDate": "2022-11-14T16:01:51Z",
            "mfaAuthenticated": "false"
          }
        }
```

```
      },
      "eventTime": "2022-11-14T16:10:38Z",
      "eventSource": "arc-zonal-shift.amazonaws.com",
      "eventName": "StartZonalShift",
     "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.50",
      "userAgent": "Boto3/1.17.101 Python/3.8.10 Linux/4.14.231-180.360.amzn2.x86_64
 exec-env/AWS_Lambda_python3.8 Botocore/1.20.102",
      "errorCode": "ConflictException",
      "errorMessage": "There's already an active zonal shift for that resource
 identifier: 'arn:aws:testservice:us-west-2:077059137270:testResource/456apples'.
 Active zonal shift: 'bac23b74-176e-c073-de8f-484ca508910f'",
      "requestParameters": {
        "resourceIdentifier": "arn:aws:testservice:us-
west-2:077059137270:testResource/456apples",
        "awayFrom": "usw2-az1",
        "expiresIn": "2m",
        "comment": "HIDDEN_FOR_SECURITY_REASONS"
      },
      "responseElements": null,
      "requestID": "OP4OYXZ54HUPMIPGWH_EXAMPLE",
      "eventID": "0bca6660-e999-43a5-9008-EXAMPLE",
      "readOnly": false,
      "eventType": "AwsApiCall",
      "managementEvent": true,
      "recipientAccountId": "111122223333"
      "eventCategory": "Management"
      }
    }
```

Identity and Access Management per il cambiamento di zona in ARC

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 le risorse ARC. IAM è uno Servizio AWS strumento che puoi utilizzare senza costi aggiuntivi.

Indice

- Come funziona il cambio di zona con IAM
- IAM e autorizzazioni per lo spostamento zonale

- Esempi di politiche basate sull'identità per il cambiamento di zona in ARC

Come funziona il cambio di zona con IAM

Prima di utilizzare IAM per gestire l'accesso allo spostamento zonale in Amazon Application Recovery Controller (ARC), scopri quali funzionalità IAM sono disponibili per l'uso con lo spostamento zonale.

Funzionalità IAM che puoi utilizzare con lo spostamento zonale

Funzionalità IAM	Supporto per turni zonali
Policy basate sull'identità	Sì
Policy basate su risorse	No
Operazioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione delle policy	Sì
ACLs	No
ABAC (tag nelle policy)	Parziale
Credenziali temporanee	Sì
Autorizzazioni del principale	Sì
Ruoli di servizio	No
Ruoli collegati al servizio	Sì

Per avere una panoramica generale di alto livello su come AWS i 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 ARC

Supporta le policy basate sull'identità: sì

Le policy basate sull'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 di IAM.

Con le policy basate sull'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. 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 IAM.

Per visualizzare esempi di politiche basate sull'identità ARC, vedere. Esempi di policy basate sull'identità in Amazon Application Recovery Controller (ARC)

Politiche basate sulle risorse all'interno di ARC

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 di 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.

Azioni politiche per il cambiamento zonale

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

Per visualizzare un elenco di azioni ARC per lo spostamento di zona, consulta Azioni definite da Amazon Route 53 Zonal Shift nel Service Authorization Reference.

Le azioni politiche in ARC per lo spostamento zonale utilizzano i seguenti prefissi prima dell'azione:

```
arc-zonal-shift
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola. Ad esempio, quanto segue:

```
"Action": [
      "arc-zonal-shift:action1",
      "arc-zonal-shift:action2"
         ]
```

È possibile specificare più azioni tramite caratteri jolly (*). Ad esempio, per specificare tutte le azioni che iniziano con la parola `Describe`, includi la seguente azione:

```
"Action": "arc-zonal-shift:Describe*"
```

Per visualizzare esempi di politiche basate sull'identità ARC per il cambiamento di zona, vedere. Esempi di politiche basate sull'identità per il cambiamento di zona in ARC

Risorse politiche per il cambiamento zonale

Supporta le risorse relative alle policy: sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità 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. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). Per le azioni che non supportano le autorizzazioni a livello di risorsa, si utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

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

Per visualizzare un elenco dei tipi di risorse e delle relative ARNs azioni e le azioni che è possibile specificare con l'ARN di ciascuna risorsa, vedere il seguente argomento nel Service Authorization Reference:

- Azioni definite da Amazon Route 53 - Zonal Shift

Per visualizzare le azioni e le risorse che puoi utilizzare con una chiave di condizione, consulta il seguente argomento nel Service Authorization Reference:

- Chiavi di condizione definite da Amazon Route 53 - Zonal Shift

Per visualizzare esempi di politiche ARC basate sull'identità per lo spostamento di zona, consulta. Esempi di politiche basate sull'identità per il cambiamento di zona in ARC

Chiavi delle condizioni politiche per lo spostamento zonale

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 entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento `Condition` specifica quando le istruzioni vengono eseguite in base a criteri definiti. 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. 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 dello spostamento zonale, consulta il seguente argomento nel Service Authorization Reference:

- Chiavi di condizione definite da Amazon Route 53 - Zonal Shift

Per visualizzare le azioni e le risorse che puoi utilizzare con una chiave di condizione, consulta i seguenti argomenti nel Service Authorization Reference:

- Azioni definite da Amazon Route 53 - Zonal Shift
- Tipi di risorse definiti da Amazon Route 53 - Zonal Shift

Per visualizzare esempi di politiche ARC basate sull'identità per lo spostamento di zona, consulta. Esempi di politiche basate sull'identità per il cambiamento di zona in ARC

Liste di controllo degli accessi () in ARC ACLs

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.

Controllo degli accessi basato sugli attributi (ABAC) con ARC

Supporta ABAC (tag nelle policy): parzialmente

Il controllo degli accessi basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi, chiamati tag. Puoi allegare tag a entità e AWS risorse IAM, quindi progettare politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag sulla risorsa.

Per controllare l'accesso basato su tag, fornire 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 Sì. Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per maggiori informazioni su ABAC, consulta Definizione delle autorizzazioni con autorizzazione ABAC nella Guida per l'utente di 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.

ARC include il seguente supporto parziale per ABAC:

- Zonal shift supporta ABAC per le risorse gestite registrate in ARC per lo spostamento zonale. Per ulteriori informazioni sulle risorse gestite di ABAC for Network Load Balancer e Application Load Balancer, consulta ABAC with Elastic Load Balancing nella Elastic Load Balancing User Guide.

Utilizzo di credenziali temporanee con ARC

Supporta le credenziali temporanee: sì

Le credenziali temporanee forniscono un accesso a breve termine alle AWS risorse e vengono create automaticamente quando si utilizza la federazione o si cambia ruolo. AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza temporanee in IAM e Servizi AWS compatibili con IAM nella Guida per l'utente IAM.

Autorizzazioni principali multiservizio per ARC

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

Quando utilizzi un'entità IAM (utente o ruolo) per eseguire azioni AWS, sei considerato un principale. Le policy concedono autorizzazioni a un'entità. Quando si utilizzano alcuni servizi, è possibile

eseguire un'azione che attiva un'altra azione in un servizio diverso. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni.

Per vedere se un'azione richiede azioni dipendenti aggiuntive in una policy, consulta il seguente argomento nel Service Authorization Reference:

- Spostamento zonale Amazon Route 53

Ruoli di servizio per ARC

Supporta i ruoli di servizio: no

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 Create a role to delegate permissions to an Servizio AWS nella Guida per l'utente IAM.

Ruoli collegati ai servizi per ARC

Supporta i ruoli collegati ai servizi: sì

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'operazione 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 al servizio, ma non modificarle.

Lo spostamento zonale non utilizza ruoli collegati al servizio.

IAM e autorizzazioni per lo spostamento zonale

Questa sezione fornisce informazioni aggiuntive su come funzionano le autorizzazioni per la funzionalità di spostamento zonale in Amazon Application Recovery Controller (ARC), specialmente se utilizzi la funzionalità di un altro AWS servizio, come Elastic Load Balancing. Per scoprire come le funzionalità ARC funzionano con IAM e le autorizzazioni in generale, consulta le informazioni nell'argomento di panoramica,. Identity and Access Management per il cambiamento di zona in ARC

Zonal shift supporta Application Load Balancer, Network Load Balancer, gruppi Amazon EC2 Auto Scaling e Amazon EKS. Puoi utilizzare le chiavi delle condizioni IAM per definire una politica di autorizzazione IAM per queste risorse. Di seguito è riportato un esempio di policy che utilizza una chiave di condizione con più risorse di diverso tipo:

```
{
    "Condition": {
        "StringLike": {
            "arc-zonal-shift:ResourceIdentifier": [
                "arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/net/
*",
                "arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/app/
*",
                "arn:aws:eks:us-east-1:123456789012:cluster/*"
            ]
        }
    },
    "Action": [
        "arc-zonal-shift:StartZonalShift"
    ],
    "Resource": "*",
    "Effect": "Allow"
}
```

Per ulteriori informazioni, consulta Risorse supportate.

Oltre alle autorizzazioni descritte nell'argomento di panoramica su IAM, quanto segue si applica allo spostamento di zona per IAM e alle autorizzazioni:

- Assicurati di disporre delle autorizzazioni necessarie per lavorare con lo spostamento zonale in ARC. Per ulteriori informazioni, vedere Zonal Shift Console Access e Zonal Shift Operations Access.
- Non è necessario aggiungere ulteriori autorizzazioni Elastic Load Balancing con IAM per utilizzare i turni zonali per le risorse gestite di bilanciamento del carico nel proprio account in ARC.
- Una policy AWS gestita che fornisce l'accesso completo a Elastic Load Balancing include le autorizzazioni per lavorare con i turni zonali. Se utilizzi policy AWS gestite per l'accesso a Elastic Load Balancing, non sono necessarie autorizzazioni aggiuntive in IAM for zonal shift per avviare turni zonali per i sistemi di bilanciamento del carico o utilizzarli nella console Elastic Load Balancing. Per ulteriori informazioni, consulta le politiche AWS gestite per Elastic Load Balancing.

Esempi di politiche basate sull'identità per il cambiamento di zona in ARC

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare risorse ARC. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM.

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 di IAM.

Per dettagli sulle azioni e sui tipi di risorse definiti da ARC, incluso il formato di ARNs per ogni tipo di risorsa, consulta Azioni, risorse e chiavi di condizione per Amazon Application Recovery Controller (ARC) nel Service Authorization Reference.

Argomenti

- Best practice per le policy
- Esempio: accesso alla console a turni zonali
- Esempio: azioni dell'API Zonal Shift

Best practice per le policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare le risorse ARC nel tuo account. Queste azioni possono comportare costi aggiuntivi per l' Account AWS. Quando si creano o modificano policy basate sull'identità, seguire 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 maggiori informazioni, consulta Policy gestite da AWS o Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente di IAM.
- Applicazione delle autorizzazioni con privilegio minimo - Quando si impostano le autorizzazioni con le policy IAM, concedere 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 privilegio minimo. Per maggiori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente di IAM.

- Condizioni d’uso nelle policy IAM per limitare ulteriormente l’accesso - Per limitare l’accesso ad azioni e risorse è possibile aggiungere una condizione alle 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 CloudFormation. Per maggiori informazioni, consultare la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l’utente di IAM.
- Utilizzo dello strumento di analisi degli accessi IAM per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali - Lo strumento di analisi degli accessi IAM convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio (JSON) della policy IAM e alle best practice di IAM. Lo strumento di analisi degli accessi IAM offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per maggiori informazioni, consultare Convalida delle policy per il Sistema di analisi degli accessi IAM nella Guida per l’utente di 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, aggiungere le condizioni MFA alle policy. Per maggiori informazioni, consultare Protezione dell’accesso API con MFA nella Guida per l’utente di IAM.

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

Esempio: accesso alla console a turni zonali

Per accedere alla console Amazon Application Recovery Controller (ARC), devi disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle risorse ARC 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 agli utenti che effettuano chiamate solo verso AWS CLI o l' AWS API. Al contrario, è opportuno concedere l’accesso solo alle azioni che corrispondono all’operazione API che stanno cercando di eseguire.

Per consentire agli utenti l'accesso completo all'utilizzo di zonal shift in Console di gestione AWS, allega all'utente una policy come la seguente:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                   "arc-zonal-shift:ListManagedResources",
                   "arc-zonal-shift:GetManagedResource",
                   "arc-zonal-shift:ListZonalShifts",
                   "arc-zonal-shift:StartZonalShift",
                   "arc-zonal-shift:UpdateZonalShift",
                   "arc-zonal-shift:CancelZonalShift"
             ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeAvailabilityZones",
            "Resource": "*"
        }
    ]
}
```

Esempio: azioni dell'API Zonal Shift

L'API zonal shift allontana temporaneamente il traffico da una zona di disponibilità per ripristinare un'applicazione.

Per garantire che un utente possa utilizzare le azioni dell'API zonal shift, allega una policy che corrisponda alle operazioni API con cui l'utente deve lavorare, come le seguenti:

JSON

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

```
            "Action": [
                  "arc-zonal-shift:ListManagedResources",
                  "arc-zonal-shift:GetManagedResource",
                  "arc-zonal-shift:ListZonalShifts",
                  "arc-zonal-shift:StartZonalShift",
                  "arc-zonal-shift:UpdateZonalShift",
                  "arc-zonal-shift:CancelZonalShift"
             ],
            "Resource": "*"
        }
    ]
}
```

Zonal autoshift in ARC

Con lo spostamento automatico zonale, autorizzi AWS a spostare il traffico di risorse di un'applicazione da una zona di disponibilità (AZ) durante gli eventi, per tuo conto, per ridurre i tempi di ripristino. AWS avvia uno spostamento automatico quando la telemetria interna indica che esiste un problema nella zona di disponibilità che potrebbe avere un impatto potenziale sui clienti. Quando AWS inizia uno spostamento automatico, il traffico delle applicazioni verso le risorse che hai configurato per lo spostamento automatico zonale inizia a spostarsi dalla zona di disponibilità.

Tieni presente che ARC non controlla lo stato delle singole risorse. AWS avvia uno spostamento automatico quando la AWS telemetria rileva che esiste una limitazione della zona di disponibilità che potrebbe avere un impatto sui clienti. In alcuni casi, il traffico potrebbe essere spostato verso risorse che non subiscono alcun impatto.

Con lo spostamento automatico zonale, autorizzi anche AWS a spostare il traffico di risorse di un'applicazione da una zona di disponibilità, per tuo conto, per le normali sessioni di pratica. Le prove pratiche sono necessarie per lo spostamento automatico zonale. I cambiamenti zonali che ARC avvia per le esercitazioni pratiche aiutano a garantire che lo spostamento del traffico da una zona di disponibilità durante un trasferimento automatico sia sicuro per l'applicazione. La pratica viene eseguita regolarmente per verificare che l'applicazione possa funzionare normalmente senza una zona di disponibilità avviando turni zonali che spostano il traffico di una risorsa lontano da una zona di disponibilità. Le esercitazioni si svolgono settimanalmente e forniscono un risultato, ad esempio `SUCCEEDED` o, che consente di `FAILED` capire se l'applicazione funziona come previsto.

> **Important**
>
> Prima di configurare le sessioni pratiche o abilitare lo spostamento automatico zonale, si consiglia vivamente di predimensionare la capacità delle risorse applicative in tutte le zone di disponibilità della regione in cui vengono distribuite le risorse applicative. Non dovreste fare affidamento sulla scalabilità su richiesta all'avvio di un cambio automatico o di un'esecuzione pratica. Lo spostamento automatico zonale, incluse le esercitazioni, funziona in modo indipendente e non attende il completamento delle azioni di ridimensionamento automatico. Affidarsi alla scalabilità automatica, anziché alla prescalabilità, può richiedere più tempo per il ripristino dell'applicazione.
>
> Se utilizzi la scalabilità automatica per gestire cicli di traffico regolari, ti consigliamo vivamente di configurare la capacità minima della scalabilità automatica per continuare a funzionare normalmente con la perdita di una zona di disponibilità.

Se prevedi di abilitare lo spostamento automatico zonale o configurare le sessioni pratiche, dopo aver predimensionato la capacità delle risorse dell'applicazione, verifica che l'applicazione possa funzionare normalmente senza una zona di disponibilità. Per verificarlo, avviate uno spostamento zonale per spostare il traffico di una risorsa lontano da una zona di disponibilità.

Dopo aver abilitato lo spostamento automatico zonale, ti consigliamo di verificare, avviando e valutando una pratica on-demand run zonal shift, che l'applicazione possa continuare a funzionare normalmente con il traffico spostato lontano da una zona di disponibilità. Quindi, le normali procedure eseguite da ARC consentono di confermare, su base continuativa, di disporre di una capacità sufficiente per un trasferimento automatico.

Per garantire che i test con spostamento zonale siano efficaci, è importante verificare che il traffico si esaurisca come previsto dalla zona di residenza da cui ci si allontana. Ad esempio, sia Application Load Balancer che Network Load Balancer forniscono metriche per AZ in Amazon CloudWatch che puoi utilizzare per monitorare questa situazione. A seconda del periodo di riutilizzo delle connessioni da parte del servizio e dei client, il traffico potrebbe continuare verso la zona dalla quale ti sei allontanato più a lungo del previsto. Per ulteriori informazioni, consulta Limita il tempo in cui i client rimangono connessi ai tuoi endpoint.

Puoi abilitare lo spostamento automatico zonale, per una risorsa supportata, nella console ARC. Oppure, nella console Amazon EC2, hai la possibilità di abilitare lo spostamento automatico zonale per una risorsa di bilanciamento del carico specifica. Per ulteriori informazioni sull'attivazione dello

spostamento automatico di zona con Elastic Load Balancing, consulta Zonal shift nella Elastic Load Balancing User Guide.

Gli spostamenti automatici e i turni zonali per la corsa pratica sono temporanei. Con gli spostamenti automatici, quando la zona di disponibilità interessata viene ripristinata, interrompe lo spostamento del traffico destinato alle risorse lontano dalla zona di disponibilità. AWS Il traffico delle applicazioni per i clienti ritorna in tutte le zone di disponibilità della regione. Con un'esecuzione pratica, il traffico viene spostato da una zona di disponibilità a una singola risorsa per circa 30 minuti, quindi reindirizzato verso tutte le zone di disponibilità della regione.

Puoi configurare EventBridge le notifiche di Amazon per avvisarti dei cambi automatici e delle sessioni di pratica. Per ulteriori informazioni, consulta Utilizzo dello spostamento automatico zonale con Amazon EventBridge.

Come funzionano gli autoshift e le esecuzioni pratiche zonali

La funzionalità di trasferimento automatico zonale di Amazon Application Recovery Controller (ARC) consente di AWS spostare il traffico di una risorsa lontano da una zona di disponibilità, per tuo conto, quando si AWS determina che c'è una compromissione che potrebbe potenzialmente influire sui clienti nella zona di disponibilità. L'autoshift zonale è progettato per una risorsa predimensionata in tutte le zone di disponibilità di una Regione AWS, in modo che un'applicazione possa funzionare normalmente con la perdita di una zona di disponibilità.

Con l'autoshift zonale, è necessario configurare le sessioni pratiche, in cui ARC sposta regolarmente il traffico relativo alla risorsa lontano da una zona di disponibilità. ARC pianifica le esercitazioni circa settimanali per ogni risorsa a cui è associata una configurazione di esecuzione pratica. Le esercitazioni per ogni risorsa sono programmate in modo indipendente.

Per ogni esercitazione, ARC registra un risultato. Se un'esercitazione viene interrotta da una condizione di blocco, l'esito dell'esercitazione non viene contrassegnato come riuscito. Per ulteriori informazioni sui risultati delle esercitazioni, vedi Risultati delle esercitazioni.

Puoi configurare EventBridge le notifiche di Amazon per inviarti informazioni sugli spostamenti automatici e sulle sessioni di pratica. Per ulteriori informazioni, consulta Utilizzo dello spostamento automatico zonale con Amazon EventBridge.

Indice

- Informazioni su zonal autoshift
- Quando avvia AWS e arresta i cambi automatici

- Quando ARC pianifica, avvia e termina, le esercitazioni vengono eseguite
- Controlli della capacità per le esercitazioni
- Notifica per le prove e i turni automatici
- Precedenza per i turni zonali
- Interruzione di un cambio automatico o di un'esecuzione pratica attiva per una risorsa
- Come viene spostato il traffico
- Allarmi per le corse di allenamento
- Finestre bloccate e finestre consentite (in UTC)

Informazioni su zonal autoshift

L'autoshift zonale è una funzionalità che AWS sposta il traffico delle risorse delle applicazioni lontano da una zona di disponibilità, per conto dell'utente. AWS avvia uno spostamento automatico quando la telemetria interna indica che esiste una limitazione della zona di disponibilità che potrebbe avere un impatto sui clienti. La telemetria interna incorpora metriche provenienti da diverse fonti, tra cui la AWS rete e i servizi Amazon EC2 ed Elastic Load Balancing.

È necessario abilitare manualmente lo spostamento automatico zonale per le risorse supportate. AWS

Quando distribuisci ed esegui AWS applicazioni su sistemi di bilanciamento del carico in più (in genere tre) AZs in una regione e esegui la scalabilità preimpostata per supportare la stabilità statica, puoi ripristinare rapidamente le applicazioni dei clienti in una zona di zona deviando il traffico con uno spostamento automatico. AWS Spostando il traffico di risorse verso altri AZs utenti della regione, è AWS possibile ridurre la durata e la gravità del potenziale impatto causato da interruzioni dell'alimentazione, problemi hardware o software in una zona AZ o altri problemi.

Le risorse supportate da ARC forniscono integrazioni che contrassegnano la zona di zona specificata come non integra, il che comporta lo spostamento del traffico dalla zona di zona compromessa.

Quando abiliti lo spostamento automatico zonale per una risorsa, devi anche configurare un'esecuzione pratica per la risorsa. AWS esegue esercitazioni circa settimanali, per 30 minuti, per aiutarvi ad assicurarvi di avere una capacità sufficiente per eseguire l'applicazione senza una delle zone di disponibilità della regione.

Analogamente al trasferimento zonale, esistono alcuni scenari specifici in cui lo spostamento automatico zonale non sposta il traffico dalla zona AZ. Ad esempio, se i gruppi target del sistema di

bilanciamento del carico AZs non dispongono di alcuna istanza o se tutte le istanze non sono integre, il sistema di bilanciamento del carico è in uno stato di fail-open e non è possibile spostarne una. AZs

Per ulteriori informazioni sullo spostamento automatico zonale, consulta. Zonal autoshift in ARC

Quando avvia AWS e arresta i cambi automatici

Quando abiliti lo spostamento automatico zonale per una risorsa, autorizzi AWS a spostare il traffico di risorse di un'applicazione da una zona di disponibilità durante gli eventi, per tuo conto, per ridurre i tempi di ripristino.

A tal fine, l'autoshift zonale utilizza la AWS telemetria per rilevare, il prima possibile, l'esistenza di una compromissione della zona di disponibilità che potrebbe avere un impatto sui clienti. Quando AWS inizia un trasferimento automatico, il traffico verso le risorse configurate inizia immediatamente a spostarsi dalla zona di disponibilità compromessa, il che potrebbe avere un impatto potenziale sui clienti.

L'autoshift zonale è una funzionalità progettata per i clienti che hanno predimensionato le risorse applicative per tutte le zone di disponibilità in un'unica soluzione. Regione AWS Non dovresti fare affidamento sulla scalabilità su richiesta quando inizia un cambio automatico o un'esecuzione pratica.

AWS termina uno spostamento automatico quando determina che la zona di disponibilità è stata ripristinata.

Quando ARC pianifica, avvia e termina, le esercitazioni vengono eseguite

ARC pianifica settimanalmente un'esercitazione per una risorsa, per circa 30 minuti. ARC pianifica, avvia e gestisce le esercitazioni per ciascuna risorsa in modo indipendente. ARC non raggruppa le esercitazioni relative alle risorse dello stesso account. È inoltre possibile avviare autonomamente delle esercitazioni su richiesta, per verificare che la configurazione sia sicura per un evento di spostamento automatico zonale.

Quando un'esercitazione continua per la durata prevista, senza interruzioni, viene contrassegnata con un risultato di. `SUCCESSFUL` Esistono molti altri risultati possibili:`FAILED`,`INTERRUPTED`, `CAPACITY_CHECK_FAILED` e. `PENDING` I valori e le descrizioni dei risultati sono inclusi nella sezione Risultati per le prove pratiche.

In alcuni scenari ARC interrompe un'esercitazione e la termina. Ad esempio, se un cambio automatico si avvia durante un'esercitazione, ARC interrompe l'esercitazione e la termina. Come altro

esempio, supponiamo che la risorsa reagisca in modo negativo all'esecuzione di un'esercitazione e provochi un allarme che avete specificato per monitorare l'esecuzione dell'esercitazione. `ALARM` In questo scenario, ARC interrompe inoltre l'esecuzione dell'esercitazione e la termina.

Inoltre, esistono diversi scenari in cui ARC non avvia un'esercitazione di pianificazione per una risorsa.

In risposta alle sessioni di pratica interrotte e bloccate per una risorsa, ARC esegue le seguenti operazioni:

- Se l'esecuzione di un'esercitazione per una risorsa viene interrotta mentre è in corso, ARC considera terminata l'esercitazione settimanale e pianifica una nuova esercitazione per la risorsa per la settimana successiva. L'esito dell'esercitazione settimanale `INTERRUPTED` rientra in questo scenario, non`FAILED`. L'esito dell'esercitazione è impostato su `FAILED` solo quando l'allarme di esito che monitora l'esercitazione entra in uno `ALARM` stato durante l'esercitazione.
- Se esiste un vincolo di blocco quando è pianificato l'avvio di un'esercitazione per una risorsa, ARC non avvia l'esercitazione. ARC continua a monitorare regolarmente, per determinare se esistono ancora uno o più vincoli di blocco. Quando non ci sono vincoli di blocco, ARC avvia l'esecuzione pratica per la risorsa.

Di seguito sono riportati alcuni esempi di vincoli di blocco che impediscono ad ARC di avviare o continuare l'esecuzione di un'esercitazione per una risorsa:

- ARC non avvia o continua le esercitazioni quando è in corso un AWS Fault Injection Service esperimento. Se un AWS FIS evento è attivo quando ARC ha programmato l'inizio di un'esercitazione, ARC non avvia l'esercitazione. ARC monitora durante le sessioni di pratica per bloccare i vincoli, incluso un evento. AWS FIS Se un AWS FIS evento inizia mentre è attiva un'esercitazione pratica, ARC termina l'esercitazione e non tenta di avviarne un altro fino alla successiva esercitazione regolarmente programmata per la risorsa.
- Se c'è un AWS evento in corso in una regione, ARC non avvia le esercitazioni pratiche per le risorse e termina le esercitazioni attive nella regione.

Quando l'esercitazione termina senza essere interrotta, ARC pianifica la sessione di pratica successiva tra una settimana, come al solito. Se un'esercitazione non viene avviata a causa di un vincolo di blocco, ad esempio un AWS FIS esperimento o una finestra temporale bloccata che hai specificato, ARC continua a tentare di avviare un'esercitazione fino a quando l'esercitazione non può essere avviata.

Controlli della capacità per le esercitazioni

Quando inizia un'esercitazione, per allontanare temporaneamente il traffico da una zona di disponibilità, ARC esegue un controllo per verificare che nelle altre zone di disponibilità sia disponibile una capacità sufficiente per allontanare in sicurezza il traffico dalla AZ. Se la capacità disponibile non è sufficiente, il Traffic Shift per l'esercitazione non viene avviato e l'esercitazione termina.

Inoltre, ARC esegue un controllo della capacità delle risorse di bilanciamento del carico al termine di un cambio automatico di zona, prima che ARC termini lo spostamento del traffico avviato dallo spostamento automatico. Se il controllo della capacità fallisce al termine dell'autoshift, il traffico non viene spostato nuovamente nella zona di disponibilità da cui è stato allontanato.

I controlli della capacità bilanciata vengono completati solo per i sistemi di bilanciamento del carico e i gruppi di Auto Scaling.

Per una risorsa di bilanciamento del carico, i controlli della capacità convalidano che gli host integri associati al sistema di bilanciamento del carico siano distribuiti tra le zone di disponibilità. In particolare, i controlli della capacità assicurano che il numero di host integri in tutte le zone di disponibilità in cui è registrata la risorsa sia bilanciato. Per quanto riguarda i controlli della capacità, bilanciato significa che la capacità integra di ciascuna zona di disponibilità è pari a quella delle altre zone, con una piccola differenza.

Si noti che i controlli di capacità non vengono applicati ai sistemi di bilanciamento del carico con gruppi target di tipo Lambda né agli Application Load Balancer, poiché tali destinazioni non sono configurate a livello di zone.

I controlli della capacità sono stati completati anche per i gruppi Auto Scaling. Per un gruppo Auto Scaling, i controlli di capacità convalidano che la capacità zonale integra totale di un gruppo Auto Scaling, ovvero il numero di host integri totali in tutte le zone di disponibilità, soddisfi la capacità desiderata impostata per quel gruppo di Auto Scaling.

Quando un controllo della capacità fallisce

Quando un controllo della capacità rileva che la capacità disponibile non è bilanciata per una risorsa, il risultato dell'esercitazione è`CAPACITY_CHECK_FAILED`. Per ulteriori informazioni sul motivo per cui un controllo della capacità non è riuscito, consulta il campo dei commenti relativo a`ZonalShiftSummary`. Per trovare il campo dei commenti per il tuo turno zonale di Practice Run, procedi come segue:

1. Utilizzando AWS CLI, elenca i turni zonali per la risorsa specificata nell'esecuzione dell'esercitazione utilizzando l'ListZonalShiftsoperazione API.

   FOr ad esempio, per restituire i turni zonali, è possibile eseguire un comando simile al seguente:

   ```
   aws arc-zonal-shift start-practice-run
       --resource-
   identifier="arn:aws:elasticloadbalancing:Region:111122223333:ExampleALB123456890"
   ```

2. Esamina la serie di `ZonalShiftSummary` oggetti restituiti per trovare lo spostamento zonale relativo all'esecuzione pratica che non è riuscito a causa dei controlli della capacità.
3. Per lo spostamento zonale applicabile, consulta le informazioni nel `Comment` campo.

Notifica per le prove e i turni automatici

Puoi scegliere di ricevere notifiche sulle sessioni di pratica e sugli spostamenti automatici della tua risorsa configurando le notifiche Amazon. EventBridge Puoi configurare EventBridge le notifiche anche se non hai abilitato lo spostamento automatico zonale per nessuna risorsa, noto come notifica autoshift observer. Con la notifica autoshift observer, si riceve una notifica di tutti gli spostamenti automatici che ARC avvia quando una zona di disponibilità è potenzialmente compromessa. Tieni presente che devi configurare questa opzione in ognuna delle quali desideri ricevere notifiche. Regione AWS

Per vedere i passaggi per abilitare la notifica autoshift observer, consulta. Abilitazione o disabilitazione della notifica autoshift observer Per ulteriori informazioni sulle opzioni di notifica e su come configurarle in, consulta. EventBridge Utilizzo dello spostamento automatico zonale con Amazon EventBridge

Precedenza per i turni zonali

Non può essere applicato più di uno spostamento zonale alla volta. Cioè, solo una pratica esegue il cambio di zona, il cambiamento di zona avviato dal cliente, lo spostamento automatico o l'esperimento per la risorsa. AWS FIS Quando viene avviato un secondo spostamento zonale, ARC segue una precedenza per determinare quale tipo di spostamento zonale è valido per una risorsa.

Il principio generale di precedenza è che i turni zonali avviati come cliente hanno la precedenza sugli altri tipi di turni. Tuttavia, tieni presente che un'esercitazione AWS avviata attualmente in esecuzione impedisce di iniziare un'esercitazione su richiesta.

Per illustrare la precedenza in ARC, di seguito viene illustrato il funzionamento della precedenza, ad esempio negli scenari:

Tipo di spostamento zonale applicato	Tipo di spostamento zonale avviato	Risultato
AWS FIS esperimento	Corsa pratica	L'esercitazione non avrà inizio, poiché l' AWS FIS esperimento ha la precedenza.
AWS FIS esperimento	Spostamento zonale manuale	L' AWS FIS esperimento verrà annullato e verrà applicato lo spostamento zonale manuale.
AWS FIS esperimento	Spostamento zonale automatico	L' AWS FIS esperimento verrà annullato e verrà applicato lo spostamento automatico zonale.
AWS FIS esperimento	AWS FIS esperimento	L' AWS FIS esperimento iniziato non verrà avviato perché è in corso un esperimento esistente che ha attivato l'azione di cambio AWS FIS automatico.
Corsa pratica	Spostamento zonale manuale	L'esercitazione verrà annullata e il risultato impostato sarà lo stesso e verrà `INTERRUPTED` applicato lo spostamento zonale.
Corsa pratica	AWS FIS esperimento	L'esercitazione verrà annullata e il risultato impostato sarà impostato`INTERRUPTED` , e l' AWS FIS esperimento verrà applicato.

Tipo di spostamento zonale applicato	Tipo di spostamento zonale avviato	Risultato
Corsa pratica	Spostamento zonale automatico	L'esercitazione verrà annullata e il risultato impostato su`INTERRUPTED` , e verrà applicato lo spostamento automatico zonale.
Spostamento zonale manuale	Corsa pratica	L'esercitazione non avrà inizio.
Spostamento zonale manuale	AWS FIS esperimento	L' AWS FIS esperimento non verrà avviato o fallirà se è già in corso.
Spostamento zonale manuale	Spostamento zonale automatico	Lo spostamento automatico zonale avverrà `ACTIVE` ma non sulla risorsa. `APPLIED` Lo spostamento zonale manuale ha la precedenza.
Spostamento zonale automatico	AWS FIS esperimento	L' AWS FIS esperimento non verrà avviato o fallirà se è in corso.
Spostamento zonale automatico	Spostamento zonale manuale	Lo spostamento automatico zonale avverrà `ACTIVE` ma non sulla risorsa. `APPLIED` Lo spostamento zonale manuale ha la precedenza.
Spostamento zonale automatico	Corsa pratica	L'esercitazione non verrà avviata, poiché lo spostamen to automatico zonale ha la precedenza.

Lo spostamento del traffico attualmente in vigore per la risorsa ha uno stato di spostamento zonale applicato impostato su `APPLIED`. È impostato su `APPLIED` un solo spostamento alla volta. Gli altri turni in corso sono impostati, ma rimangono invariati`NOT_APPLIED`. `ACTIVE`

Interruzione di un cambio automatico o di un'esecuzione pratica attiva per una risorsa

Per interrompere uno spostamento automatico in corso per una risorsa, è necessario annullare lo spostamento di zona.

Per la risorsa si svolgono ancora prove pratiche regolari, secondo lo stesso programma. Se si desidera interrompere le esercitazioni oltre a disabilitare gli spostamenti automatici, è necessario eliminare la configurazione dell'esecuzione pratica associata alla risorsa.

Quando si elimina una configurazione di esecuzione pratica, AWS interrompe l'esecuzione delle esercitazioni che spostano il traffico della risorsa lontano da una zona di disponibilità ogni settimana. Inoltre, poiché lo spostamento automatico zonale richiede delle esercitazioni pratiche, quando si elimina una configurazione di esecuzione pratica utilizzando la console ARC, questa azione disabilita anche lo spostamento automatico zonale per la risorsa. Tuttavia, tieni presente che se utilizzi l'API zonal autoshift per eliminare un'esercitazione, devi prima disabilitare l'autoshift zonale per la risorsa.

Per ulteriori informazioni, consultare Annullamento di un cambio automatico zonale e Abilitazione e utilizzo dell'autoshift zonale.

Come viene spostato il traffico

Per gli spostamenti automatici e per fare pratica con i turni zonali, il traffico viene spostato da una zona di disponibilità utilizzando lo stesso meccanismo utilizzato da ARC per i turni zonali avviati dal cliente. A seguito di un controllo dello stato non corretto, Amazon Route 53 ritira gli indirizzi IP corrispondenti della risorsa dal DNS, in modo che il traffico venga reindirizzato dalla zona di disponibilità. Le nuove connessioni vengono ora instradate invece verso altre zone di disponibilità. Regione AWS

Con uno spostamento automatico, quando una zona di disponibilità si ripristina e AWS decide di interrompere lo spostamento automatico, ARC inverte il processo di controllo dello stato, richiedendo l'annullamento dei controlli di integrità della Route 53. Quindi, gli indirizzi IP zonali originali vengono ripristinati e, se i controlli di integrità continuano a essere corretti, la zona di disponibilità viene nuovamente inclusa nel routing dell'applicazione.

È importante tenere presente che gli spostamenti automatici non si basano su controlli di integrità che monitorano lo stato di base dei sistemi di bilanciamento del carico o delle applicazioni. ARC utilizza

i controlli di integrità per allontanare il traffico dalle zone di disponibilità, richiedendo che i controlli di integrità siano impostati su «non integri», quindi ripristina nuovamente i controlli di integrità alla normalità quando termina uno spostamento automatico o uno spostamento di zona.

Allarmi per le corse di allenamento

È possibile specificare due tipi di CloudWatch allarmi per le esercitazioni in autoshift zonale: allarmi di esito e allarmi di blocco.

Allarmi sui risultati (obbligatori)

Per il primo tipo di allarme, l'allarme di risultato, è necessario specificare almeno un allarme. È necessario configurare gli allarmi di esito per monitorare lo stato dell'applicazione quando il traffico viene spostato da una zona di disponibilità durante ogni esercizio di 30 minuti.

Affinché un'esercitazione sia efficace, specifica come allarmi di esito almeno un CloudWatch allarme che soddisfi entrambi i seguenti criteri:

L'allarme monitora le metriche relative alla risorsa o all'applicazione

AND

L'allarme risponde con uno `ALARM` stato in cui l'applicazione viene influenzata negativamente dalla perdita di una zona di disponibilità.

Per ulteriori informazioni, consulta la sezione Allarmi specificati per le esecuzioni pratiche in. Le migliori pratiche per la configurazione dell'autoshift zonale

Gli allarmi sui risultati forniscono anche informazioni sull'esito dell'esercitazione che ARC riporta per ogni sessione di esercitazione. Se un allarme di esito entra in uno `ALARM` stato, ARC termina l'esecuzione dell'esercitazione e restituisce il risultato dell'esecuzione dell'`FAILED`esercitazione. Se l'esecuzione dell'esercitazione completa il periodo di test di 30 minuti e nessuno degli allarmi di risultato che hai specificato entra in uno `ALARM` stato, il risultato restituito è. `SUCCEEDED` Un elenco di tutti i valori dei risultati, con le relative descrizioni, è disponibile nella sezione Risultati per le esercitazioni.

Blocco degli allarmi (opzionale)

Facoltativamente, puoi specificare un secondo tipo di allarme, l'allarme di blocco. La pratica del blocco degli allarmi viene eseguita dall'inizio o dalla continuazione quando uno o più allarmi si

trovano in uno stato. `ALARM` Il blocco degli allarmi blocca l'avvio dell'esercitazione, i turni di traffico e interrompe tutte le esercitazioni in corso quando almeno uno degli allarmi è in uno stato. `ALARM`

Ad esempio, in un'architettura di grandi dimensioni con più microservizi, quando un microservizio presenta un problema, in genere si desidera interrompere tutte le altre modifiche nell'ambiente dell'applicazione, incluso il blocco delle procedure di esecuzione. A tale scopo, è possibile aggiungere un allarme di blocco in ARC.

Finestre bloccate e finestre consentite (in UTC)

È possibile bloccare o consentire le esercitazioni per date di calendario specifiche o per finestre temporali specifiche, ovvero giorni e ore, specificati in UTC.

Ad esempio, se hai programmato il lancio di un aggiornamento dell'applicazione per il 1° maggio 2024 e non desideri che le sessioni di esercitazione allontanino il traffico in quel momento, puoi impostare una data bloccata per. `2024-05-01`

Oppure, supponiamo che tu esegua riepiloghi di report aziendali tre giorni alla settimana. In questo scenario, puoi impostare i seguenti giorni e orari ricorrenti come finestre bloccate, per esempio, in UTC:. `MON-20:30-21:30 WED-20:30-21:30 FRI-20:30-21:30`

In alternativa, potreste decidere che il mercoledì e il venerdì, da mezzogiorno alle 5:00, siano gli orari migliori per ARC per iniziare le prove pratiche e testare la configurazione. In questo scenario, puoi impostare i seguenti giorni e orari ricorrenti come finestre consentite, ad esempio in UTC:. `WED-12:00-17:00 FRI-12:00-17:00`

Regione AWS disponibilità per lo spostamento automatico zonale

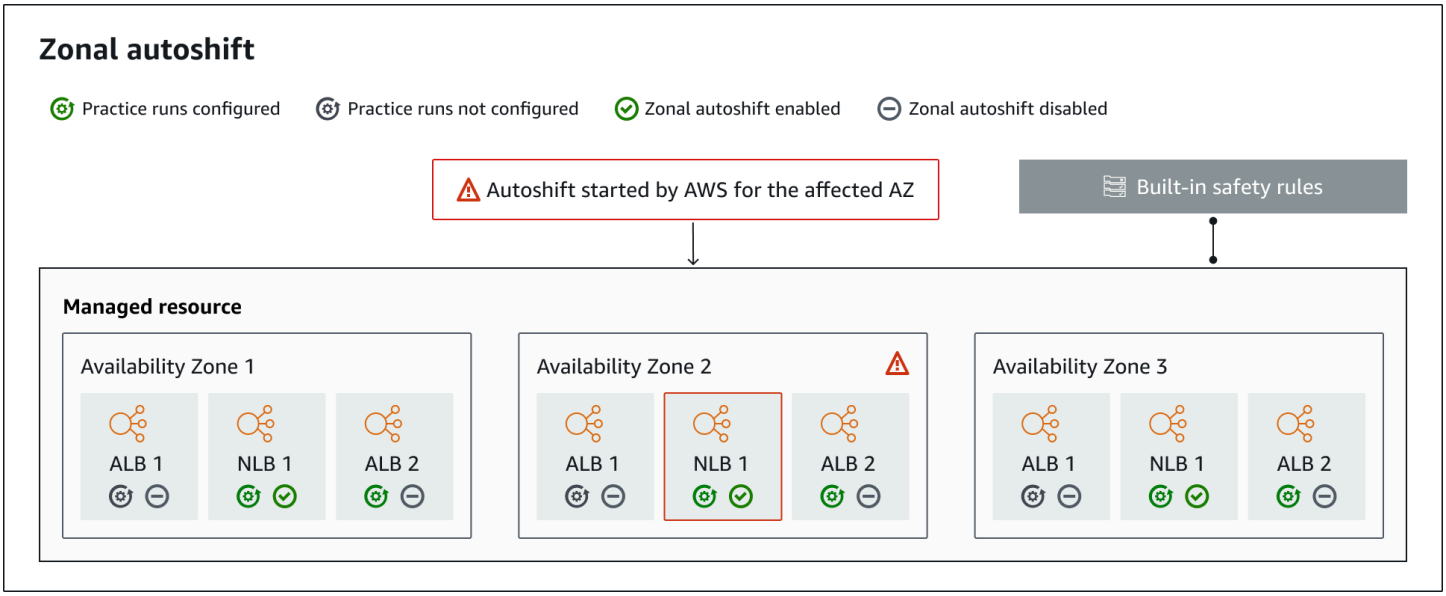
Il cambio di zona e lo spostamento automatico di zona sono attualmente disponibili nelle regioni commerciali e cinesi Regioni AWS, ovvero nella regione Cina (Pechino) e nella regione Cina (Ningxia).

Le risorse che utilizzano Amazon Application Recovery Controller (ARC) possono includere considerazioni aggiuntive. Per ulteriori informazioni, consulta Risorse supportate.

Per un elenco di regioni e informazioni dettagliate sul supporto regionale e sugli endpoint di servizio per ARC, consulta gli endpoint e le quote di Amazon Application Recovery Controller (ARC) nell'Amazon Web Services General Reference.

Zonal autoshift components

Il diagramma seguente illustra un esempio di trasferimento automatico che sposta il traffico lontano da una zona di disponibilità. AWS avvia uno spostamento automatico quando la telemetria interna indica che esiste una limitazione della zona di disponibilità che potrebbe avere un impatto sui clienti.



Di seguito sono riportati i componenti delle funzionalità di cambio automatico zonale in ARC.

Spostamenti automatici zonali

Lo spostamento automatico zonale sposta il traffico verso una risorsa, senza che sia necessario intraprendere alcuna azione. Lo spostamento automatico zonale è una funzionalità di ARC che AWS avvia uno spostamento automatico quando la telemetria interna indica che esiste una limitazione della zona di disponibilità che potrebbe avere un impatto sui clienti. Tieni presente che, in alcuni casi, potrebbero essere spostate via risorse che non subiscono alcun impatto.

Corse di pratica

Quando abiliti lo spostamento automatico zonale per una risorsa, devi anche configurare le esecuzioni pratiche di spostamento automatico zonale per la risorsa. AWS esegue un turno zonale per le sessioni di pratica circa settimanali, per circa 30 minuti. È inoltre possibile pianificare le esercitazioni su richiesta.

Le sessioni di esercitazione assicurano che l'applicazione possa funzionare normalmente senza la perdita di una zona di disponibilità. In un'esercitazione, AWS sposta il traffico relativo a una risorsa lontano da una zona di disponibilità con uno spostamento zonale, quindi riporta il traffico indietro al termine dell'esecuzione dell'esercitazione.

Configurazioni per l'esecuzione pratica

Con una configurazione di esecuzione pratica, è possibile definire gli intervalli di tempo (finestre bloccate o consentite) entro i quali ARC può avviare un'esecuzione pratica per una risorsa con spostamento automatico zonale. È inoltre possibile definire gli CloudWatch allarmi per un'esercitazione. AWS È possibile modificare la configurazione di un'esercitazione in qualsiasi momento, aggiungere o modificare finestre bloccate o consentite o aggiornare gli allarmi per l'esercitazione.

Per abilitare lo spostamento automatico zonale, è necessario disporre di una configurazione di esecuzione pratica per una risorsa.

È possibile eliminare un'esercitazione, ma prima è necessario disabilitare lo spostamento automatico zonale.

Esercitati, esegui allarmi

Quando si configurano le sessioni di esercitazione, si specificano gli CloudWatch allarmi (che vengono creati per la prima volta CloudWatch), in base ai requisiti di risorse e applicazioni. Gli allarmi specificati possono bloccare l'avvio di un'esercitazione o interrompere un'esercitazione in corso, se l'applicazione è influenzata negativamente dall'esecuzione dell'esercitazione.

Se un avviso specificato entra in uno `ALARM` stato, ARC interrompe lo spostamento zonale per l'esecuzione dell'esercitazione, in modo che il traffico della risorsa non venga più spostato dalla zona di disponibilità.

Esistono due tipi di allarmi specificati per le esercitazioni: gli allarmi dei risultati, per monitorare lo stato della risorsa e dell'applicazione durante l'esecuzione dell'esercitazione, e gli allarmi di blocco, che è possibile configurare per impedire l'avvio delle esercitazioni o per interrompere un'esercitazione in corso. È richiesto almeno un allarme di esito; il blocco degli allarmi è facoltativo.

Risultati della sessione pratica

ARC riporta un risultato per ogni esercitazione. Di seguito sono riportati i possibili esiti della prova pratica:

- IN SOSPESO: Il turno zonale per l'esercitazione è attivo (in corso). Non ci sono ancora esiti.
- RIUSCITA: L'allarme relativo all'esito non è `ALARM` stato attivato durante l'esercitazione e l'esercitazione ha completato l'intero periodo di prova di 30 minuti.
- INTERROTTA: L'esercitazione è terminata per un motivo diverso dall'allarme relativo all'esito. `ALARM` Una prova pratica può essere interrotta per una serie di motivi. Ad esempio,

un'esercitazione che termina perché l'allarme di blocco specificato per l'esercitazione è entrato in uno `ALARM` stato ha il risultato di`INTERRUPTED`. Per ulteriori informazioni sui motivi di un esito `INTERRUPTED`, consulta Outcomes for practice runs.

- FALLITA: l'allarme di esito è entrato in uno stato `ALARM` durante la prova pratica.
- CAPACITY_CHECK_FAILED: la verifica della capacità bilanciata nelle zone di disponibilità per le risorse del gruppo di bilanciamento del carico e Auto Scaling non è riuscita.

Regole di sicurezza integrate

Le regole di sicurezza integrate in ARC impediscono che si verifichi più di un cambio di traffico per una risorsa alla volta. In altre parole, solo un cambio di zona avviato dal cliente, un cambio zonale di tipo Practice Run (avviato da AWS o da un cliente) o lo spostamento automatico della risorsa possono spostare attivamente il traffico lontano da una zona di disponibilità. Ad esempio, se si avvia uno spostamento di zona per una risorsa quando è attualmente spostata via con lo spostamento automatico, il cambiamento di zona ha la precedenza. Per ulteriori informazioni, consulta Precedenza per i turni zonali.

Identificatore di risorsa

L'identificatore di una risorsa per cui abilitare lo spostamento automatico zonale, ovvero l'Amazon Resource Name (ARN) della risorsa. Puoi abilitare lo spostamento automatico zonale solo per le risorse del tuo account che fanno parte di un servizio supportato da ARC. AWS

Risorsa gestita

Gli Application Load Balancer registrano automaticamente le risorse con ARC per lo spostamento automatico zonale. È necessario attivare manualmente altre risorse per lo spostamento automatico zonale.

Nome risorsa

Il nome di una risorsa gestita in ARC.

Stato applicato

Uno stato applicato indica se per una risorsa è in corso uno spostamento del traffico. Quando si configura lo spostamento automatico zonale, una risorsa può avere più di uno spostamento di traffico attivo, ad esempio un cambio di zona eseguito in pratica, uno spostamento di zona avviato dal cliente o uno spostamento automatico. Tuttavia, ne viene applicato solo uno alla volta, ossia è valido per la risorsa. Lo spostamento con lo stato `APPLIED` determina la zona di disponibilità in cui il traffico dell'applicazione è stato spostato verso una risorsa e quando termina tale spostamento di traffico.

Tipo di turno

Definisce il tipo di spostamento zonale. I turni zonali possono avere uno dei seguenti tipi:

- ZONAL_SHIFT
- ZONAL_AUTOSHIFT
- ESERCITAZIONE_CORRI
- FIS EXPERIMENT

Piani di dati e controllo per lo spostamento automatico zonale

Quando pianifichi il failover e il disaster recovery, considera la resilienza dei tuoi meccanismi di failover. Ti consigliamo di assicurarti che i meccanismi da cui dipendi durante il failover siano altamente disponibili, in modo da poterli utilizzare quando ne hai bisogno in uno scenario di emergenza. In genere, è consigliabile utilizzare le funzioni del piano dati per i meccanismi ogni volta che è possibile, per la massima affidabilità e tolleranza ai guasti. In quest'ottica, è importante capire in che modo la funzionalità di un servizio è suddivisa tra piani di controllo e piani dati e quando è possibile contare su un'aspettativa di estrema affidabilità con il piano dati di un servizio.

In generale, un piano di controllo consente di eseguire funzioni di gestione di base, come creare, aggiornare ed eliminare risorse nel servizio. Un piano dati fornisce le funzionalità principali di un servizio.

Per ulteriori informazioni sui piani dati, sui piani di controllo e su come AWS crea servizi per soddisfare gli obiettivi di alta disponibilità, consulta il paper Static stability using Availability Zones in Amazon Builders' Library.

Prezzi per l'autoshift zonale in ARC

Per quanto riguarda lo spostamento automatico zonale, AWS sposta il traffico da una zona di disponibilità per conto dell'utente verso le risorse supportate quando AWS determina l'esistenza di un potenziale problema che può influire negativamente sulle applicazioni dei clienti. Non sono previsti costi aggiuntivi per l'attivazione dello spostamento automatico zonale.

Per informazioni dettagliate sui prezzi di ARC ed esempi di prezzi, consulta ARC Pricing.

Le migliori pratiche per la configurazione dell'autoshift zonale

Tieni presente le seguenti best practice e considerazioni quando abiliti l'autoshift zonale in Amazon Application Recovery Controller (ARC).

L'autoshift zonale include due tipi di turni di traffico: turni automatici e turni zonali Practice Run.

- Lo spostamento automatico AWS consente di ridurre i tempi di ripristino allontanando il traffico delle risorse applicative da una zona di disponibilità durante gli eventi, per conto dell'utente.
- Con le esercitazioni, ARC avvia un turno di allenamento zonale per tuo conto oppure tu inizi un turno di pratica a turni zonali. L'esecuzione AWS pratica del turno zonale sposta il traffico da una zona di disponibilità a una risorsa e viceversa, con cadenza settimanale. Le esecuzioni pratiche aiutano ad accertarsi di aver ampliato la capacità necessaria per le zone di disponibilità in una regione affinché l'applicazione possa tollerare la perdita di una zona di disponibilità.

Esistono diverse best practice e considerazioni da tenere a mente per quanto riguarda gli spostamenti automatici e le esecuzioni pratiche. Consulta i seguenti argomenti prima di abilitare lo spostamento automatico zonale o configurare le sessioni pratiche per una risorsa.

Argomenti

- Limita il tempo in cui i client rimangono connessi ai tuoi endpoint
- Prescalate la vostra capacità di risorse e testate il traffico mutevole
- Sii consapevole dei tipi e delle restrizioni delle risorse
- Specificate gli allarmi per le prove
- Valuta i risultati delle prove

Limita il tempo in cui i clienti rimangono connessi ai tuoi endpoint

Quando Amazon Application Recovery Controller (ARC) allontana il traffico da un problema, ad esempio utilizzando lo spostamento zonale o lo spostamento automatico di zona, il meccanismo utilizzato da ARC per spostare il traffico dell'applicazione è un aggiornamento DNS. Un aggiornamento DNS fa sì che tutte le nuove connessioni vengano indirizzate lontano dalla posizione compromessa. Tuttavia, i client con connessioni aperte preesistenti potrebbero continuare a effettuare richieste nei confronti della posizione compromessa fino alla riconnessione dei client. Per garantire un ripristino rapido, ti consigliamo di limitare il periodo di tempo in cui i client rimangono connessi ai tuoi endpoint.

Se si utilizza un Application Load Balancer, è possibile utilizzare l'`keepalive`opzione per configurare la durata delle connessioni. Ti consigliamo di abbassare il `keepalive` valore per adattarlo all'obiettivo del tempo di ripristino per l'applicazione, ad esempio 300 secondi. Quando

scegli un `keepalive` orario, considera che questo valore rappresenta un compromesso tra la riconnessione più frequente in generale, il che può influire sulla latenza, e lo spostamento più rapido di tutti i client da una zona o regione compromessa.

Per ulteriori informazioni sull'impostazione dell'`keepalive`opzione per Application Load Balancer, vedete la durata del client HTTP keepalive nella Application Load Balancer User Guide.

Prescalate la vostra capacità di risorse e testate il traffico variabile

Quando si AWS sposta il traffico da una zona di disponibilità a favore di uno spostamento di zona o di uno spostamento automatico, è importante che le zone di disponibilità rimanenti siano in grado di soddisfare le maggiori percentuali di richiesta della risorsa. Questo modello è noto come stabilità statica. Per ulteriori informazioni, consulta il white paper sulla stabilità statica con le zone di disponibilità nella libreria di Amazon Builder.

Ad esempio, se l'applicazione richiede 30 istanze per servire i propri clienti, è necessario effettuare il provisioning di 15 istanze in tre zone di disponibilità, per un totale di 45 istanze. In questo modo, quando si AWS sposta il traffico da una zona di disponibilità, con uno spostamento automatico o durante un'esecuzione pratica, è comunque AWS possibile servire i client dell'applicazione con il totale rimanente di 30 istanze, su due zone di disponibilità.

La funzionalità di trasferimento automatico zonale di ARC consente di ripristinare rapidamente AWS gli eventi in una zona di disponibilità quando si dispone di un'applicazione con risorse predimensionate per funzionare normalmente con la perdita di una zona di disponibilità. Prima di abilitare lo spostamento automatico zonale per una risorsa, scalate la capacità delle risorse in tutte le zone di disponibilità configurate in un'unica. Regione AWS Quindi, avvia i turni zonali per la risorsa, per verificare che l'applicazione funzioni ancora normalmente quando il traffico viene spostato da una zona di disponibilità.

Dopo aver eseguito il test con i turni zonali, abilita lo spostamento automatico zonale e configurato le esecuzioni pratiche per le risorse dell'applicazione. Eseguite le vostre sessioni pratiche su richiesta per assicurarvi che la configurazione sia scalata correttamente. Le esercitazioni regolari con zonal autoshift vi aiutano ad assicurarvi, su base continuativa, che la vostra capacità sia ancora scalata in modo appropriato. Con una capacità sufficiente in tutte le zone di disponibilità, l'applicazione può continuare a servire i clienti, senza interruzioni, durante un trasferimento automatico.

Per ulteriori informazioni sull'avvio di uno spostamento di zona per una risorsa, vedere. Zonal shift in ARC

Sii consapevole dei tipi e delle restrizioni delle risorse

Lo spostamento automatico zonale supporta lo spostamento del traffico da una zona di disponibilità per tutte le risorse supportate dallo spostamento zonale. In alcuni scenari di risorse specifici, lo spostamento automatico zonale non sposta il traffico da una zona di disponibilità a uno spostamento automatico.

Ad esempio, se i gruppi target del sistema di bilanciamento del carico nelle zone di disponibilità non dispongono di istanze o se tutte le istanze non sono integre, il sistema di bilanciamento del carico si trova in uno stato di fail-open. Se AWS avvia uno spostamento automatico per un sistema di bilanciamento del carico in questo scenario, lo spostamento automatico non modifica le zone di disponibilità utilizzate dal sistema di bilanciamento del carico, poiché il sistema di bilanciamento del carico è già in uno stato di fail-open. Questo è il comportamento previsto. Lo spostamento automatico non può causare il malfunzionamento di una zona di disponibilità e spostare il traffico verso le altre zone di disponibilità se tutte le zone di disponibilità non sono aperte (non integre). Regione AWS

Per visualizzare i dettagli sulle risorse supportate, inclusi tutti i requisiti e le eccezioni di cui tenere conto, vedere. Risorse supportate

Specificare gli allarmi per le sessioni di pratica

È necessario configurare almeno un tipo di allarme (un allarme di esito) per le esercitazioni con spostamento automatico zonale. Facoltativamente, puoi anche configurare un secondo tipo di allarme (blocco degli allarmi).

Quando consideri gli CloudWatch allarmi che configuri per le sessioni di esercitazione per la tua risorsa, tieni presente quanto segue:

- È necessario configurare almeno un allarme di esito per una configurazione di esecuzione pratica. Per quanto riguarda gli allarmi di esito, ti consigliamo di configurare gli CloudWatch allarmi in modo che entrino in uno `ALARM` stato in cui le metriche relative alla risorsa o all'applicazione indicano che lo spostamento del traffico dalla zona di disponibilità influisce negativamente sulle prestazioni. Ad esempio, puoi determinare una soglia per i tassi di richiesta per la tua risorsa e quindi configurare un allarme in modo che entri in uno `ALARM` stato quando la soglia viene superata. L'utente è responsabile della configurazione degli allarmi appropriati che causino la AWS fine dell'esecuzione dell'esercitazione e la restituzione di un risultato. `FAILED`
- Ti consigliamo di seguire il AWS Well Architected Framework, che ti consiglia di implementare gli indicatori chiave di prestazione () KPIs come allarmi. CloudWatch In tal caso, è possibile

utilizzare questi allarmi per creare un allarme composito da utilizzare come trigger di sicurezza, per evitare che vengano avviate sessioni di prova che potrebbero causare il mancato rispetto di un KPI nell'applicazione. Quando l'allarme non è più in uno `ALARM` stato, ARC avvia le esercitazioni la prossima volta che viene pianificata un'esecuzione pratica per la risorsa.

- Per fare pratica sugli allarmi di blocco, se scegli di configurarne uno (o più), puoi scegliere di tenere traccia di metriche specifiche che utilizzi per indicare che non desideri che un' AWS esercitazione abbia inizio, ad esempio quando un allarme indica che è in corso un incidente.
- Per fare pratica, devi specificare l'Amazon Resource Name (ARN) per ogni allarme, quindi devi prima configurare l'allarme in Amazon. CloudWatch Gli CloudWatch allarmi che specifichi possono essere allarmi compositi, per consentirti di includere diverse metriche e controlli per l'applicazione e la risorsa in grado di attivare lo stato dell'allarme. `ALARM` In alternativa, è possibile configurare allarmi separati e quindi specificare più di un allarme di ogni tipo per la configurazione dell'esecuzione pratica. Per ulteriori informazioni, consulta Combinare gli allarmi nella Amazon CloudWatch User Guide.
- Assicurati che gli CloudWatch allarmi che specifichi per le esercitazioni si trovino nella stessa regione della risorsa per cui stai configurando un'esercitazione.

Valuta i risultati delle esercitazioni

ARC riporta un risultato per ogni esercitazione. Dopo un'esercitazione, valuta il risultato e determina se è necessario agire. Ad esempio, potrebbe essere necessario scalare la capacità o modificare la configurazione per un allarme.

Di seguito sono riportati i possibili esiti della prova pratica:

- RIUSCITA: durante l'esercitazione non è `ALARM` stato attivato alcun allarme di esito e l'esercitazione ha completato l'intero periodo di test di 30 minuti.
- FALLITO: almeno un allarme di esito è entrato in uno `ALARM` stato durante l'esecuzione dell'esercitazione.
- INTERROTTA: L'esercitazione è terminata per un motivo diverso dall'allarme di esito che entrava in uno `ALARM` stato. Un'esercitazione può essere interrotta per diversi motivi, tra cui i seguenti:
  - L'esercitazione è stata interrotta perché è stato AWS avviato un cambio automatico nella regione Regione AWS o si è verificata una condizione di allarme nella regione.
  - L'esecuzione pratica è stata terminata perché la configurazione dell'esecuzione pratica è stata eliminata per la risorsa.

  - L'esecuzione dell'esercitazione è stata interrotta perché è stato avviato uno spostamento di zona avviato dal cliente per la risorsa nella zona di disponibilità da cui il trasferimento zonale dell'esecuzione dell'esercitazione stava allontanando il traffico.
  - L'esecuzione dell'esercitazione è stata interrotta perché non era più possibile accedere all' CloudWatch allarme specificato per la configurazione dell'esercitazione.
  - L'esercitazione è stata terminata perché un allarme di blocco specificato per l'esercitazione è entrato in uno `ALARM` stato.
  - L'esercitazione è stata interrotta per un motivo sconosciuto.
  - L'esercitazione è stata interrotta perché è stato avviato un cambio automatico di zona con precedenza. Vedi Precedenza per i cambiamenti zonali.
- CAPACITY_CHECK_FAILED: la verifica della capacità bilanciata nelle zone di disponibilità per le risorse del gruppo di bilanciamento del carico e Auto Scaling non è riuscita.
- IN SOSPESO: L'esercitazione è attiva (in corso). Non ci sono ancora esiti.

Operazioni Zonal Autoshift API

La tabella seguente elenca le operazioni dell'API ARC che è possibile utilizzare con lo spostamento automatico zonale. Per esempi di utilizzo delle operazioni dell'API zonal autoshift con, vedere. AWS CLI

Per esempi di come utilizzare le comuni operazioni dell'API zonal autoshift con, vedere. AWS Command Line InterfaceEsempi di utilizzo della funzione AWS CLI con cambio automatico zonale

Azione	Utilizzo della console ARC	Utilizzando l'API ARC
Crea una configurazione di esecuzione pratica	Consulta Enabling or disabling zonal autoshift.	Consulta la sezione CreatePracticeRunConfiguration
Eliminare una configurazione di esecuzione pratica	Consulta Configurazione, modifica o eliminazione di una configurazione di esecuzione pratica.	Consulta la sezione DeletePracticeRunConfiguration
Elenca i turni automatici	Consulta Zonal autoshift in ARC.	Consulta la sezione ListAutoshifts

Azione	Utilizzo della console ARC	Utilizzando l'API ARC
Elenca le risorse per lo spostamento automatico zonale	Consulta Risorse supportate.	Consulta la sezione ListManagedResources
Ottieni risorse per lo spostamento automatico zonale	Consulta Risorse supportate.	Consulta la sezione GetManagedResource
Modifica una configurazione di esecuzione pratica	Consulta Configurazione, modifica o eliminazione di una configurazione di esecuzione pratica.	Consulta la sezione UpdatePracticeRunConfiguration
Abilita o disabilita lo spostamento automatico zonale	Consulta Enabling or disabling zonal autoshift.	Consulta la sezione UpdateZonalAutoshiftConfiguration
Abilita o disabilita la notifica autoshift observer	Consulta Abilitazione e utilizzo dell'autoshift zonale.	Consulta la sezione UpdateAutoshiftObserverNotificationStatus
Inizia una corsa pratica	Consulta Avvio di una corsa pratica (spostamento zonale).	Consulta la sezione StartPracticeRun
Annullare un'esercitazione	Consulta Annullamento di un'esercitazione (turno zonale).	Consulta la sezione CancelPracticeRun

Esempi di utilizzo della funzione AWS CLI con cambio automatico zonale

Questa sezione illustra semplici esempi applicativi di utilizzo dell'autoshift zonale, dell'utilizzo della AWS Command Line Interface funzionalità di trasferimento automatico zonale in Amazon Application Recovery Controller (ARC) utilizzando le operazioni API. Gli esempi hanno lo scopo di aiutarti a sviluppare una comprensione di base su come lavorare con l'autoshift zonale utilizzando la CLI.

L'autoshift zonale è una funzionalità di ARC. Con l'autoshift zonale, autorizzi AWS a spostare il traffico delle risorse delle applicazioni supportate da una zona di disponibilità durante gli eventi, per tuo conto, per ridurre i tempi di ripristino. Per ulteriori informazioni sulle risorse che è possibile utilizzare con lo spostamento automatico zonale, vedere. Risorse supportate

L'autoshift zonale include prove pratiche, che allontanano anche il traffico dalle zone di disponibilità, per verificare che gli spostamenti automatici siano sicuri per l'applicazione in uso.

Per un elenco delle azioni dell'API Zonal Autoshift e i collegamenti a ulteriori informazioni, consulta. Operazioni Zonal Autoshift API Per ulteriori informazioni sull'utilizzo di AWS CLI, vedere Command Reference.AWS CLI

Indice

- Creare una configurazione per l'esecuzione pratica
- Abilita o disabilita gli spostamenti automatici
- Avvia un'esercitazione su richiesta
- Annullare un'esercitazione in corso
- Annullare un cambio automatico in corso
- Modificare una configurazione di esecuzione pratica
- Eliminare una configurazione di esecuzione pratica

Creare una configurazione per l'esecuzione pratica

Prima di poter abilitare lo spostamento automatico zonale per una risorsa, è necessario creare una configurazione di esecuzione pratica per la risorsa, in modo da scegliere le opzioni per le esercitazioni richieste. È possibile creare una configurazione di esecuzione pratica per una risorsa con la CLI utilizzando il `create-practice-run-configuration` comando.

Tieni presente quanto segue quando crei una configurazione di esecuzione pratica per una risorsa:

- L'unico tipo di allarme supportato al momento è`CLOUDWATCH`.
- È necessario utilizzare allarmi che siano gli stessi in Regione AWS cui è distribuita la risorsa.
- È necessario specificare un allarme di esito. La specificazione di un allarme di blocco è facoltativa.
- La specificazione di date o finestre bloccate o consentite è facoltativa.

È possibile creare una configurazione di esecuzione pratica con la CLI utilizzando il `create-practice-run-configuration` comando.

Ad esempio, per creare una configurazione di esecuzione pratica per una risorsa, utilizzate un comando come il seguente:

```
aws arc-zonal-shift create-practice-run-configuration \
      --resource-
identifier="arn:aws:elasticloadbalancing:Region:111122223333:ExampleALB123456890" \
      --outcome-alarms
 type=CLOUDWATCH,alarmIdentifier=arn:aws:cloudwatch:Region:111122223333:alarm:Region-
MyAppHealthAlarm \
      --blocking-alarms
 type=CLOUDWATCH,alarmIdentifier=arn:aws:cloudwatch:Region:111122223333:alarm:Region-
BlockWhenALARM \
      --blocked-dates 2023-12-01 --blocked-windows Mon:10:00-Mon:10:30
```

```
{
   "arn": "arn:aws:elasticloadbalancing:us-west-2:111122223333:ExampleALB123456890",
   "name": "zonal-shift-elb"
   "zonalAutoshiftStatus": "DISABLED",
   "practiceRunConfiguration": {
       "blockingAlarms": [
                  {
              "type": "CLOUDWATCH",
              "alarmIdentifier": "arn:aws:cloudwatch:us-west-2:111122223333:alarm:us-
west-2-BlockWhenALARM"
           }
       ]
       "outcomeAlarms": [
           {
               "type": "CLOUDWATCH",
               "alarmIdentifier": "arn:aws:cloudwatch:us-west-2:111122223333:alarm:us-
west-2-MyAppHealthAlarm"
           }
       ],
       "blockedWindows": [
           "Mon:10:00-Mon:10:30"
       ],
       "blockedDates": [
           "2023-12-01"
       ]
```

```
}
```

Abilita o disabilita gli spostamenti automatici

Puoi abilitare o disabilitare gli spostamenti automatici per una risorsa aggiornando lo stato dello spostamento automatico zonale con la CLI. Per modificare lo stato del cambio automatico zonale, usa il comando. `update-zonal-autoshift-configuration`

Ad esempio, per abilitare gli spostamenti automatici per una risorsa, utilizzate un comando come il seguente:

```
aws arc-zonal-shift update-zonal-autoshift-configuration \
      --resource-
identifier="arn:aws:elasticloadbalancing:Region:111122223333:ExampleALB123456890" \
      --zonal-autoshift-status="ENABLED"
```

```
{
   "resourceIdentifier": "arn:aws:elasticloadbalancing:us-
west-2:111122223333:ExampleALB123456890",
   "zonalAutoshiftStatus": "ENABLED"
}
```

Avvia un'esercitazione su richiesta

È possibile avviare un'esercitazione su richiesta run zonal shift con la CLI utilizzando il comando. `start-practice-run`

Ad esempio, per avviare un'esercitazione su una risorsa, utilizzate un comando come il seguente:

```
aws arc-zonal-shift start-practice-run
    --resource-
identifier="arn:aws:elasticloadbalancing:Region:111122223333:ExampleALB123456890" \
    "awayFrom": "usw2-az1",
```

```
{
    "awayFrom": "usw2-az1",
    "comment": "Practice run started. Shifting traffic away from Availability Zone
 usw2-az1.",
}
```

Annullare un'esercitazione in corso

È possibile annullare un'esercitazione in corso con la CLI utilizzando `cancel-practice-run` il comando.

Ad esempio, per annullare l'esecuzione di un'esercitazione per una risorsa, utilizzate un comando come il seguente:

```
aws arc-zonal-shift cancel-practice-run \
   --zonal-shift-id="="arn:aws:testservice::111122223333:ExampleALB123456890"
```

```
{
    "zonalShiftId": "2222222-3333-444-1111",
    "resourceIdentifier": "arn:aws:testservice::111122223333:ExampleALB123456890",
    "awayFrom": "usw2-az1",
    "expiryTime": 2024-11-15T10:35:42+00:00,
    "startTime": 2024-11-15T09:35:42+00:00,
    "status": "CANCELED",
    "comment": "Practice run canceled"
}
```

Annullare un cambio automatico in corso

È possibile annullare un cambio automatico in corso con la CLI annullando lo spostamento automatico zonale per la risorsa. Per annullare un cambio automatico zonale, usa il. `cancel-zonal-shift command`

```
aws arc-zonal-shift cancel-zonal-shift --zonal-shift-id
 9ac9ec1e-1df1-0755-3dc5-8cf573cd9c38
```

```
{
    "awayFrom": "usw2-az1",
    "comment": "Zonal autoshift started. Shifting traffic away from Availability Zone
 usw2-az1.",
    "expiryTime": "2024-12-17T22:29:38-08:00",
    "resourceIdentifier": "arn:aws:elasticloadbalancing:us-
east-1:111122223333:loadbalancer/app/Testing/5a19403ecd42dc05",
    "startTime": "2024-12-17T21:27:26-08:00",
    "status": "CANCELED",
    "zonalShiftId": "9ac9ec1e-1df1-0755-3dc5-8cf573cd9c38"
}
```

Modificare una configurazione di esecuzione pratica

È possibile modificare la configurazione di un'esecuzione pratica per una risorsa con la CLI per aggiornare diverse opzioni di configurazione, ad esempio modificare gli allarmi per le esercitazioni o aggiornare le date bloccate o le finestre bloccate, quando ARC non avvia le esercitazioni. Per modificare la configurazione di un'esercitazione, usa il `update-practice-run-configuration` comando.

Tieni presente quanto segue quando modifichi una configurazione di esecuzione pratica per una risorsa:

- L'unico tipo di allarme supportato al momento è`CLOUDWATCH`.
- È necessario utilizzare allarmi che siano gli stessi in Regione AWS cui è distribuita la risorsa.
- È necessario specificare un allarme di esito. La specificazione di un allarme di blocco è facoltativa.
- La specificazione di date o finestre bloccate è facoltativa.
- Le date bloccate o le finestre bloccate specificate sostituiscono tutti i valori esistenti.

Ad esempio, per modificare una configurazione di esecuzione pratica per una risorsa al fine di specificare una nuova data di blocco, utilizzate un comando come il seguente:

```
aws arc-zonal-shift update-practice-run-configuration \
      --resource-
identifier="arn:aws:elasticloadbalancing:Region:111122223333:ExampleALB123456890" \
      --blocked-dates 2024-03-01
```

```
{
   "arn": "arn:aws:elasticloadbalancing:us-west-2:111122223333:ExampleALB123456890",
   "name": "zonal-shift-elb"
   "zonalAutoshiftStatus": "DISABLED",
   "practiceRunConfiguration": {
       "blockingAlarms": [
                   {
               "type": "CLOUDWATCH",
               "alarmIdentifier": "arn:aws:cloudwatch:us-west-2:111122223333:alarm:us-
west-2-BlockWhenALARM"
           }
       ]
       "outcomeAlarms": [
           {
```

```
                "type": "CLOUDWATCH",
                "alarmIdentifier": "arn:aws:cloudwatch:us-west-2:111122223333:alarm:us-
west-2-MyAppHealthAlarm"
            }
        ],
        "blockedWindows": [
            "Mon:10:00-Mon:10:30"
        ],
        "blockedDates": [
            "2024-03-01"
        ]
}
```

Eliminare una configurazione di esecuzione pratica

È possibile eliminare una configurazione di esecuzione pratica per una risorsa, ma è necessario prima disabilitare lo spostamento automatico zonale per la risorsa. È necessaria una risorsa per disporre di una configurazione di esecuzione pratica per abilitare l'autoshift zonale. Le esercitazioni regolari aiutano a garantire che l'applicazione possa funzionare normalmente senza una zona di disponibilità.

Per eliminare una configurazione di esecuzione pratica utilizzando la CLI, disabilita innanzitutto l'autoshift zonale, se necessario utilizzando il comando. `update-zonal-autoshift` Quindi, per eliminare la configurazione dell'esecuzione pratica, utilizzate il comando. `delete-practice-run-configuration`

Innanzitutto, disattivate lo spostamento automatico zonale per la risorsa, utilizzando un comando come il seguente:

```
aws arc-zonal-shift update-zonal-autoshift-configuration \
      --resource-
identifier="arn:aws:elasticloadbalancing:Region:111122223333:ExampleALB123456890" \
      --zonal-autoshift-status="DISABLED"
```

```
{
   "resourceIdentifier": "arn:aws:elasticloadbalancing:us-
west-2:111122223333:ExampleALB123456890",
   "zonalAutoshiftStatus": "DISABLED"
}
```

Quindi, eliminate la configurazione dell'esecuzione pratica utilizzando un comando come il seguente:

```
aws arc-zonal-shift delete-practice-run-configuration \
      --resource-
identifier="arn:aws:elasticloadbalancing:Region:111122223333:ExampleALB123456890"
```

```
{
   "arn": "arn:aws:elasticloadbalancing:us-west-2:111122223333:ExampleALB123456890",
   "name": "TestResource",
   "zonalAutoshiftStatus": "DISABLED"
}
```

Abilitazione e utilizzo dell'autoshift zonale

Questa sezione fornisce le procedure per lavorare con gli spostamenti automatici zonali in Amazon Application Recovery Controller (ARC). Dopo aver abilitato l'autoshift zonale, puoi apportare modifiche alle configurazioni delle esecuzioni pratiche, avviare un'esercitazione su richiesta, annullare un turno in corso, comprese le esercitazioni, o abilitare le notifiche di autoshift observer.

Enabling or disabling zonal autoshift

I passaggi seguenti spiegano come abilitare o disabilitare lo spostamento automatico zonale sulla console Amazon Application Recovery Controller (ARC). Per utilizzare l'autoshift zonale a livello di codice, consulta la Guida di riferimento alle API Zonal Shift and Zonal Autoshift.

Quando l'autoshift zonale è abilitato, autorizzi AWS a spostare il traffico delle risorse applicative da una zona di disponibilità durante gli eventi, per tuo conto, per ridurre i tempi di ripristino.

Per abilitare o disabilitare lo spostamento automatico zonale

1. Apri la console ARC all'indirizzo. https://console.aws.amazon.com/route53recovery/zonalshift/home#/autoshift
2. In Resource zonal autoshift configurations, scegli una risorsa.
3. Nel menu Azioni, scegli Abilita trasferimento automatico zonale, quindi segui i passaggi per completare l'aggiornamento.

Se la risorsa non dispone di una configurazione di esecuzione pratica, Enable zonal autoshift non è disponibile. Per configurare una configurazione di esecuzione pratica e abilitare lo spostamento automatico zonale, scegli Configura lo spostamento automatico zonale.

Indice

- Configurazione, modifica o eliminazione di una configurazione di esecuzione pratica
- Annullamento di un cambio automatico zonale
- Avvio di una corsa pratica (spostamento zonale)
- Annullamento di un'esercitazione (turno zonale)
- Abilitazione o disabilitazione della notifica autoshift observer

Configurazione, modifica o eliminazione di una configurazione di esecuzione pratica

I passaggi di questa sezione spiegano come modificare o eliminare una configurazione di esecuzione pratica sulla console Amazon Application Recovery Controller (ARC). Per utilizzare l'autoshift zonale a livello di codice, comprese le modifiche alle configurazioni di esecuzione pratica, consulta la Guida di riferimento alle API Zonal Shift e Zonal Autoshift.

Se elimini una configurazione di esecuzione pratica nella console, l'autoshift zonale viene disabilitato. Prima di poter eliminare una configurazione di esecuzione pratica con un'operazione API, è necessario disabilitare l'autoshift zonale. È possibile configurare un'esecuzione pratica senza abilitare lo spostamento automatico zonale. Tuttavia, per abilitare lo spostamento automatico zonale per una risorsa, è necessario che un'esecuzione pratica sia configurata per la risorsa.

Per configurare un'esecuzione pratica

1. Apri la console ARC all'indirizzohttps://console.aws.amazon.com/route53recovery/zonalshift/home#/autoshift.
2. Scegli Configure zonal autoshift.
3. Scegli una risorsa da configurare per lo spostamento automatico zonale.
4. Scegli di disabilitare lo spostamento automatico zonale se non desideri avviare uno spostamento automatico AWS per una risorsa in caso di evento. AWS Se lo desideri, puoi continuare con la procedura guidata per configurare una configurazione pratica senza abilitare gli spostamenti automatici.
5. Scegliete le opzioni per le esercitazioni relative alla risorsa. Per gli allarmi, è possibile fare quanto segue:

   - (Obbligatorio) Specificate almeno un allarme di esito per monitorare le sessioni di pratica relative a questa risorsa.
   - (Facoltativo) Specificate uno o più allarmi di blocco per le esercitazioni relative a questa risorsa.

Per ulteriori informazioni, consulta la sezione Allarmi specificati per le esercitazioni in. Le migliori pratiche per la configurazione dell'autoshift zonale

6. Facoltativamente, specificate le finestre bloccate o consentite, per impedire ad ARC di avviare le esercitazioni o consentire ad ARC di avviare le esercitazioni relative a questa risorsa. Tutte le date e gli orari sono in UTC.
7. Seleziona la casella di controllo per confermare di aver letto la nota di riconoscimento.
8. Scegli Create (Crea).

Per modificare una configurazione di esecuzione pratica

1. Apri la console ARC all'indirizzohttps://console.aws.amazon.com/route53recovery/zonalshift/home#/autoshift.
2. In Resource zonal autoshift configurations, scegli una risorsa.
3. Nel menu Azioni, scegli Modifica pratica ed esegui configurazione.
4. Apporta modifiche alla configurazione dell'esercitazione per eseguire una o più delle seguenti operazioni:
   - Per gli allarmi, è possibile fare quanto segue:
     - Per bloccare gli allarmi, puoi aggiungere uno o più allarmi o eliminare gli allarmi.
     - Per gli allarmi con esito, puoi aggiungere uno o più allarmi o eliminare gli allarmi. È richiesto almeno un allarme di esito, quindi non è possibile eliminare tutti gli allarmi di esito in una configurazione.
   - Per le finestre bloccate e le finestre consentite, puoi aggiungere nuove date o giorni e orari oppure rimuovere o aggiornare date o giorni e orari esistenti. Tutte le date e gli orari sono in UTC.
5. Scegli Save (Salva).

Per eliminare una configurazione di esecuzione pratica

1. Apri la console ARC all'indirizzohttps://console.aws.amazon.com/route53recovery/zonalshift/home#/autoshift.
2. In Resource zonal autoshift configurations, scegli una risorsa.
3. Nel menu Azioni, scegli Elimina pratica ed esegui configurazione.

4. Nella finestra di dialogo modale di conferma, digitate`Delete`, quindi scegliete Elimina.

   Tieni presente che l'eliminazione di una configurazione di esecuzione pratica nella console disabilita anche lo spostamento automatico zonale per la risorsa. Lo spostamento automatico zonale richiede la configurazione di un'esecuzione pratica per la risorsa.

Annullamento di un cambio automatico zonale

Per interrompere uno spostamento automatico zonale in corso per una risorsa, è necessario annullare lo spostamento automatico zonale.

Per interrompere un cambio automatico zonale in corso

1. Apri la console ARC all'indirizzo. https://console.aws.amazon.com/route53recovery/zonalshift/home#/
2. Seleziona uno spostamento automatico zonale che desideri annullare, quindi scegli Annulla spostamento zonale.
3. Nella finestra di dialogo modale di conferma, scegliete Conferma.

Avvio di una corsa pratica (spostamento zonale)

I passaggi di questa sezione spiegano come avviare un'esercitazione on demand run zonal shift sulla console ARC. Per utilizzare programmaticamente lo zonal shift e lo zonal autoshift, consulta la Guida di riferimento alle API Zonal Shift and Zonal Autoshift.

Puoi avviare una sessione pratica zonal shift dopo aver configurato zonal autoshift e aver creato una configurazione di esecuzione pratica.

Per iniziare un'esercitazione, esegui un turno zonale

1. Apri la console ARC all'indirizzohttps://console.aws.amazon.com/route53recovery/zonalshift/home#/.
2. In Zonal autoshift resources, accedi a una singola risorsa per cui è configurato lo spostamento automatico zonale.
3. Nella pagina di panoramica delle risorse, scegli Inizia l'esercitazione.
4. Seleziona una zona di disponibilità, quindi inserisci un commento per l'esercitazione. L'esercitazione allontanerà il traffico dalla zona di disponibilità selezionata.

5. Scegli Avvia.

Annullamento di un'esercitazione (turno zonale)

I passaggi di questa sezione spiegano come annullare un cambiamento di zona sulla console ARC. Per utilizzare programmaticamente lo zonal shift e lo zonal autoshift, consulta la Guida di riferimento alle API Zonal Shift and Zonal Autoshift.

Puoi annullare i turni zonali o le sessioni di pratica iniziate tu stesso. È inoltre possibile annullare i turni zonali che AWS iniziano per una risorsa destinata a un'esercitazione per lo spostamento automatico di zona.

Per annullare un'esercitazione, esegui un turno zonale.

1. Apri la console ARC all'indirizzohttps://console.aws.amazon.com/route53recovery/zonalshift/home#/.
2. Seleziona un'esercitazione, il turno zonale che desideri annullare, quindi scegli Annulla turno zonale o Annulla esecuzione dell'esercitazione.
3. Nella finestra di dialogo modale di conferma, scegli Conferma.

Abilitazione o disabilitazione della notifica autoshift observer

Puoi configurare lo spostamento automatico zonale in modo che ti avvisi, tramite Amazon EventBridge, ogni volta che AWS avvia uno spostamento automatico per allontanare il traffico da una zona di disponibilità potenzialmente compromessa. Devi configurare questa opzione in Regione AWS ognuna delle quali desideri ricevere notifiche. Non è necessario configurare alcuna risorsa specifica con lo spostamento automatico zonale per abilitare queste notifiche separate. Per ulteriori informazioni, consulta Utilizzo dello spostamento automatico zonale con Amazon EventBridge.

I passaggi di questa sezione spiegano come abilitare la notifica autoshift observer utilizzando la console Amazon Application Recovery Controller (ARC). Per utilizzare l'autoshift zonale a livello di codice, consulta la Guida di riferimento alle API Zonal Shift and Zonal Autoshift.

Per abilitare o disabilitare la notifica autoshift observer

1. Apri la console ARC all'indirizzo. https://console.aws.amazon.com/route53recovery/zonalshift/home#/
2. In Guida introduttiva, scegli Abilita la notifica dell'osservatore con spostamento automatico.

3. Nella finestra di dialogo di conferma, scegli Abilita notifica all'osservatore.

Test dell'autoshift zonale con AWS FIS

Puoi utilizzarlo AWS Fault Injection Service per configurare ed eseguire esperimenti che ti aiutino a simulare condizioni reali, come lo scenario AZ Availability: Power Interruption, che dimostrerà cosa succede quando AWS avvia un cambio automatico zonale sulle risorse abilitate al cambio automatico durante una compromissione della zona Z potenzialmente diffusa.

L'azione start `aws:arc:start-zonal-autoshift` recovery consente di dimostrare come AWS Will sposta automaticamente il traffico, per le risorse zonali abilitate allo spostamento automatico, lontano da una zona di zona potenzialmente compromessa e lo reindirizza verso l'integrità della stessa Regione AWS durante l'esecuzione dello scenario di disponibilità della zona. AZs

Ad esempio, è possibile utilizzare la libreria di AWS FIS scenari per simulare una compromissione della zona di attività causata da un'interruzione dell'alimentazione. In questo esperimento, cinque minuti dopo l'inizio dell'interruzione dell'alimentazione AZ, l'azione di ripristino sposta `aws:arc:start-zonal-autoshift` automaticamente il traffico di risorse lontano dalla zona di disponibilità specificata. Il traffico viene spostato per i restanti 25 minuti dopo l'interruzione dell'alimentazione, per dimostrare come si innescherebbe lo spostamento automatico in caso di problemi di AZ potenzialmente diffusi. Al termine dell'esperimento, lo spostamento del traffico termina e il traffico riprende a fluire verso tutto il suo corso. AZs Questo processo dimostra un ripristino completo da un evento di alimentazione che ha un impatto su una zona AZ.

In che modo gli esperimenti differiscono dalle esecuzioni pratiche di cambio automatico zonale

AWS FIS gli esperimenti differiscono dalle pratiche di spostamento automatico zonale in quanto, durante le esercitazioni, ARC sposta il traffico relativo alla risorsa da una zona di zona all'altra come parte di un normale processo per garantire che l'applicazione possa tollerare la perdita di una AZ. Tuttavia, durante un AWS FIS esperimento, AWS FIS dimostra come verranno attivati per conto dell'utente una compromissione AZ e uno spostamento automatico per le risorse abilitate allo spostamento automatico, quindi annulla l'autoshift quando il problema è stato risolto.

Non AWS è possibile aggiornare uno spostamento zonale avviato dal FIS mentre è in esecuzione. Inoltre, se si annulla uno spostamento zonale al di fuori di AWS FIS, l'esperimento termina. AWS FIS

AWS FIS meccanismo di sicurezza basato sulla scadenza

AWS FIS gestisce lo spostamento di zona utilizzando le operazioni StartZonalShiftUpdateZonalShift, e CancelZonalShiftAPI, con il `expiresIn` campo per queste richieste impostato su 1 minuto come meccanismo di sicurezza. Ciò consente di AWS FIS ripristinare rapidamente lo spostamento zonale in caso di eventi imprevisti, come interruzioni della rete o problemi di sistema. Nella console ARC, il campo del tempo di scadenza verrà visualizzato AWS FIS-managed e la scadenza effettiva prevista è determinata dalla durata specificata nell'azione di spostamento zonale. Per ulteriori informazioni sulle esercitazioni, vedi Come funzionano lo spostamento automatico zonale e le esecuzioni pratiche

Non può essere applicato più di un turno zonale alla volta. Cioè, solo una pratica esegue il cambio di zona, il cambiamento di zona avviato dal cliente, lo spostamento automatico o l'esperimento per la risorsa. AWS FIS Quando viene avviato un secondo spostamento zonale, ARC segue una precedenza per determinare quale tipo di spostamento zonale è valido per una risorsa. Per ulteriori informazioni sulla precedenza per i turni zonali, vedere. Precedenza per i turni zonali

Per ulteriori informazioni sulle azioni di AWS FIS ripristino, fare riferimento all'azione di AWS FIS ripristino nella Guida per l'AWS Fault Injection Service utente.

Registrazione e monitoraggio per lo spostamento automatico zonale in Amazon Application Recovery Controller (ARC)

Puoi usare AWS CloudTrail Amazon EventBridge per monitorare l'autoshift zonale in Amazon Application Recovery Controller (ARC), per analizzare i modelli e aiutare a risolvere i problemi.

Argomenti

- Registrazione delle chiamate API zonal autoshift utilizzando AWS CloudTrail
- Utilizzo dello spostamento automatico zonale con Amazon EventBridge

Registrazione delle chiamate API zonal autoshift utilizzando AWS CloudTrail

Zonal autoshift for ARC è integrato con AWS CloudTrail, un servizio che fornisce una registrazione delle azioni intraprese da un utente, ruolo o servizio in ARC. AWS CloudTrail acquisisce tutte le chiamate API per lo spostamento di zona come eventi. Le chiamate acquisite includono chiamate dalla console ARC e chiamate in codice alle operazioni dell'API ARC per lo spostamento di zona.

Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per lo spostamento zonale. 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, è possibile determinare la richiesta di spostamento di zona effettuata ad ARC, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e altri dettagli.

Per ulteriori informazioni CloudTrail, consulta la Guida per l'AWS CloudTrail utente.

Informazioni sullo spostamento automatico zonale in CloudTrail

CloudTrail è abilitato sul tuo account al Account AWS momento della creazione dell'account. Quando si verifica un'attività in ARC for zonal autoshift, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi di AWS servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare eventi recenti nel tuo. Account AWS Per ulteriori informazioni, consulta Lavorare con la cronologia CloudTrail degli eventi.

Per una registrazione continua degli eventi della tua area Account AWS, compresi gli eventi relativi al cambio automatico di zona in ARC, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando si crea un percorso nella console, questo sarà valido in tutte le Regioni AWS. Il trail registra gli eventi di tutte le regioni della AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica della creazione di un percorso
- CloudTrail servizi e integrazioni supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di CloudTrail registro da più regioni e ricezione di file di CloudTrail registro da più account

Tutte le azioni ARC vengono registrate CloudTrail e documentate nella Routing Control API Reference Guide for Amazon Application Recovery Controller. Ad esempio, le chiamate alle `ListManagedResources` azioni `StartZonalShift` e generano voci nei file di registro. CloudTrail

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con credenziali utente root o AWS Identity and Access Management (IAM).
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro AWS servizio.

Per ulteriori informazioni, consulta Elemento CloudTrail userIdentity.

Visualizzazione degli eventi ARC nella cronologia degli eventi

CloudTrail consente di visualizzare gli eventi recenti nella cronologia degli eventi. Per ulteriori informazioni, consulta Lavorare con la cronologia degli CloudTrail eventi nella Guida AWS CloudTrail per l'utente.

Comprensione delle voci dei file di registro zonali autoshift

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'`ListManagedResources`azione per lo spostamento automatico zonale.


```
{
      "eventVersion": "1.08",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:role/admin",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "sessionIssuer": {
            "type": "Role",
            "principalId": "AROA33L3W36EXAMPLE",
            "arn": "arn:aws:iam::111122223333:role/admin",
            "accountId": "111122223333",
            "userName": "EXAMPLENAME"
```

```
          },
          "webIdFederationData": {},
          "attributes": {
            "creationDate": "2022-11-14T16:01:51Z",
            "mfaAuthenticated": "false"
          }
        }
      },
      "eventTime": "2022-11-14T16:14:41Z",
      "eventSource": "arc-zonal-shift.amazonaws.com",
      "eventName": "ListManagedResources",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.50",
      "userAgent": "Boto3/1.17.101 Python/3.8.10 Linux/4.14.231-180.360.amzn2.x86_64
exec-env/AWS_Lambda_python3.8 Botocore/1.20.102",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "VGXG4ZUE7UZTVCMTJGIAF_EXAMPLE",
      "eventID": "4b5c42df-1174-46c8-be99-d67_EXAMPLE",
      "readOnly": true,
      "eventType": "AwsApiCall",
      "managementEvent": true,
      "recipientAccountId": "111122223333"
      "eventCategory": "Management"
      }
    }
```

Utilizzo dello spostamento automatico zonale con Amazon EventBridge

Con Amazon EventBridge, puoi configurare regole basate sugli eventi che monitorano le tue risorse di spostamento automatico zonale e avviano azioni mirate che utilizzano altri servizi. AWS Ad esempio, puoi impostare una regola per l'invio di notifiche e-mail segnalando un argomento di Amazon SNS quando inizia un'esercitazione per lo spostamento automatico zonale.

Puoi creare regole in Amazon EventBridge per agire sullo spostamento automatico zonale. Un evento per lo spostamento automatico zonale specifica le informazioni sullo stato delle esercitazioni o dei cambi automatici, ad esempio, quando viene avviata un'esercitazione. È possibile configurare l'autoshift zonale per notificare gli eventi di trasferimento automatico zonale per le risorse abilitate per il servizio.

Puoi anche scegliere, in aggiunta o al posto di altre notifiche, di abilitare la notifica autoshift observer, che fornisce un evento di notifica ogni volta che avvia uno spostamento automatico per una zona di

disponibilità potenzialmente compromessa. AWS La notifica di Autoshift Observer è separata dalle notifiche che ricevi quando il traffico per le risorse che hai abilitato per lo spostamento automatico zonale viene spostato da una zona di disponibilità. Non è necessario configurare alcuna risorsa con l'autoshift zonale per abilitare la notifica autoshift observer. Per ulteriori informazioni, consulta Abilitazione e utilizzo dell'autoshift zonale.

Per registrare eventi di spostamento automatico zonale specifici che ti interessano, definisci modelli specifici dell'evento da utilizzare per rilevare gli eventi. EventBridge I pattern di eventi hanno la stessa struttura degli eventi a cui corrispondono. Il modello cita i campi che desideri abbinare e fornisce i valori che stai cercando.

Gli eventi vengono emessi secondo il principio del massimo sforzo. Vengono consegnati da ARC a quasi EventBridge in tempo reale, in normali circostanze operative. Tuttavia, possono verificarsi situazioni che potrebbero ritardare o impedire la consegna di un evento.

Per informazioni su come EventBridge le regole funzionano con i modelli di eventi, consulta Eventi e modelli di eventi in EventBridge.

Monitora una risorsa di spostamento automatico zonale con EventBridge

Con EventBridge, puoi creare regole che definiscono le azioni da intraprendere quando ARC emette eventi per le sue risorse. Ad esempio, è possibile creare una regola che invii un messaggio e-mail all'avvio di un'esercitazione per lo spostamento automatico zonale.

Per digitare o copiare e incollare uno schema di eventi nella EventBridge console, seleziona l'opzione da utilizzare Inserisci la mia opzione nella console. Per aiutarti a determinare i modelli di eventi che potrebbero esserti utili, questo argomento include esempi di modelli di abbinamento degli eventi di spostamento automatico zonale e di eventi di spostamento automatico zonale che puoi utilizzare.

Per creare una regola per un evento risorsa

1. Apri la EventBridge console Amazon all'indirizzo https://console.aws.amazon.com/events/.
2. Scegli la regione in Regione AWS cui vuoi creare la regola, ovvero la regione per cui ti interessa guardare gli eventi.
3. Scegliere Create rule (Crea regola).
4. Immettere un Name (Nome) per la regola e, facoltativamente, una descrizione.
5. Per Event bus, lascia il valore predefinito, default.
6. Scegli Next (Successivo).

7. Per il passo Build event pattern, per Event source, lascia il valore predefinito, AWS events.
8. In Evento di esempio, scegli Inserisci il mio.
9. Per gli eventi di esempio, digita o copia e incolla un modello di evento.

Esempi di modelli di eventi di spostamento automatico zonale

I pattern di eventi hanno la stessa struttura degli eventi a cui corrispondono. Il modello cita i campi che desideri abbinare e fornisce i valori che stai cercando.

È possibile copiare e incollare i modelli di eventi da questa sezione EventBridge per creare regole da utilizzare per monitorare le azioni e le risorse di spostamento automatico zonale.

Quando create modelli di eventi per eventi di trasferimento automatico zonale, potete specificare una delle seguenti opzioni per: `detail-type`

- `Autoshift In Progress`
- `Autoshift Completed`
- `Practice Run Started`
- `Practice Run Succeeded`
- `Practice Run Interrupted`
- `Practice Run Failed`
- `FIS Experiment Autoshift In Progress`
- `FIS Experiment Autoshift Completed`
- `FIS Experiment Autoshift Canceled`
- `Manual Shift Started`
- `Manual Shift Updated`
- `Manual Shift Canceled`

Quando un'esercitazione viene interrotta, per ulteriori informazioni sulla causa dell'interruzione, consulta il campo. `additionalFailureInfo`

Puoi scegliere di monitorare tutti gli spostamenti automatici abilitando le AWS notifiche autoshift observer. Dopo aver abilitato la notifica dell'autoshift observer, per ricevere le notifiche, scegli

di ricevere una notifica per il tipo di dettaglio zonale dello spostamento automatico. `Autoshift In Progress` Per vedere i passaggi per abilitare la notifica dell'osservatore con spostamento automatico, consulta. Abilitazione e utilizzo dell'autoshift zonale

Per alcuni esempi, consulta la sezione Esempi di eventi di spostamento automatico zonale.

- Seleziona tutti gli eventi dallo spostamento automatico zonale in cui è iniziato un cambio automatico.

  Tenere presente quanto segue:

  - Se hai abilitato la notifica autoshift observer, ARC restituisce tutti gli eventi di trasferimento automatico.
  - Se non hai abilitato la notifica autoshift observer, ARC restituisce gli eventi di spostamento automatico solo quando una risorsa che hai configurato per lo spostamento automatico zonale è inclusa in un cambio automatico.

```
{
    "source": [
        "aws.arc-zonal-shift"
    ],
    "detail-type": [
        "Autoshift In Progress"
    ]
}
```

- Seleziona tutti gli eventi dallo spostamento automatico zonale in cui è iniziata un'esercitazione.

```
{
    "source": [
        "aws.arc-zonal-shift"
    ],
    "detail-type": [
        "Practice Run Started"
    ]
}
```

- Seleziona tutti gli eventi dal cambio automatico zonale in cui un'esercitazione non è riuscita.

```
{
    "source": [
        "aws.arc-zonal-shift"
```

```
    ],
    "detail-type": [
        "Practice Run Failed"
    ]
}
```

Esempi di eventi di spostamento automatico zonale

Questa sezione include eventi di esempio per azioni di cambio automatico zonale.

Di seguito è riportato un esempio di evento relativo all'`Autoshift In Progress`azione, quando 1) la notifica autoshift observer è abilitata e 2) non è stata configurata una risorsa con cambio automatico zonale inclusa in un cambio automatico:

```
{
    "version": "0",
    "id": "05d4d2d5-9c76-bfea-72d2-d4614802adb4",
    "detail-type": "Autoshift In Progress",
    "source": "aws.arc-zonal-shift",
    "account": "111122223333",
    "time": "2023-11-16T23:38:14Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "version": "0.0.1",
        "data": "",
        "metadata": {
            "awayFrom": "use1-az2",
            "notes":"AWS has started an autoshift for an impaired Availability Zone.
 This notification
            is separate from autoshift notifications for resources, if any, that you
 have configured for
            zonal autoshift. For details, see the Developer Guide."
        }
    }
}
```

Di seguito è riportato un esempio di evento per l'`Autoshift In Progress`azione, quando 1) la notifica autoshift observer è disabilitata e 2) è stata configurata una risorsa con autoshift zonale inclusa in un cambio automatico:

```
{
    "version": "0",
    "id": "05d4d2d5-9c76-bfea-72d2-d4614802adb4",
    "detail-type": "Autoshift In Progress",
    "source": "aws.arc-zonal-shift",
    "account": "111122223333",
    "time": "2023-11-16T23:38:14Z",
    "region": "us-east-1",
    "resources": [
        "TEST-EXAMPLE-2023-11-16-23-28-11-5"
    ],
    "detail": {
        "version": "0.0.1",
        "data": "",
        "metadata": {
            "awayFrom": "use1-az2",
            "notes":""
        }
    }
}
```

Di seguito è riportato un esempio di evento relativo all'azione: `Practice Run Interrupted`

```
{
    "version": "0",
    "id": "05d4d2d5-9c76-bfea-72d2-d4614802adb4",
    "detail-type": "Practice Run Interrupted",
    "source": "aws.arc-zonal-shift",
    "account": "111122223333",
    "time": "2023-11-16T23:38:14Z",
    "region": "us-east-1",
    "resources": [
        "TEST-EXAMPLE-2023-11-16-23-28-11-5"
    ],
    "detail": {
        "version": "0.0.1",
        "data": {
            "additionalFailureInfo": "Practice run interrupted. The blocking alarm
 entered ALARM state."
        },
        "metadata": {
            "awayFrom": "use1-az2"
        }
```

```
    }
}
```

Di seguito è riportato un esempio di evento relativo all'`FIS Experiment Autoshift In Progress`azione:

```
{
    "version": "0",
    "id": "05d4d2d5-9c76-bfea-72d2-d4614802adb4",
    "detail-type": "FIS Experiment Autoshift In Progress",
    "source": "aws.arc-zonal-shift",
    "account": "111122223333",
    "time": "2023-11-16T23:38:14Z",
    "region": "us-east-1",
    "resources": [
        "TEST-EXAMPLE-2023-11-16-23-28-11-5"
    ],
    "detail": {
        "version": "0.0.1",
        "data": "",
        "metadata": {
            "awayFrom": "use1-az2",
            "notes":""
        }
    }
}
```

Di seguito è riportato un esempio di evento relativo all'`Manual Shift Started`azione. Viene emesso quando l'`StartZonalShift`API viene chiamata su una risorsa:

```
{
    "version": "0",
    "id": "05d4d2d5-9c76-bfea-72d2-d4614802adb4",
    "detail-type": "Manual Shift Started",
    "source": "aws.arc-zonal-shift",
    "account": "111122223333",
    "time": "2023-11-16T23:38:14Z",
    "region": "us-east-1",
    "resources": [
        "TEST-EXAMPLE-2023-11-16-23-28-11-5"
    ],
    "detail": {
```

```
        "version": "0.0.1",
        "data": "",
        "metadata": {
            "awayFrom": "use1-az2",
            "notes":""
        }
    }
}
```

Specificare un gruppo di CloudWatch log da utilizzare come destinazione

Quando si crea una EventBridge regola, è necessario specificare la destinazione a cui vengono inviati gli eventi corrispondenti alla regola. Per un elenco degli obiettivi disponibili per EventBridge, vedi Target disponibili nella EventBridge console. Uno degli obiettivi che puoi aggiungere a una EventBridge regola è un gruppo di CloudWatch log Amazon. Questa sezione descrive i requisiti per aggiungere gruppi di CloudWatch log come destinazioni e fornisce una procedura per aggiungere un gruppo di log quando si crea una regola.

Per aggiungere un gruppo di CloudWatch log come destinazione, è possibile effettuare una delle seguenti operazioni:

- Creare un nuovo gruppo di log
- Scegli un gruppo di log esistente

Se specifichi un nuovo gruppo di log utilizzando la console quando crei una regola, crea EventBridge automaticamente il gruppo di log per te. Assicurati che il gruppo di log che usi come destinazione per la EventBridge regola inizi con`/aws/events`. Se desideri scegliere un gruppo di log esistente, tieni presente che solo i gruppi di log che iniziano con `/aws/events` appaiono come opzioni nel menu a discesa. Per ulteriori informazioni, consulta Creare un nuovo gruppo di log nella Amazon CloudWatch User Guide.

Se crei o utilizzi un gruppo di CloudWatch log da utilizzare come destinazione utilizzando CloudWatch operazioni esterne alla console, assicurati di impostare le autorizzazioni correttamente. Se utilizzi la console per aggiungere un gruppo di log a una EventBridge regola, la politica basata sulle risorse per il gruppo di log viene aggiornata automaticamente. Tuttavia, se si utilizza AWS Command Line Interface o un AWS SDK per specificare un gruppo di log, è necessario aggiornare la politica basata sulle risorse per il gruppo di log. La seguente politica di esempio illustra le autorizzazioni che è necessario definire in una politica basata sulle risorse per il gruppo di log:

JSON

```
{
    "Version":"2012-10-17",

    "Statement": [
        {
            "Action": [
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "events.amazonaws.com",
                    "delivery.logs.amazonaws.com"
                ]
            },
            "Resource": "arn:aws:logs:us-east-1:222222222222:log-group:/aws/
events/*:*",
            "Sid": "TrustEventsToStoreLogEvent"
        }
    ]
}
```

Non è possibile configurare una politica basata sulle risorse per un gruppo di log utilizzando la console. Per aggiungere le autorizzazioni richieste a una politica basata sulle risorse, utilizza l'operazione API. CloudWatch PutResourcePolicy Quindi, puoi utilizzare il comando describe-resource-policiesCLI per verificare che la tua politica sia stata applicata correttamente.

Per creare una regola per un evento di risorsa e specificare un target per un gruppo di CloudWatch log

1. Apri la EventBridge console Amazon all'indirizzo https://console.aws.amazon.com/events/.
2. Scegli Regione AWS quello in cui vuoi creare la regola.
3. Scegli Crea regola e inserisci tutte le informazioni su quella regola, come lo schema dell'evento o i dettagli della pianificazione.

Per ulteriori informazioni sulla creazione di EventBridge regole per ARC, consulta le sezioni precedenti di questo argomento.

4. Nella pagina Seleziona destinazione, scegli CloudWatchcome obiettivo.
5. Scegli un gruppo di CloudWatch log dal menu a discesa.

Identity and Access Management per lo spostamento automatico zonale in ARC

AWS Identity and Access Management (IAM) è un dispositivo 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 le risorse ARC. IAM è uno Servizio AWS strumento che puoi utilizzare senza costi aggiuntivi.

Indice

- Come funziona l'autoshift zonale in ARC con IAM
- Esempi di policy basate sull'identità per lo spostamento automatico zonale in ARC
- Utilizzo del ruolo collegato al servizio per lo spostamento automatico zonale in ARC
- AWS politiche gestite per lo spostamento automatico zonale in ARC

Come funziona l'autoshift zonale in ARC con IAM

Prima di utilizzare IAM per gestire l'accesso all'autoshift zonale in Amazon Application Recovery Controller (ARC), scopri quali funzionalità IAM sono disponibili per l'uso con l'autoshift zonale.

Funzionalità IAM che puoi utilizzare con l'autoshift zonale in ARC

Funzionalità IAM	Supporto per lo spostamento automatico zonale
Policy basate sull'identità	Sì
Policy basate su risorse	No
Operazioni di policy	Sì

Funzionalità IAM	Supporto per lo spostamento automatico zonale
Risorse relative alle policy	Sì
Chiavi di condizione delle policy	Sì
ACLs	No
ABAC (tag nelle policy)	Parziale
Credenziali temporanee	Sì
Autorizzazioni del principale	Sì
Ruoli di servizio	No
Ruoli collegati al servizio	Sì

Per avere una visione generale di alto livello di come AWS i 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 ARC

Supporta le policy basate sull'identità: sì

Le policy basate sull'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 di IAM.

Con le policy basate sull'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. 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 IAM.

Per visualizzare esempi di politiche basate sull'identità ARC, vedere. Esempi di policy basate sull'identità in Amazon Application Recovery Controller (ARC)

Politiche basate sulle risorse all'interno di ARC

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 di 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.

Azioni politiche per ARC

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

Per visualizzare un elenco di azioni ARC per lo spostamento automatico zonale, consulta Azioni definite da Amazon Route 53 Zonal Shift nel Service Authorization Reference.

Le azioni politiche in ARC per lo spostamento automatico zonale utilizzano i seguenti prefissi prima dell'azione:

```
arc-zonal-shift
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola. Ad esempio, quanto segue:

```
"Action": [
      "arc-zonal-shift:action1",
      "arc-zonal-shift:action2"
         ]
```

È possibile specificare più azioni tramite caratteri jolly (*). Ad esempio, per specificare tutte le azioni che iniziano con la parola `Describe`, includi la seguente azione:

```
"Action": "arc-zonal-shift:Describe*"
```

Per visualizzare esempi di politiche basate sull'identità ARC per lo spostamento automatico zonale, vedere. Esempi di policy basate sull'identità per lo spostamento automatico zonale in ARC

Risorse politiche per il trasferimento automatico zonale in ARC

Supporta le risorse relative alle policy: sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità 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. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). Per le azioni che non supportano le autorizzazioni a livello di risorsa, si utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

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

Per visualizzare un elenco dei tipi di risorse e delle relative ARNs azioni e le azioni che è possibile specificare con l'ARN di ciascuna risorsa, vedere il seguente argomento nel Service Authorization Reference:

- Azioni definite da Amazon Route 53 - Zonal Shift

Per visualizzare le azioni e le risorse che puoi utilizzare con una chiave di condizione, consulta il seguente argomento nel Service Authorization Reference:

- Chiavi di condizione definite da Amazon Route 53 - Zonal Shift

Per visualizzare esempi di politiche ARC basate sull'identità per lo spostamento automatico zonale, consulta. Esempi di policy basate sull'identità per lo spostamento automatico zonale in ARC

Chiavi relative alle condizioni delle policy per lo spostamento automatico zonale in ARC

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 entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento `Condition` specifica quando le istruzioni vengono eseguite in base a criteri definiti. 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. 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 ARC per lo spostamento automatico zonale, consulta i seguenti argomenti nel Service Authorization Reference:

- Chiavi delle condizioni per Amazon Route 53 Zonal Shift

Per visualizzare le azioni e le risorse che puoi utilizzare con una chiave di condizione, consulta i seguenti argomenti nel Service Authorization Reference:

- Azioni definite da Amazon Route 53 Zonal Shift

Per visualizzare esempi di politiche ARC basate sull'identità per lo spostamento automatico zonale, consulta. Esempi di policy basate sull'identità per lo spostamento automatico zonale in ARC

Liste di controllo degli accessi () in ARC ACLs

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.

Controllo degli accessi basato sugli attributi (ABAC) con ARC

Supporta ABAC (tag nelle policy): parzialmente

Il controllo degli accessi basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi, chiamati tag. Puoi allegare tag a entità e AWS risorse IAM, quindi progettare politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag sulla risorsa.

Per controllare l'accesso basato su tag, fornire 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 Sì. Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per maggiori informazioni su ABAC, consulta Definizione delle autorizzazioni con autorizzazione ABAC nella Guida per l'utente di 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.

L'autoshift zonale in ARC include il seguente supporto parziale per ABAC:

- L'autoshift zonale supporta ABAC per le risorse gestite registrate in ARC per lo spostamento zonale. Per ulteriori informazioni sulle risorse gestite di ABAC for Network Load Balancer e Application Load Balancer, consulta ABAC with Elastic Load Balancing nella Elastic Load Balancing User Guide.

Utilizzo di credenziali temporanee con ARC

Supporta le credenziali temporanee: sì

Le credenziali temporanee forniscono un accesso a breve termine alle AWS risorse e vengono create automaticamente quando si utilizza la federazione o si cambia ruolo. AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza temporanee in IAM e Servizi AWS compatibili con IAM nella Guida per l'utente IAM.

Autorizzazioni principali multiservizio per ARC

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

Quando utilizzi un'entità IAM (utente o ruolo) per eseguire azioni AWS, sei considerato un principale. Le policy concedono autorizzazioni a un'entità. Quando si utilizzano alcuni servizi, è possibile eseguire un'azione che attiva un'altra azione in un servizio diverso. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni.

Per vedere se un'azione richiede azioni dipendenti aggiuntive in una policy, consulta il seguente argomento nel Service Authorization Reference:

- Spostamento zonale Amazon Route 53

Ruoli di servizio per ARC

Supporta i ruoli di servizio: no

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 Create a role to delegate permissions to an Servizio AWS nella Guida per l'utente IAM.

Ruoli collegati ai servizi per ARC

Supporta i ruoli collegati ai servizi: sì

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'operazione 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 al servizio, ma non modificarle.

Per informazioni dettagliate sulla creazione o la gestione di ruoli collegati ai servizi ARC, consulta. Utilizzo del ruolo collegato al servizio per lo spostamento automatico zonale in ARC

Per ulteriori informazioni su come creare e gestire i ruoli collegati ai servizi, consulta Servizi AWS supportati da IAM. Trova un servizio nella tabella che include un `Yes` nella colonna Service-linked role (Ruolo collegato ai servizi). Scegli il collegamento Sì per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Esempi di policy basate sull'identità per lo spostamento automatico zonale in ARC

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare risorse ARC. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM.

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 di IAM.

Per dettagli sulle azioni e sui tipi di risorse definiti da ARC, incluso il formato di ARNs per ogni tipo di risorsa, consulta Azioni, risorse e chiavi di condizione per Amazon Application Recovery Controller (ARC) nel Service Authorization Reference.

Argomenti

- Best practice per le policy
- Esempio: accesso alla console Zonal Autoshift
- Esempi: azioni dell'API ARC

Best practice per le policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare le risorse ARC nel tuo account. Queste azioni possono comportare costi aggiuntivi per l' Account AWS. Quando si creano o modificano policy basate sull'identità, seguire 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 maggiori informazioni, consulta Policy gestite da AWS o Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente di IAM.
- Applicazione delle autorizzazioni con privilegio minimo - Quando si impostano le autorizzazioni con le policy IAM, concedere 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 privilegio minimo. Per maggiori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso - Per limitare l'accesso ad azioni e risorse è possibile aggiungere una condizione alle 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 CloudFormation. Per maggiori informazioni, consultare la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente di IAM.
- Utilizzo dello strumento di analisi degli accessi IAM per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali - Lo strumento di analisi degli accessi IAM convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio (JSON) della policy IAM e alle best practice di IAM. Lo strumento di analisi degli accessi IAM offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per maggiori informazioni, consultare Convalida delle policy per il Sistema di analisi degli accessi IAM nella Guida per l'utente di 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, aggiungere le condizioni MFA alle policy. Per maggiori informazioni, consultare Protezione dell'accesso API con MFA nella Guida per l'utente di IAM.

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

Esempio: accesso alla console Zonal Autoshift

Per accedere alla console Amazon Application Recovery Controller (ARC), devi disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle risorse ARC 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 agli utenti che effettuano chiamate solo verso AWS CLI o l' AWS API. Al contrario, è opportuno concedere l'accesso solo alle azioni che corrispondono all'operazione API che stanno cercando di eseguire.

Per eseguire alcune attività, gli utenti devono disporre dell'autorizzazione per creare il ruolo collegato al servizio associato allo spostamento automatico zonale in ARC. Per ulteriori informazioni, consulta Utilizzo del ruolo collegato al servizio per lo spostamento automatico zonale in ARC.

Per consentire agli utenti l'accesso completo all'utilizzo dell'autoshift zonale in Console di gestione AWS, allega all'utente una politica come la seguente:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                   "arc-zonal-shift:ListManagedResources",
                   "arc-zonal-shift:GetManagedResource",
                   "arc-zonal-shift:ListZonalShifts",
                   "arc-zonal-shift:StartZonalShift",
                   "arc-zonal-shift:UpdateZonalShift",
                   "arc-zonal-shift:CancelZonalShift",
                   "arc-zonal-shift:CreatePracticeRunConfiguration",
                   "arc-zonal-shift:DeletePracticeRunConfiguration",
                   "arc-zonal-shift:ListAutoshifts",
                   "arc-zonal-shift:UpdatePracticeRunConfiguration",
                   "arc-zonal-shift:UpdateZonalAutoshiftConfiguration"
             ],
```

```
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeAvailabilityZones",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "cloudwatch:DescribeAlarms",
            "Resource": "*"
        }
    ]
}
```

Esempi: azioni dell'API ARC

È possibile utilizzare una policy per garantire che un utente possa utilizzare le azioni dell'API ARC per lo spostamento automatico zonale per configurare lo AWS spostamento automatico zonale in modo da spostare il traffico delle risorse delle applicazioni da una zona di disponibilità, per conto dell'utente, a quello integro AZs nella, per ridurre i tempi di ripristino durante gli Regione AWS eventi. Per fornire queste autorizzazioni, allega una policy che corrisponda alle operazioni API con cui l'utente deve lavorare, come descritto di seguito.

Per eseguire alcune attività, gli utenti devono disporre delle autorizzazioni per il ruolo collegato al servizio associato ad ARC. Le autorizzazioni necessarie per creare il ruolo collegato al servizio sono incluse nella seguente politica di esempio. Per ulteriori informazioni, consulta Utilizzo del ruolo collegato al servizio per lo spostamento automatico zonale in ARC.

Per utilizzare le operazioni API per lo spostamento automatico zonale, allega all'utente una policy come la seguente:

JSON

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

```
                    "arc-zonal-shift:ListManagedResources",
                    "arc-zonal-shift:GetManagedResource",
                    "arc-zonal-shift:ListZonalShifts",
                    "arc-zonal-shift:StartZonalShift",
                    "arc-zonal-shift:UpdateZonalShift",
                    "arc-zonal-shift:CancelZonalShift",
                    "arc-zonal-shift:CreatePracticeRunConfiguration",
                    "arc-zonal-shift:DeletePracticeRunConfiguration",
                    "arc-zonal-shift:ListAutoshifts",
                    "arc-zonal-shift:UpdatePracticeRunConfiguration",
                    "arc-zonal-shift:UpdateZonalAutoshiftConfiguration"
                ],
                "Resource": "*"
            },
            {
                "Effect" : "Allow",
                "Action" : [
                        "cloudwatch:DescribeAlarms",
                        "health:DescribeEvents"
                ],
                "Resource" : "*"
            },
            {
                "Effect" : "Allow",
                "Action" : [
                        "arc-zonal-shift:CancelZonalShift",
                        "arc-zonal-shift:GetManagedResource",
                        "arc-zonal-shift:StartZonalShift",
                        "arc-zonal-shift:UpdateZonalShift"
                ],
                "Resource" : "*"
            }
        ]
}
```

Utilizzo del ruolo collegato al servizio per lo spostamento automatico zonale in ARC

L'autoshift zonale in Amazon Application Recovery Controller utilizza AWS Identity and Access Management un ruolo collegato al servizio (IAM). Un ruolo collegato al servizio è un tipo unico di ruolo IAM collegato direttamente a un servizio, in questo caso ARC. Il ruolo collegato al servizio è predefinito da ARC e include tutte le autorizzazioni richieste dal servizio per chiamare altri AWS servizi per conto dell'utente per scopi specifici.

Un ruolo collegato al servizio semplifica la configurazione di ARC perché non è necessario aggiungere manualmente le autorizzazioni necessarie. ARC definisce le autorizzazioni per il ruolo collegato al servizio e, se non diversamente definito, solo ARC può assumerne i ruoli. Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere collegata a nessun'altra entità IAM.

È possibile eliminare un ruolo collegato ai servizi solo dopo aver eliminato le risorse correlate. Questo protegge le tue risorse ARC zonali autoshift perché non puoi rimuovere inavvertitamente l'autorizzazione ad accedere alle risorse.

Per informazioni su altri servizi che supportano i ruoli collegati ai servizi, consulta AWS Servizi che funzionano con IAM e cerca i servizi con Sì nella colonna Ruolo collegato ai servizi. Scegli Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Autorizzazioni di ruolo collegate ai servizi per AWSService RoleForZonalAutoshiftPracticeRun

ARC utilizza il ruolo collegato al servizio denominato AWSServiceRoleForZonalAutoshiftPracticeRunper effettuare le seguenti operazioni:

- Monitora gli CloudWatch allarmi Amazon forniti dai clienti e Health Dashboard gli eventi dei clienti per le sessioni di prova
- Gestisci le sessioni di pratica (pratica i turni zonali)

Questa sezione descrive le autorizzazioni per il ruolo collegato al servizio e le informazioni sulla creazione, la modifica e l'eliminazione del ruolo.

Autorizzazioni di ruolo collegate al servizio per AWSService RoleForZonalAutoshiftPracticeRun

Questo ruolo collegato al servizio utilizza la policy gestita. `AWSZonalAutoshiftPracticeRunSLRPolicy`

Ai fini dell'assunzione del ruolo, il ruolo collegato ai servizi AWSServiceRoleForZonalAutoshiftPracticeRun considera attendibile il seguente servizio:

- `practice-run.arc-zonal-shift.amazonaws.com`

Per vedere le autorizzazioni per questa policy, consulta AWSZonalAutoshiftPracticeRunSLRPolicy nella Guida di riferimento sulle policy gestite da AWS .

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Creazione del ruolo collegato al AWSServiceRoleForZonalAutoshiftPracticeRunservizio per ARC

Non devi creare manualmente il ruolo collegato al servizio AWSServiceRoleForZonalAutoshiftPracticeRun. Quando create la configurazione della prima esecuzione pratica in Console di gestione AWS, il o un AWS SDK AWS CLI, ARC crea automaticamente il ruolo collegato al servizio.

Se elimini questo ruolo collegato ai servizi, è possibile ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Quando crei la prima configurazione di esecuzione pratica, ARC crea nuovamente il ruolo collegato al servizio per te.

Modifica del ruolo collegato al AWSServiceRoleForZonalAutoshiftPracticeRunservizio per ARC

ARC non consente di modificare il ruolo collegato al AWSServiceRoleForZonalAutoshiftPracticeRunservizio. Dopo aver creato il ruolo collegato al servizio, non è possibile modificare il nome del ruolo perché altre entità potrebbero farvi riferimento. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Eliminazione del ruolo collegato al AWSServiceRoleForZonalAutoshiftPracticeRunservizio per ARC

Se non è più necessario utilizzare una funzionalità o un servizio che richiede un ruolo collegato al servizio, ti consigliamo di eliminare il ruolo. In questo modo non sarà più presente un'entità non utilizzata che non viene monitorata e gestita attivamente. Tuttavia, è necessario ripulire le risorse per un ruolo collegato al servizio prima di poterlo eliminare manualmente.

Dopo aver disabilitato lo spostamento automatico, puoi eliminare il ruolo collegato al servizio. AWSServiceRoleForZonalAutoshiftPracticeRun Per ulteriori informazioni sulla funzionalità di trasferimento automatico, vedere. Zonal shift in ARC

> **Note**
>
> Se il servizio ARC utilizza il ruolo quando si tenta di eliminare le risorse, l'eliminazione del ruolo di servizio potrebbe non riuscire. In tal caso, attendi qualche minuto e riprova a eliminare il ruolo.

Per eliminare manualmente il ruolo collegato ai servizi mediante IAM

Utilizza la console IAM AWS CLI, o l' AWS API per eliminare il ruolo AWSService RoleForZonalAutoshiftPracticeRun collegato al servizio. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato al servizio nella Guida per l'utente di IAM.

Aggiornamenti al ruolo ARC collegato al servizio per lo spostamento automatico zonale

Per gli aggiornamenti alle politiche AWS gestite per i ruoli collegati ai servizi ARC, consulta la tabella degli aggiornamenti delle politiche gestite per ARC.AWS È inoltre possibile abbonarsi agli avvisi RSS automatici nella pagina della cronologia dei documenti ARC.

AWS politiche gestite per lo spostamento automatico zonale in ARC

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 Si consiglia pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente specifiche per i propri 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, consultare Policy gestite da AWS nella Guida per l'utente di IAM.

AWS politica gestita: AWSZonal AutoshiftPracticeRun SLRPolicy

Non è possibile collegare `AWSZonalAutoshiftPracticeRunSLRPolicy`alle entità IAM. Questa policy è associata a un ruolo collegato al servizio che consente ad Amazon Application Recovery Controller (ARC) di eseguire le seguenti operazioni per l'autoshift zonale:

- Monitora gli CloudWatch allarmi Amazon forniti dai clienti e Health Dashboard gli eventi dei clienti per le sessioni di prova
- Gestisci le sessioni di pratica (pratica i turni zonali)

- Gestisci controlli bilanciati della capacità per le sessioni di pratica e i turni automatici

Per ulteriori informazioni, consulta Utilizzo del ruolo collegato al servizio per lo spostamento automatico zonale in ARC.

Aggiornamenti per le politiche AWS gestite per lo spostamento automatico zonale

Per i dettagli sugli aggiornamenti alle politiche AWS gestite per lo spostamento automatico zonale in ARC da quando questo servizio ha iniziato a tenere traccia di queste modifiche, vedere. Aggiornamenti alle politiche AWS gestite per Amazon Application Recovery Controller (ARC) Per avvisi automatici sulle modifiche a questa pagina, iscriviti al feed RSS nella pagina della cronologia dei documenti ARC.

Quote per lo spostamento automatico zonale

L'autoshift zonale in Amazon Application Recovery Controller (ARC) è soggetto alle seguenti quote.

Entità	Quota
Numero di allarmi di esito per configurazione dell'esecuzione pratica	10 Puoi richiedere un aumento della quota.
Numero di allarmi di blocco per configurazione dell'esecuzione pratica	10 Puoi richiedere un aumento della quota.

Usa il controllo del routing per ripristinare applicazioni multiregionali in ARC

Questa sezione spiega come utilizzare la funzionalità di controllo del routing in Amazon Application Recovery Controller (ARC) per ridurre al minimo le interruzioni e contribuire a fornire continuità agli utenti quando un' AWS applicazione è distribuita in più applicazioni. Regioni AWS

Puoi anche conoscere il Readiness Check, una funzionalità di ARC che puoi utilizzare per capire se le tue applicazioni e risorse sono pronte per il ripristino.

Gli argomenti di questa sezione descrivono le funzionalità di controllo del routing e di controllo della disponibilità, come configurarle e come utilizzarle.

Argomenti

- Controllo del routing in ARC
- Controllo di prontezza in ARC
- Cambio di regione in ARC

Controllo del routing in ARC

Per eseguire il failover del traffico verso più repliche di applicazioni Regioni AWS, puoi utilizzare i controlli di routing in Amazon Application Recovery Controller (ARC) che sono integrati con un tipo specifico di controllo dello stato di salute in Amazon Route 53. I controlli di routing sono semplici switch on-off che consentono di spostare il traffico client da una replica regionale all'altra. Il reindirizzamento del traffico viene eseguito mediante controlli di integrità del controllo del routing configurati con i record DNS di Amazon Route 53. Ad esempio, i record di failover DNS, associati ai nomi di dominio utilizzati per le repliche delle applicazioni in ogni regione.

Questa sezione spiega come funziona il controllo del routing, come configurare i componenti di controllo del routing e come utilizzarli per reindirizzare il traffico per il failover.

I componenti di controllo del routing in ARC sono: cluster, pannelli di controllo, controlli di routing e controlli dello stato del controllo del routing. Tutti i controlli di routing sono raggruppati su pannelli di controllo. È possibile raggrupparli nel pannello di controllo predefinito creato da ARC per il cluster oppure creare pannelli di controllo personalizzati. È necessario creare un cluster prima di poter creare

un pannello di controllo o un controllo di routing. Ogni cluster in ARC è un piano dati di endpoint su cinque. Regioni AWS

Dopo aver creato i controlli di routing e i controlli di integrità del controllo del routing, è possibile creare regole di sicurezza per il controllo del routing per prevenire gli effetti collaterali involontari dell'automazione del ripristino. È possibile aggiornare gli stati di controllo del routing per reindirizzare il traffico, singolarmente o in batch, utilizzando le azioni AWS CLI o API (consigliato) o utilizzando il. Console di gestione AWS

Questa sezione spiega come funzionano i controlli di routing e come crearli e utilizzarli per reindirizzare il traffico per l'applicazione.

> **Important**
>
> Per ulteriori informazioni su come prepararsi a utilizzare ARC per reindirizzare il traffico come parte di un piano di failover per l'applicazione in uno scenario di emergenza, consulta. Le migliori pratiche per il controllo del routing in ARC

Informazioni sul controllo del routing

Il controllo del routing reindirizza il traffico utilizzando i controlli di integrità in Amazon Route 53 configurati con record DNS associati alla risorsa di primo livello delle celle del gruppo di ripristino, come un sistema di bilanciamento del carico Elastic Load Balancing. È possibile reindirizzare il traffico da una cella all'altra, ad esempio aggiornando uno stato di controllo del routing su `Off` (per interrompere il flusso di traffico verso una cella) e aggiornando un altro stato di controllo del routing su 0n (per avviare il flusso di traffico verso un'altra). Il processo che modifica il flusso del traffico è il controllo dello stato della Route 53 associato al controllo del routing, dopo che ARC lo ha aggiornato per impostarlo come integro o meno, in base allo stato di controllo del routing corrispondente.

I controlli di routing supportano il failover su qualsiasi AWS servizio dotato di un endpoint DNS. È possibile aggiornare gli stati di controllo del routing per eseguire il failover del traffico per il disaster recovery, quando si rilevano cali di latenza per l'applicazione o altri problemi.

Puoi anche configurare le regole di sicurezza per il controllo del routing, per assicurarti che il reindirizzamento del traffico utilizzando i controlli di routing non comprometta la disponibilità. Per ulteriori informazioni, consulta Creazione di regole di sicurezza per il controllo del routing.

È importante notare che i controlli di routing non sono di per sé controlli di integrità che monitorano lo stato di base degli endpoint. Ad esempio, a differenza di un controllo dello stato di Route 53, un

controllo di routing non monitora i tempi di risposta o i tempi di connessione TCP. Un controllo del routing è un semplice interruttore di accensione e spegnimento che controlla un controllo dello stato di salute. In genere, si modifica lo stato per reindirizzare il traffico e tale modifica di stato sposta il traffico verso un particolare endpoint per l'intero stack di applicazioni o impedisce il routing verso l'intero stack di applicazioni. Ad esempio, in uno scenario semplice, quando modificate lo stato di controllo del routing da `On` a `Off`, viene aggiornato un controllo dello stato di Route 53, che avete associato a un record di failover DNS per spostare il traffico da un endpoint.

Come utilizzare il controllo del routing

Per aggiornare lo stato di controllo del routing, in modo da poter reindirizzare il traffico, è necessario connettersi a uno degli endpoint del cluster in ARC. Se l'endpoint a cui tenti di connetterti non è disponibile, prova a cambiare lo stato con un altro endpoint del cluster. Il processo di modifica degli stati di controllo del routing dovrebbe essere pronto a provare ogni endpoint a rotazione, poiché gli endpoint del cluster vengono alternati tra gli stati disponibili e non disponibili per manutenzione e aggiornamenti regolari.

Quando si creano controlli di routing, si configurano i record DNS in modo da associare i controlli di integrità del controllo di routing ai nomi DNS di Route 53 presenti nella replica di ogni applicazione. Ad esempio, per controllare i failover del traffico su due sistemi di bilanciamento del carico, uno in ciascuna delle due regioni, si creano due controlli di integrità del controllo del routing e li si associa a due record DNS, ad esempio record Alias con politiche di routing di failover, con i nomi di dominio dei rispettivi sistemi di bilanciamento del carico.

È inoltre possibile configurare scenari di failover del traffico più complessi utilizzando il controllo del routing ARC insieme ai controlli di integrità e ai set di record DNS di Route 53, utilizzando record DNS con politiche di routing ponderate. Per un esempio dettagliato, consulta la sezione sul failover del traffico utente nel seguente post di AWS blog: Creazione di applicazioni altamente resilienti utilizzando Amazon Application Recovery Controller (ARC), parte 2: Stack multiregionale

Quando avvii un failover per un controllo del routing in Regione AWS uso, a causa delle fasi relative al flusso del traffico, potresti non vedere immediatamente il traffico uscire dalla regione. Inoltre, il completamento delle connessioni esistenti e in corso nella regione può richiedere un breve periodo di tempo, a seconda del comportamento del client e del riutilizzo della connessione. A seconda delle impostazioni DNS e di altri fattori, le connessioni esistenti possono essere completate in pochi minuti o potrebbero richiedere più tempo. Per ulteriori informazioni, consulta Garantire che i cambiamenti di traffico finiscano rapidamente.

Vantaggi del controllo del routing

Un controllo del routing in ARC presenta diversi vantaggi rispetto al reindirizzamento del traffico con i controlli sanitari tradizionali. Esempio:

- Un controllo del routing consente di eseguire il failover di un intero stack di applicazioni. Ciò è in contrasto con il failover dei singoli componenti di uno stack, come fanno le istanze Amazon EC2, sulla base di controlli dello stato a livello di risorsa.
- Il controllo del routing ti offre un override manuale semplice e sicuro che puoi utilizzare per spostare il traffico per eseguire la manutenzione o per ripristinare i guasti quando i monitor interni non rilevano alcun problema.
- È possibile utilizzare un controllo del routing insieme a regole di sicurezza per prevenire gli effetti collaterali comuni che possono verificarsi con l'automazione completamente automatizzata basata su controlli dello stato di salute, come il failover su un'infrastruttura di standby non preparata per il failover.

Ecco un esempio di come incorporare i controlli di routing nella strategia di failover, per migliorare la resilienza e la disponibilità delle applicazioni. AWS

È possibile supportare AWS applicazioni ad alta disponibilità AWS eseguendo più repliche ridondanti (in genere tre) in tutte le regioni. Quindi puoi utilizzare il controllo del routing di Amazon Route 53 per indirizzare il traffico verso la replica appropriata.

Ad esempio, puoi configurare una replica dell'applicazione in modo che sia attiva e serva il traffico delle applicazioni, mentre un'altra è una replica in standby. In caso di errori nella replica attiva, è possibile reindirizzare il traffico degli utenti in quella sede per ripristinare la disponibilità dell'applicazione. È necessario decidere se rifiutare o meno una replica in base alle informazioni fornite dai sistemi di monitoraggio e controllo dello stato.

Se si desidera consentire ripristini più rapidi, un'altra opzione che è possibile scegliere per l'architettura è un'implementazione attiva-attiva. Con questo approccio, le repliche sono attive contemporaneamente. Ciò significa che è possibile ripristinare gli errori allontanando gli utenti da una replica dell'applicazione compromessa semplicemente reindirizzando il traffico verso un'altra replica attiva.

AWS Disponibilità regionale per il controllo del routing

Per informazioni dettagliate sul supporto regionale e sugli endpoint di servizio per Amazon Application Recovery Controller (ARC), consulta gli endpoint e le quote di Amazon Application Recovery Controller (ARC) nel riferimento generale di Amazon Web Services.

> **Note**
>
> Il controllo del routing in Amazon Application Recovery Controller (ARC) è una funzionalità globale. Tuttavia, è necessario specificare la regione degli Stati Uniti occidentali (Oregon) (specificare il parametro`--region us-west-2`) nei comandi ARC AWS CLI regionali. Cioè, quando si creano risorse come cluster, pannelli di controllo o controlli di routing.

Un controllo di routing ARC è uno on/off switch che modifica lo stato di un controllo di integrità ARC, che può quindi essere associato a un record DNS che reindirizza il traffico, ad esempio, da una replica di distribuzione primaria a una replica di distribuzione in standby.

Se si verifica un errore dell'applicazione o un problema di latenza, è possibile aggiornare gli stati di controllo del routing per spostare il traffico dalla replica principale, ad esempio, a una replica in standby. Utilizzando le operazioni altamente affidabili dell'API ARC data plane per effettuare query di controllo del routing e aggiornare lo stato di controllo del routing, puoi fare affidamento su ARC per il failover durante gli scenari di disaster recovery. Per ulteriori informazioni, consulta Ottenere e aggiornare gli stati di controllo del routing utilizzando l'API ARC (consigliato).

ARC mantiene gli stati di controllo del routing in un cluster, che è un set di cinque endpoint regionali ridondanti. ARC propaga le modifiche dello stato di controllo del routing su tutto il cluster, che si trova in una flotta Amazon EC2, per ottenere un quorum in cinque regioni. AWS Dopo la propagazione, quando si interroga ARC per uno stato di controllo del routing, utilizzando l'API e il piano dati altamente affidabile, viene restituita la visualizzazione di consenso.

È possibile interagire con uno qualsiasi dei cinque endpoint del cluster per aggiornare lo stato di un controllo di routing da, ad esempio, a. `Off` `On` Quindi ARC propaga l'aggiornamento tra le cinque regioni del cluster.

La coerenza dei dati su tutti e cinque gli endpoint del cluster viene raggiunta in media entro 5 secondi e dopo non più di 15 secondi al massimo.

ARC offre un'affidabilità estrema con il suo piano dati che consente di eseguire manualmente il failover dell'applicazione su più celle. ARC garantisce che almeno tre dei cinque endpoint del cluster

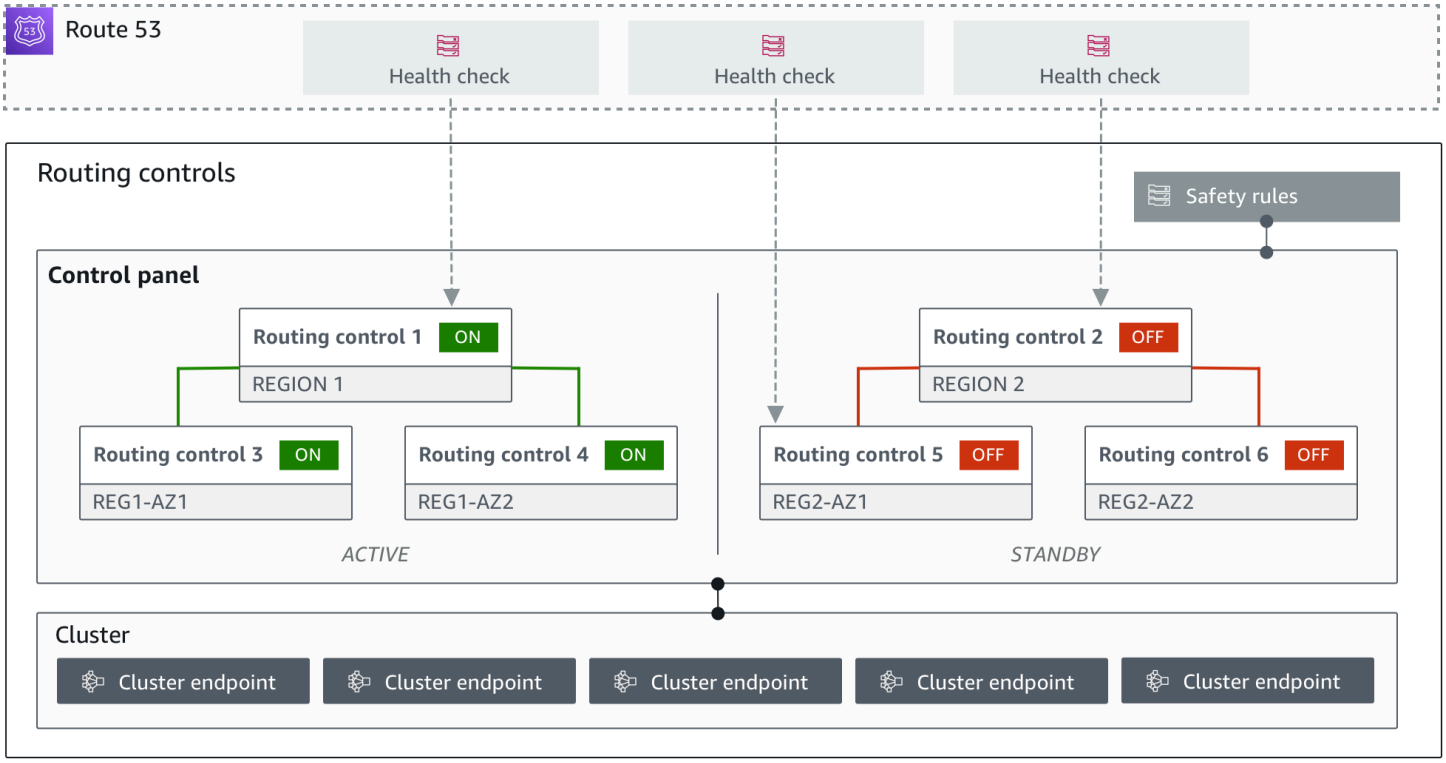
siano sempre accessibili all'utente per modificare lo stato di controllo del routing. Tieni presente che ogni cluster ARC è a tenant singolo, per assicurarti di non essere influenzato da «vicini rumorosi» che potrebbero rallentare i tuoi schemi di accesso.

Quando apporti modifiche agli stati di controllo del routing, ti affidi ai seguenti tre criteri, che è altamente improbabile che abbiano esito negativo:

- Almeno tre dei cinque endpoint sono disponibili e fanno parte del quorum.
- Disponi di credenziali IAM funzionanti e puoi autenticarti su un endpoint del cluster regionale funzionante.
- Il piano dati di Route 53 è integro (questo piano dati è progettato per soddisfare uno SLA di disponibilità del 100%).

Componenti per il controllo del routing

Il diagramma seguente illustra un esempio di componenti che supportano la funzionalità di controllo del routing in ARC. I controlli di routing mostrati qui (raggruppati in un unico pannello di controllo) consentono di gestire il traffico verso due zone di disponibilità in ciascuna delle due regioni. Quando aggiorni gli stati di controllo del routing, ARC modifica i controlli di integrità in Amazon Route 53, che reindirizzano il traffico DNS verso celle diverse. Le regole di sicurezza configurate per il controllo del routing aiutano a evitare scenari di fail-open e altre conseguenze non intenzionali.



Di seguito sono riportati i componenti della funzionalità di controllo del routing in ARC.

Cluster

Un cluster è un insieme di cinque endpoint regionali ridondanti rispetto ai quali si avviano chiamate API per aggiornare o ottenere gli stati di controllo del routing. Un cluster include un pannello di controllo predefinito ed è possibile ospitare più pannelli di controllo e controlli di routing su un unico cluster.

Controlli di routing

Un controllo del routing è un semplice on/off switch, ospitato su un cluster, utilizzato per controllare il routing del traffico client in entrata e in uscita dalle celle. Quando si crea un controllo di routing, si aggiunge un controllo di integrità ARC in Route 53. Ciò consente di reindirizzare il traffico (utilizzando i controlli di integrità, configurati con i record DNS per le applicazioni) quando si aggiorna lo stato di controllo del routing in ARC.

Controllo dello stato del routing

I controlli di routing sono integrati con i controlli di integrità in Route 53. I controlli di integrità sono associati ai record DNS che precedono ogni replica dell'applicazione, ad esempio i record di failover. Quando si modificano gli stati di controllo del routing, ARC aggiorna i controlli di integrità corrispondenti, che reindirizzano il traffico, ad esempio verso il failover sulla replica di standby.

Pannello di controllo

Un pannello di controllo raggruppa una serie di controlli di routing correlati. È possibile associare più controlli di routing a un unico pannello di controllo e quindi creare regole di sicurezza per il pannello di controllo per garantire che gli aggiornamenti di reindirizzamento del traffico effettuati siano sicuri. Ad esempio, puoi configurare un controllo di routing per ciascuno dei tuoi sistemi di bilanciamento del carico in ogni zona di disponibilità e quindi raggrupparli nello stesso pannello di controllo. Quindi puoi aggiungere una regola di sicurezza (una «regola di asserzione») che assicuri che almeno una zona (rappresentata da un controllo di routing) sia attiva contemporaneamente, per evitare scenari di «fail-open» involontari.

Pannello di controllo predefinito

Quando si crea un cluster, ARC crea un pannello di controllo predefinito. Per impostazione predefinita, tutti i controlli di routing creati sul cluster vengono aggiunti al pannello di controllo predefinito. In alternativa, è possibile creare pannelli di controllo personalizzati per raggruppare i controlli di routing correlati.

Regola di sicurezza

Le regole di sicurezza sono regole da aggiungere al controllo del routing per garantire che le azioni di ripristino non compromettano accidentalmente la disponibilità dell'applicazione. Ad esempio, è possibile creare una regola di sicurezza che crei un controllo di routing che funga da interruttore «on/off» generale in modo da poter abilitare o disabilitare una serie di altri controlli di routing.

Endpoint (endpoint del cluster)

Ogni cluster in ARC dispone di cinque endpoint regionali che è possibile utilizzare per impostare e recuperare gli stati di controllo del routing. Il processo di accesso agli endpoint dovrebbe presupporre che ARC attivi e disattivi regolarmente gli endpoint per la manutenzione, quindi dovresti provare ogni endpoint in successione finché non ti connetti a uno solo. È possibile accedere agli endpoint per visualizzare lo stato attuale dei controlli di routing (On o Off) e attivare i failover per le applicazioni modificando gli stati di controllo del routing.

Piani di controllo e dati per il controllo del routing

Quando pianifichi il failover e il disaster recovery, considera la resilienza dei tuoi meccanismi di failover. Ti consigliamo di assicurarti che i meccanismi da cui dipendi durante il failover siano altamente disponibili, in modo da poterli utilizzare quando ne hai bisogno in uno scenario di

emergenza. In genere, è consigliabile utilizzare le funzioni del piano dati per i meccanismi ogni volta che è possibile, per la massima affidabilità e tolleranza ai guasti. In quest'ottica, è importante capire in che modo la funzionalità di un servizio è suddivisa tra piani di controllo e piani dati e quando è possibile contare su un'aspettativa di estrema affidabilità con il piano dati di un servizio.

Come per la maggior parte dei AWS servizi, la funzionalità per la funzionalità di controllo del routing è supportata da piani di controllo e piani dati. Sebbene entrambi siano progettati per essere affidabili, un piano di controllo è ottimizzato per la coerenza dei dati, mentre un piano dati è ottimizzato per la disponibilità. Un piano dati è progettato per la resilienza in modo da poter mantenere la disponibilità anche durante eventi di interruzione, quando un piano di controllo potrebbe non essere disponibile.

In generale, un piano di controllo consente di eseguire funzioni di gestione di base, come creare, aggiornare ed eliminare risorse nel servizio. Un piano dati fornisce le funzionalità principali di un servizio. Per questo motivo, si consiglia di utilizzare le operazioni del piano dati quando la disponibilità è importante, ad esempio quando è necessario reindirizzare il traffico verso una replica in standby durante un'interruzione.

Per il controllo del routing, i piani di controllo e i piani dati sono suddivisi come segue:

- L'API del piano di controllo per il controllo del routing è l'API Recovery Control Configuration, supportata nella regione Stati Uniti occidentali (Oregon) (us-west-2). Queste operazioni API vengono utilizzate oppure Console di gestione AWS per creare o eliminare cluster, pannelli di controllo e controlli di routing, per prepararsi a un evento di disaster recovery in cui potrebbe essere necessario reindirizzare il traffico per l'applicazione. Il piano di controllo della configurazione del controllo del routing non è altamente disponibile.
- Il piano dati di controllo del routing è un cluster dedicato in cinque regioni AWS geograficamente isolate. Ogni cliente crea uno o più cluster utilizzando il piano di controllo del routing. Il cluster ospita pannelli di controllo e controlli di routing. Quindi utilizzi l'API Routing Control (Recovery Cluster) per ottenere, elencare e aggiornare gli stati di controllo del routing quando desideri reindirizzare il traffico per la tua applicazione. Il piano dati di controllo del routing È altamente disponibile.

Poiché il piano dati di controllo del routing è altamente disponibile, si consiglia di utilizzarlo per AWS Command Line Interface effettuare chiamate API per gestire gli stati di controllo del routing quando si desidera eseguire il failover per ripristinare un evento. Per ulteriori informazioni sulle considerazioni chiave da prendere in considerazione per la preparazione e il completamento di un'operazione di ripristino con il controllo del routing, consulta. Le migliori pratiche per il controllo del routing in ARC

Per ulteriori informazioni sui piani dati, sui piani di controllo e su come AWS crea servizi per soddisfare gli obiettivi di alta disponibilità, consulta il paper Static stability using Availability Zones in Amazon Builders' Library.

Tagging per il controllo del routing in Amazon Application Recovery Controller (ARC)

I tag sono parole o frasi (metadati) che usi per identificare e organizzare le tue risorse. AWS È possibile aggiungere più tag a ogni risorsa e ogni tag include una chiave e un valore che definisci. Ad esempio, la chiave potrebbe essere l'ambiente e il valore potrebbe essere la produzione. Puoi cercare e filtrare le tue risorse in base ai tag che aggiungi.

Puoi taggare le seguenti risorse nel controllo del routing in ARC:

- Cluster
- Pannelli di controllo
- Regole di sicurezza

L'etichettatura in ARC è disponibile solo tramite l'API, ad esempio utilizzando il AWS CLI.

Di seguito sono riportati alcuni esempi di etichettatura nel controllo del routing utilizzando. AWS CLI

```
aws route53-recovery-control-config --region us-west-2 create-cluster --
cluster-name example1-cluster --tags Region=PDX,Stage=Prod
```

```
aws route53-recovery-control-config --region us-west-2 create-control-panel
--control-panel-name example1-control-panel --cluster-arn arn:aws:route53-
recovery-control::111122223333:cluster/5678abcd-abcd-5678-abcd-5678abcdefgh
--tags Region=PDX,Stage=Prod
```

Per ulteriori informazioni, consulta TagResourcela Recovery Control Configuration API Reference Guide per Amazon Application Recovery Controller (ARC).

Prezzi per il controllo del routing in ARC

Per il controllo del routing in ARC, paghi un costo orario per cluster creato. Ogni cluster può ospitare più controlli di routing, da utilizzare per attivare i failover delle applicazioni.

Per aiutare a gestire i costi e migliorare l'efficienza, è possibile configurare la condivisione tra account per un cluster, in modo da condividere un cluster con più account. AWS Per ulteriori informazioni, consulta Supporta più account per i cluster in ARC.

Per informazioni dettagliate sui prezzi di ARC ed esempi di prezzi, consulta ARC Pricing.

Guida introduttiva al ripristino multiregionale in Amazon Application Recovery Controller (ARC)

Per eseguire il failover delle applicazioni utilizzando il controllo del routing in Amazon Application Recovery Controller (ARC), è necessario disporre di più AWS Regioni AWS applicazioni. Per iniziare, assicurati innanzitutto che le applicazioni siano configurate in repliche in silos in ciascuna regione, in modo da poter eseguire il failover da una all'altra durante un evento. È quindi possibile creare controlli di routing per reindirizzare il traffico delle applicazioni in modo da effettuare il failover da un'applicazione principale a una secondaria, garantendo la continuità per gli utenti.

> **Note**
>
> Se disponi di un'applicazione isolata per zone di disponibilità, prendi in considerazione l'utilizzo dello spostamento zonale o dello spostamento automatico di zona per il ripristino in caso di failover. Non è necessaria alcuna configurazione per utilizzare lo spostamento zonale o lo spostamento automatico di zona per ripristinare in modo affidabile le applicazioni in caso di problemi relativi alla zona di disponibilità. Per ulteriori informazioni, consulta Usa lo spostamento zonale e lo spostamento automatico di zona per ripristinare le applicazioni in ARC.

Per poter utilizzare il controllo del routing ARC per ripristinare le applicazioni durante un evento, si consiglia di configurare almeno due applicazioni che siano repliche l'una dell'altra. Ogni replica, o cella, rappresenta un. Regione AWS Dopo aver configurato le risorse dell'applicazione per l'allineamento con le regioni, assicurati che l'applicazione sia configurata per il corretto ripristino eseguendo i passaggi seguenti.

Suggerimento: per semplificare la configurazione, forniamo CloudFormation modelli HashiCorp Terraform che creano un'applicazione con repliche ridondanti che falliscono indipendentemente l'una dall'altra. Per saperne di più e scaricare i modelli, consulta. Configurazione di un'app di esempio

Per prepararti a utilizzare il controllo del routing, assicurati che l'applicazione sia configurata per essere resiliente effettuando le seguenti operazioni:

1. Crea copie indipendenti dello stack di applicazioni (livello di rete e di elaborazione) che siano repliche l'una dell'altra in ciascuna regione, in modo da poter effettuare il failover del traffico dall'una all'altra in caso di evento. Assicurati di non avere dipendenze interregionali nel codice dell'applicazione che potrebbero causare il fallimento di una replica a ripercuotersi sull'altra. Per eseguire correttamente il failover tra le due aree Regioni AWS, i limiti dello stack devono trovarsi all'interno di una regione.
2. Duplica tutti i dati stateful richiesti per l'applicazione tra le repliche. È possibile utilizzare i servizi di AWS database per aiutare a replicare i dati.

Inizia a controllare il routing per il failover del traffico

Il controllo del routing in Amazon Application Recovery Controller (ARC) consente di attivare il failover per il failover del traffico tra copie ridondanti dell'applicazione, o repliche, che vengono eseguite separatamente. Regioni AWS Il failover viene eseguito con DNS, utilizzando il piano dati Amazon Route 53.

Dopo aver configurato le repliche in ciascuna regione, come descritto nella sezione successiva, puoi associare ognuna di esse a un controllo di routing. Innanzitutto, associ i controlli di routing ai nomi di dominio di primo livello delle repliche in ciascuna regione. Quindi, aggiungi un controllo dello stato del controllo del routing al controllo del routing in modo che possa attivare e disattivare il flusso del traffico. Ciò consente di controllare il routing del traffico tra le repliche dell'applicazione.

È possibile aggiornare gli stati di controllo del routing in modalità Console di gestione AWS di failover del traffico, ma si consiglia invece di utilizzare le azioni ARC, utilizzando l'API o AWS CLI, per modificarle. Le azioni API non dipendono dalla console, quindi sono più resilienti.

Ad esempio, per eseguire il failover tra regioni, da us-west-1 a us-east-1, puoi `update-routing-control-state` utilizzare l'azione API per impostare lo stato di to e to. `us-west-1` `Off` `us-east-1` `On`

Prima di creare componenti di controllo del routing per configurare il failover dell'applicazione, assicuratevi che l'applicazione sia inserita in silos nelle repliche regionali, in modo da poter effettuare il failover da una all'altra. Per ulteriori informazioni e iniziare a isolare una nuova applicazione o creare uno stack di esempio, consultate le sezioni successive.

Configurazione di un'app di esempio

Per aiutarti a capire come funziona il controllo del routing, forniamo un'applicazione di esempio chiamata`TicTacToe`. L'esempio utilizza CloudFormation modelli per semplificare il processo,

oltre a un CloudFormation modello scaricabile in modo che possiate esplorare rapidamente la configurazione e l'utilizzo di ARC da soli.

Dopo aver distribuito l'app di esempio, puoi utilizzare i modelli per creare componenti ARC e quindi esplorare l'utilizzo dei controlli di routing per gestire il flusso di traffico verso l'app. Puoi adattare il modello e il processo per il tuo scenario e le tue applicazioni.

Per iniziare con un'applicazione e dei CloudFormation modelli di esempio, consulta le istruzioni README nel repository ARC GitHub. Puoi saperne di più sull'uso dei CloudFormation modelli leggendo CloudFormation i concetti nella Guida per l' AWS CloudFormation utente.

Le migliori pratiche per il controllo del routing in ARC

Consigliamo le seguenti best practice per la preparazione al ripristino e al failover per il controllo del routing in ARC.

Argomenti

- Mantieni le credenziali create appositamente e di lunga durata sicure e sempre accessibili AWS
- Scegli valori TTL inferiori per i record DNS coinvolti nel failover
- Limita il tempo in cui i client rimangono connessi ai tuoi endpoint
- Aggiungi ai segnalibri o codifica i tuoi cinque endpoint del cluster regionale e il controllo del routing ARNs
- Scegli uno dei tuoi endpoint a caso per aggiornare gli stati di controllo del routing
- Utilizza l'API data plane estremamente affidabile per elencare e aggiornare gli stati di controllo del routing, non la console

Mantieni le credenziali create appositamente e di lunga durata sicure e sempre accessibili AWS

> In uno scenario di disaster recovery (DR), riduci al minimo le dipendenze dal sistema utilizzando un approccio semplice per accedere ed eseguire le attività di ripristino. AWS Crea credenziali IAM a lunga durata specifiche per le attività di DR e conservale in modo sicuro in una cassaforte fisica locale o in un deposito virtuale, a cui accedervi quando necessario. Con IAM, puoi gestire centralmente le credenziali di sicurezza, come le chiavi di accesso e le autorizzazioni per l'accesso alle risorse. AWS Per le attività diverse dal DR, ti consigliamo di continuare a utilizzare l'accesso federato, utilizzando AWS servizi come Single Sign-On.AWS

Per eseguire attività di failover in ARC con l'API del piano dati del cluster di ripristino, puoi allegare una policy ARC IAM al tuo utente. Per ulteriori informazioni, consulta Esempi di policy basate sull'identità in Amazon Application Recovery Controller (ARC).

Scegliete valori TTL inferiori per i record DNS coinvolti nel failover

Per i record DNS che potrebbe essere necessario modificare nell'ambito del meccanismo di failover, in particolare i record sottoposti a controlli di integrità, è opportuno utilizzare valori TTL inferiori. Per questo scenario, è comune impostare un TTL di 60 o 120 secondi.

L'impostazione DNS TTL (time to live) indica ai resolver DNS per quanto tempo devono memorizzare nella cache un record prima di richiederne uno nuovo. Quando scegli un TTL, fai un compromesso tra latenza e affidabilità e reattività al cambiamento. Con un TTL più breve su un record, i resolver DNS notano gli aggiornamenti del record più rapidamente perché il TTL specifica che devono eseguire query più frequentemente.

Per ulteriori informazioni, consulta Scelta dei valori TTL per i record DNS nelle migliori pratiche per Amazon Route 53 DNS.

Limita il tempo in cui i client rimangono connessi ai tuoi endpoint

Quando usi i controlli di routing per passare da uno Regione AWS all'altro, il meccanismo utilizzato da Amazon Application Recovery Controller (ARC) per spostare il traffico dell'applicazione è un aggiornamento DNS. Questo aggiornamento fa sì che tutte le nuove connessioni vengano allontanate dalla posizione compromessa.

Tuttavia, i client con connessioni aperte preesistenti potrebbero continuare a fare richieste verso la posizione compromessa fino alla riconnessione dei client. Per garantire un ripristino rapido, ti consigliamo di limitare il periodo di tempo in cui i client rimangono connessi ai tuoi endpoint.

Se si utilizza un Application Load Balancer, è possibile utilizzare l'`keepalive`opzione per configurare la durata delle connessioni. Per ulteriori informazioni, consulta la durata del client HTTP keepalive nella Guida per l'utente di Application Load Balancer.

Per impostazione predefinita, Application Load Balancer impostano il valore di durata keepalive del client HTTP su 3600 secondi o 1 ora. Ti consigliamo di abbassare il valore per adattarlo all'obiettivo del tempo di ripristino per l'applicazione, ad esempio 300 secondi. Quando scegli la durata di keepalive di un client HTTP, considera che questo valore rappresenta un compromesso tra la riconnessione più frequente in generale, il che può influire sulla latenza, e lo spostamento più rapido di tutti i client da una zona o regione compromessa.

Aggiungi ai segnalibri o codifica i tuoi cinque endpoint del cluster regionale e controlla il routing ARNs

Ti consigliamo di conservare una copia locale degli endpoint del cluster regionale ARC, nei segnalibri o salvata nel codice di automazione che usi per riprovare gli endpoint. Durante un evento di errore, potresti non essere in grado di accedere ad alcune operazioni API, incluse le operazioni API ARC che non sono ospitate nel cluster Data Plane estremamente affidabile. È possibile elencare gli endpoint per i cluster ARC utilizzando l'operazione DescribeClusterAPI.

Scegli uno dei tuoi endpoint a caso per aggiornare gli stati di controllo del routing

I controlli di routing forniscono cinque endpoint regionali per garantire un'elevata disponibilità, anche in caso di guasti. Per raggiungere la loro piena resilienza, è importante disporre di una logica di riprova in grado di utilizzare tutti e cinque gli endpoint, se necessario. Per informazioni sull'utilizzo di esempi di codice con l' AWS SDK, inclusi esempi per provare gli endpoint del cluster, consulta. Esempi di codice per l'utilizzo di Application Recovery Controller AWS SDKs

Utilizza l'API data plane estremamente affidabile per elencare e aggiornare gli stati di controllo del routing, non la console

Utilizzando l'API del piano dati ARC, visualizza i controlli e gli stati del routing insieme all'ListRoutingControlsoperazione e aggiorna gli stati di controllo del routing per reindirizzare il traffico in modo da consentire il failover dell'operazione. UpdateRoutingControlState È possibile utilizzare AWS CLI (come in questi esempi) o il codice che si scrive utilizzando uno dei. AWS SDKs ARC offre un'affidabilità estrema con l'API nel piano dati per il failover del traffico. Si consiglia di utilizzare l'API anziché modificare gli stati di controllo del Console di gestione AWS routing in.

Connect a uno degli endpoint del cluster regionale per ARC per utilizzare l'API del piano dati. Se l'endpoint non è disponibile, prova a connetterti a un altro endpoint del cluster.

Se una regola di sicurezza blocca un aggiornamento dello stato di controllo del routing, puoi ignorarla per effettuare l'aggiornamento e gestire il traffico. Per ulteriori informazioni, consulta Sostituire le regole di sicurezza per reindirizzare il traffico.

Test di failover con ARC

Eseguite regolarmente il failover con ARC Routing Control, per eseguire il failover dallo stack di applicazioni primario a uno stack di applicazioni secondario. È importante assicurarsi che le strutture ARC che avete aggiunto siano allineate con le risorse corrette dello stack e che tutto funzioni come previsto. È consigliabile verificarlo dopo aver configurato ARC per il proprio ambiente e continuare a eseguire i test periodicamente, in modo da preparare l'ambiente

di failover, prima che si verifichi una situazione di errore in cui è necessario che il sistema secondario sia attivo e funzionante rapidamente per evitare tempi di inattività per gli utenti.

Operazioni dell'API di controllo del routing

Questa sezione include tabelle con elenchi delle operazioni API che puoi utilizzare per configurare e utilizzare il controllo del routing in Amazon Application Recovery Controller (ARC), con collegamenti alla documentazione pertinente.

Per esempi di come utilizzare le comuni operazioni API di configurazione del controllo del routing con AWS Command Line Interface, consulta. Esempi di utilizzo delle operazioni dell'API di controllo del routing ARC con AWS CLI

La tabella seguente elenca le operazioni dell'API ARC che è possibile utilizzare per la configurazione del controllo del routing, con collegamenti alla documentazione pertinente.

Azione	Utilizzo della console ARC	Utilizzando l'API ARC
Creazione di un cluster	Consulta Creazione di componenti di controllo del routing in ARC.	Consulta la sezione CreateCluster
Descrizione di un cluster	Consulta Creazione di componenti di controllo del routing in ARC.	Consulta la sezione DescribeCluster
Eliminazione di un cluster	Consulta Creazione di componenti di controllo del routing in ARC.	Consulta la sezione DeleteCluster
Elenca i cluster per un account	Consulta Creazione di componenti di controllo del routing in ARC.	Consulta la sezione ListClusters
Crea un controllo di routing	Consulta Creazione di componenti di controllo del routing in ARC.	Consulta la sezione CreateRoutingControl

Azione	Utilizzo della console ARC	Utilizzando l'API ARC
Descrivi un controllo di routing	Consulta Creazione di componenti di controllo del routing in ARC.	Consulta la sezione DescribeRoutingControl
Aggiornare un controllo di routing	Consulta Creazione di componenti di controllo del routing in ARC.	Consulta la sezione UpdateRoutingControl
Eliminare un controllo di routing	Consulta Creazione di componenti di controllo del routing in ARC.	Consulta la sezione DeleteRoutingControl
Elenca i controlli di routing	Consulta Creazione di componenti di controllo del routing in ARC.	Consulta la sezione ListRoutingControls
Crea un pannello di controllo	Consulta Creazione di componenti di controllo del routing in ARC.	Consulta la sezione CreateControlPanel
Descrivi un pannello di controllo	Consulta Creazione di componenti di controllo del routing in ARC.	Consulta la sezione DescribeControlPanel
Aggiornare un pannello di controllo	Consulta Creazione di componenti di controllo del routing in ARC.	Consulta la sezione UpdateControlPanel
Eliminare un pannello di controllo	Consulta Creazione di componenti di controllo del routing in ARC.	Consulta la sezione DeleteControlPanel
Elenca i pannelli di controllo	Consulta Creazione di componenti di controllo del routing in ARC.	Consulta la sezione ListControlPanels

Azione	Utilizzo della console ARC	Utilizzando l'API ARC
Crea una regola di sicurezza	Consulta Creazione di regole di sicurezza per il controllo del routing.	Consulta la sezione CreateSafetyRule
Descrivi una regola di sicurezza	Consulta Creazione di regole di sicurezza per il controllo del routing.	Consulta la sezione DescribeSafetyRule
Aggiornare una regola di sicurezza	Consulta Creazione di regole di sicurezza per il controllo del routing.	Consulta la sezione UpdateSafetyRule
Eliminare una regola di sicurezza	Consulta Creazione di regole di sicurezza per il controllo del routing.	Consulta la sezione DeleteSafetyRule
Elenca le regole di sicurezza	Consulta Creazione di regole di sicurezza per il controllo del routing.	Consulta la sezione ListSafetyRules
Elenca i controlli sanitari associati alla Route 53	Per informazioni, consultare Creazione di un controllo dello stato del routing in ARC.	Vedi ListAssociatedRoute53HealthChecks
Elenca le politiche AWS RAM delle risorse per la condivisione dei cluster	Consulta Supporta più account per i cluster in ARC.	Vedi GetResourcePolicy

La tabella seguente elenca le operazioni comuni dell'API ARC che è possibile utilizzare per gestire il failover del traffico con il piano dati di controllo del routing, con collegamenti alla documentazione pertinente.

Azione	Utilizzo della console ARC	Utilizzando l'API ARC
Ottieni uno stato di controllo del routing	Consulta Ottenere e aggiornare gli stati di controllo del	Consulta la sezione GetRoutingControlState

Azione	Utilizzo della console ARC	Utilizzando l'API ARC
	routing in Console di gestione AWS.	
Elenca i controlli di routing	N/D	Per informazioni, consultare ListRoutingControls.
Aggiornare uno stato di controllo del routing	Consulta Ottenere e aggiornare gli stati di controllo del routing in Console di gestione AWS.	Consulta la sezione UpdateRoutingControlState
Aggiornare più stati di controllo del routing	Consulta Ottenere e aggiornare gli stati di controllo del routing in Console di gestione AWS.	Consulta la sezione UpdateRoutingControlStates

Utilizzo di questo servizio con un SDK AWS

AWS i kit di sviluppo software (SDKs) sono disponibili per molti linguaggi di programmazione più diffusi. Ogni SDK fornisce un'API, esempi di codice e documentazione che facilitano agli sviluppatori la creazione di applicazioni nel loro linguaggio preferito.

Documentazione sugli SDK	Esempi di codice
AWS SDK per C++	AWS SDK per C++ esempi di codice
AWS CLI	AWS CLI esempi di codice
AWS SDK per Go	AWS SDK per Go esempi di codice
AWS SDK per Java	AWS SDK per Java esempi di codice
AWS SDK per JavaScript	AWS SDK per JavaScript esempi di codice
AWS SDK per Kotlin	AWS SDK per Kotlin esempi di codice
AWS SDK per .NET	AWS SDK per .NET esempi di codice

Documentazione sugli SDK	Esempi di codice
AWS SDK per PHP	AWS SDK per PHP esempi di codice
AWS Strumenti per PowerShell	AWS Strumenti per PowerShell esempi di codice
AWS SDK per Python (Boto3)	AWS SDK per Python (Boto3) esempi di codice
AWS SDK per Ruby	AWS SDK per Ruby esempi di codice
AWS SDK per Rust	AWS SDK per Rust esempi di codice
AWS SDK per SAP ABAP	AWS SDK per SAP ABAP esempi di codice
AWS SDK per Swift	AWS SDK per Swift esempi di codice

Per esempi specifici del servizio, consulta Esempi di codice per l'utilizzo di Application Recovery Controller AWS SDKs.

> **Esempio di disponibilità**
>
> Non riesci a trovare quello che ti serve? Richiedi un esempio di codice utilizzando il link Fornisci un feedback nella parte inferiore di questa pagina.

Esempi di utilizzo delle operazioni dell'API di controllo del routing ARC con AWS CLI

Questa sezione illustra semplici esempi applicativi di utilizzo del controllo del routing, dell'utilizzo della funzionalità AWS Command Line Interface di controllo del routing in Amazon Application Recovery Controller (ARC) utilizzando le operazioni API. Gli esempi hanno lo scopo di aiutarti a sviluppare una comprensione di base su come lavorare con il controllo del routing utilizzando la CLI.

Con il controllo del routing in Amazon Application Recovery Controller (ARC), puoi attivare i failover del traffico tra copie ridondanti delle applicazioni, o repliche, che vengono eseguite in zone di disponibilità separate o in zone di disponibilità. Regioni AWS

Organizzi i controlli di routing in gruppi chiamati pannelli di controllo che vengono forniti su un cluster. Un cluster ARC è un set regionale di endpoint distribuito a livello globale. Gli endpoint del cluster forniscono un'API ad alta disponibilità che è possibile utilizzare per impostare e recuperare gli stati di controllo del routing. Per ulteriori informazioni sui componenti della funzionalità di controllo del routing, vedere. Componenti per il controllo del routing

> **Note**
>
> ARC è un servizio globale che supporta endpoint multipli. Regioni AWS Tuttavia, è necessario specificare la regione Stati Uniti occidentali (Oregon), ovvero specificare il parametro, nella maggior parte dei comandi ARC `--region us-west-2` CLI. Ad esempio, utilizzate il `region` parametro quando create gruppi di ripristino, pannelli di controllo e cluster.
>
> Quando si crea un cluster, ARC fornisce un set di endpoint regionali. Per ottenere o aggiornare gli stati di controllo del routing, è necessario specificare l'endpoint regionale (l' Regione AWS e l'URL dell'endpoint) nel comando CLI.

Per ulteriori informazioni sull'utilizzo di AWS CLI, consulta il Command Reference. AWS CLI Per un elenco delle azioni dell'API di controllo del routing, consulta Operazioni dell'API di controllo del routing eOperazioni dell'API di controllo del routing.

Inizieremo creando i componenti necessari per gestire il failover utilizzando i controlli di routing, iniziando con la creazione di un cluster.

Configura i componenti di controllo del routing

Il nostro primo passo è creare un cluster. Un cluster ARC è un insieme di cinque endpoint, uno per ognuno dei cinque diversi Regioni AWS. L'infrastruttura ARC consente a questi endpoint di funzionare in modo coordinato in modo da garantire un'elevata disponibilità e una coerenza sequenziale delle operazioni di failover.

1. Creazione di un cluster

1a. Crea un cluster. `network-type`È facoltativo e può essere o. `IPV4` `DUALSTACK` Il valore predefinito è `IPV4`.

```
aws route53-recovery-control-config create-cluster --cluster-name test --network-type
 DUALSTACK
```

```
"Cluster": {
    "ClusterArn": "arn:aws:route53-recovery-
control::123456789123:cluster/12341234-1234-1234-1234-123412341234",
    "Name": "test",
    "Status": "PENDING",
    "Owner": "123456789123",
    "NetworkType": "DUALSTACK"
}
```

La prima volta che si crea una risorsa ARC, questa ha lo stato `PENDING` durante la creazione del cluster. Puoi verificarne lo stato di avanzamento chiamando`describe-cluster`.

1b. Descrivi un cluster.

```
aws route53-recovery-control-config --region us-west-2 \
    describe-cluster --cluster-arn arn:aws:route53-recovery-
control::111122223333:cluster/5678abcd-abcd-5678-abcd-5678abcdefgh
```

```
"Cluster": {
    "ClusterArn": "arn:aws:route53-recovery-
control::123456789123:cluster/12341234-1234-1234-1234-123412341234",
    "Name": "test",
    "Status": "DEPLOYED",
    "Owner": "123456789123",
    "NetworkType": "DUALSTACK"
}
```

Quando lo stato è IMPLEMENTATO, ARC ha creato con successo il cluster con il set di endpoint con cui interagire. Puoi elencare tutti i tuoi cluster chiamando. `list-clusters`

1c. Elenca i tuoi cluster.

```
aws route53-recovery-control-config --region us-west-2 list-clusters
```

```
"Cluster": {
    "ClusterArn": "arn:aws:route53-recovery-
control::123456789123:cluster/12341234-1234-1234-1234-123412341234",
    "Name": "test",
    "Status": "DEPLOYED",
    "Owner": "123456789123",
```

```
    "NetworkType": "DUALSTACK"
}
```

1d. Aggiorna il tipo di rete per i tuoi cluster. Le opzioni sono `IPV4` o `DUALSTACK`.

```
aws route53-recovery-control-config update-cluster \
--cluster-arn arn:aws:route53-recovery-
control::123456789123:cluster/12341234-1234-1234-1234-123412341234 \
--network-type DUALSTACK
```

```
"Cluster": {
    "ClusterArn": "arn:aws:route53-recovery-
control::123456789123:cluster/12341234-1234-1234-1234-123412341234",
    "Name": "test",
    "Status": "PENDING",
    "Owner": "123456789123",
   "NetworkType": "DUALSTACK"
}
```

2. Crea un pannello di controllo

Un pannello di controllo è un raggruppamento logico per organizzare i controlli di routing ARC. Quando si crea un cluster, ARC fornisce automaticamente un pannello di controllo chiamato dall'utente. `DefaultControlPanel` È possibile utilizzare questo pannello di controllo immediatamente.

Un pannello di controllo può esistere solo in un cluster. Se si desidera spostare un pannello di controllo in un altro cluster, è necessario eliminarlo e quindi crearlo nel secondo cluster. Puoi vedere tutti i pannelli di controllo del tuo account chiamando`list-control-panels`. Per visualizzare solo i pannelli di controllo di un cluster specifico, aggiungi il `--cluster-arn` campo.

2a. Elenca i pannelli di controllo.

```
aws route53-recovery-control-config --region us-west-2 \
    list-control-panels --cluster-arn arn:aws:route53-recovery-
control::111122223333:cluster/eba23304-1a51-4674-ae32-b4cf06070bdd
```

```
{
    "ControlPanels": [
```

```
        {
            "ControlPanelArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/1234567dddddd1234567dddddd1234567",
            "ClusterArn": "arn:aws:route53-recovery-
control::111122223333:cluster/5678abcd-abcd-5678-abcd-5678abcdefgh",
            "DefaultControlPanel": true,
            "Name": "DefaultControlPanel",
            "RoutingControlCount": 0,
            "Status": "DEPLOYED"
        }
    ]
}
```

Facoltativamente, crea il tuo pannello di controllo `create-control-panel` chiamando.

2 b. Crea un pannello di controllo.

```
aws route53-recovery-control-config --region us-west-2 create-control-panel \
        --control-panel-name NewControlPanel2 \
        --cluster-arn arn:aws:route53-recovery-control::111122223333:cluster/5678abcd-
abcd-5678-abcd-5678abcdefgh
```

```
{
    "ControlPanel": {
        "ControlPanelArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456",
        "ClusterArn": "arn:aws:route53-recovery-control::111122223333:cluster/5678abcd-
abcd-5678-abcd-5678abcdefgh",
        "DefaultControlPanel": false,
        "Name": "NewControlPanel2",
        "RoutingControlCount": 0,
        "Status": "PENDING"
    }
}
```

Quando crei per la prima volta una risorsa ARC, lo stato è in corso di creazione. `PENDING` Puoi controllare i progressi chiamando`describe-control-panel`.

2c. Descrivi un pannello di controllo.

```
aws route53-recovery-control-config --region us-west-2 describe-control-panel \
```

```
    --control-panel-arn arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456
```

```
{
    "ControlPanel": {
        "ControlPanelArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456",
        "ClusterArn": "arn:aws:route53-recovery-control::111122223333:cluster/5678abcd-
abcd-5678-abcd-5678abcdefgh",
        "DefaultControlPanel": true,
        "Name": "DefaultControlPanel",
        "RoutingControlCount": 0,
        "Status": "DEPLOYED"
    }
}
```

3. Crea un controllo di routing

Ora che hai configurato il cluster e hai esaminato i pannelli di controllo, puoi iniziare a creare controlli di routing. Quando crei un controllo di routing, devi almeno specificare l'Amazon Resource Name (ARN) del cluster in cui desideri che si trovi il controllo del routing. È inoltre possibile specificare l'ARN di un pannello di controllo per il controllo del routing. Dovrai anche specificare il cluster in cui si trova il pannello di controllo.

Se non specifichi un pannello di controllo, il controllo del routing viene aggiunto al pannello di controllo creato automaticamente,`DefaultControlPanel`.

Crea un controllo di routing chiamando. `create-routing-control`

3a. Crea un controllo di routing.

```
aws route53-recovery-control-config --region us-west-2 create-routing-control \
    --routing-control-name NewRc1 \
    --cluster-arn arn:aws:route53-recovery-control::111122223333:cluster/5678abcd-
abcd-5678-abcd-5678abcdefgh
```

```
{
    "RoutingControl": {
        "ControlPanelArn": " arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456",
        "Name": "NewRc1",
```

```
        "RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567",
        "Status": "PENDING"
    }
}
```

I controlli di routing seguono lo stesso schema di creazione delle altre risorse ARC, quindi è possibile monitorarne l'avanzamento richiamando un'operazione di descrizione.

3b. Descrivi il controllo del routing.

```
aws route53-recovery-control-config --region us-west-2 describe-routing-control \
       --routing-control-arn arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567
```

```
{
    "RoutingControl": {
        "ControlPanelArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456",
        "Name": "NewRc1",
        "RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567",
        "Status": "DEPLOYED"
    }
}
```

È possibile elencare i controlli di routing in un pannello di controllo chiamando. `list-routing-controls` È richiesto l'ARN del pannello di controllo.

3c. Elenca i controlli di routing.

```
aws route53-recovery-control-config --region us-west-2 list-routing-controls \
        --control-panel-arn arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456
```

```
{
    "RoutingControls": [
```

```
        {
            "ControlPanelArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456",
            "Name": "Rc1",
            "RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567",
            "Status": "DEPLOYED"
        },
        {
            "ControlPanelArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456",
            "Name": "Rc2",
            "RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
hijklmnop987654321",
            "Status": "DEPLOYED"
        }
    ]
}
```

Nell'esempio seguente, in cui lavoriamo con gli stati di controllo del routing, supponiamo che siano presenti i due controlli di routing elencati in questa sezione (Rc1 e Rc2). In questo esempio, ogni controllo di routing rappresenta una zona di disponibilità in cui viene distribuita l'applicazione.

4. Crea regole di sicurezza

Quando utilizzi più controlli di routing contemporaneamente, potresti decidere di adottare alcune misure di sicurezza quando li abiliti e disabiliti, per evitare conseguenze involontarie, come la disattivazione di entrambi i controlli di routing e l'interruzione di tutto il flusso di traffico. Per creare queste protezioni, create regole di sicurezza per il controllo del routing.

Esistono due tipi di regole di sicurezza: regole di asserzione e regole di controllo. Per ulteriori informazioni sulle regole di sicurezza, consulta. Creazione di regole di sicurezza per il controllo del routing

La chiamata seguente fornisce un esempio di creazione di una regola di asserzione che assicura che almeno uno dei due controlli di routing sia impostato su un dato 0n momento. Per creare la regola, si esegue `create-safety-rule` con il `assertion-rule` parametro.

Per informazioni dettagliate sul funzionamento dell'API delle regole di asserzione, consulta AssertionRulela Routing Control API Reference Guide for Amazon Application Recovery Controller.

4a. Crea una regola di asserzione.

```
aws route53-recovery-control-config --region us-west-2 create-safety-rule \
        --assertion-rule '{"Name": "TestAssertionRule",
        "ControlPanelArn": "arn:aws:route53-recovery-
control::888888888888:controlpanel/zzz123yyy456xxx789zzz123yyy456xxx",
        "WaitPeriodMs": 5000,
        "AssertedControls":
        ["arn:aws:route53-recovery-control::888888888888:controlpanel/
zzz123yyy456xxx789zzz123yyy456xxx/routingcontrol/def123def123def"
        "arn:aws:route53-recovery-control::888888888888:controlpanel/
zzz123yyy456xxx789zzz123yyy456xxx/routingcontrol/ghi456ghi456ghi"],
        "RuleConfig": {"Threshold": 1, "Type": "ATLEAST", "Inverted": false}}'
```

```
{
    "Rule": {
        "ASSERTION": {
            "Arn": "arn:aws:route53-recovery-control::888888888888:controlpanel/
zzz123yyy456xxx789zzz123yyy456xxx/safetyrule/333333444444",
            "AssertedControls": [
                "arn:aws:route53-recovery-control::888888888888:controlpanel/
zzz123yyy456xxx789zzz123yyy456xxx/routingcontrol/def123def123def"
                "arn:aws:route53-recovery-control::888888888888:controlpanel/
zzz123yyy456xxx789zzz123yyy456xxx/routingcontrol/ghi456ghi456ghi"],
            "ControlPanelArn": "arn:aws:route53-recovery-
control::888888888888:controlpanel/zzz123yyy456xxx789zzz123yyy456xxx",
            "Name": "TestAssertionRule",
            "RuleConfig": {
                "Inverted": false,
                "Threshold": 1,
                "Type": "ATLEAST"
            },
            "Status": "PENDING",
            "WaitPeriodMs": 5000
        }
    }
}
```

La chiamata seguente fornisce un esempio di creazione di una regola di gating che fornisce uno switch generale «on/off» o «gating» per un set di controlli di routing di destinazione in un pannello di controllo. Ciò consente di non consentire l'aggiornamento dei controlli di routing di destinazione in modo che, ad esempio, l'automazione non possa effettuare aggiornamenti non autorizzati. In questo

esempio, il gating switch è un controllo di routing specificato dal `GatingControls` parametro e i due controlli di routing controllati o «controllati» sono specificati dal parametro. `TargetControls`

> **Note**
>
> Prima di creare la regola di gating, è necessario creare il controllo di routing di gating, che non include i record di failover DNS, e i controlli di routing di destinazione, che devono essere configurati con i record di failover DNS.

Per creare la regola, si esegue con il parametro. `create-safety-rule` `gating-rule`

Per informazioni dettagliate sul funzionamento dell'API delle regole di asserzione, consulta GatingRulela Routing Control API Reference Guide for Amazon Application Recovery Controller.

4 b. Crea una regola di gating.

```
aws route53-recovery-control-config --region us-west-2 create-safety-rule \
        --gating-rule '{"Name": "TestGatingRule",
        "ControlPanelArn": "arn:aws:route53-recovery-
control::888888888888:controlpanel/zzz123yyy456xxx789zzz123yyy456xxx",
        "WaitPeriodMs": 5000,
        "GatingControls": ["arn:aws:route53-recovery-
control::888888888888:controlpanel/zzz123yyy456xxx789zzz123yyy456xxx/routingcontrol/
def123def123def"]
        "TargetControls": ["arn:aws:route53-recovery-
control::888888888888:controlpanel/zzz123yyy456xxx789zzz123yyy456xxx/routingcontrol/
ghi456ghi456ghi",
        "arn:aws:route53-recovery-control::888888888888:controlpanel/
zzz123yyy456xxx789zzz123yyy456xxx/routingcontrol/lmn789lmn789lmn"],
        "RuleConfig": {"Threshold": 0, "Type": "OR", "Inverted": false}}'
```

```
{
    "Rule": {
        "GATING": {
            "Arn": "arn:aws:route53-recovery-control::888888888888:controlpanel/
zzz123yyy456xxx789zzz123yyy456xxx/safetyrule/444444444444",
            "GatingControls": [
                "arn:aws:route53-recovery-control::888888888888:controlpanel/
zzz123yyy456xxx789zzz123yyy456xxx/routingcontrol/def123def123def"
            ],
```

```
            "TargetControls": [
                "arn:aws:route53-recovery-control::888888888888:controlpanel/
zzz123yyy456xxx789zzz123yyy456xxx/routingcontrol/ghi456ghi456ghi"
                "arn:aws:route53-recovery-control::888888888888:controlpanel/
zzz123yyy456xxx789zzz123yyy456xxx/routingcontrol/lmn789lmn789lmn"
            ],
            "ControlPanelArn": "arn:aws:route53-recovery-
control::888888888888:controlpanel/zzz123yyy456xxx789zzz123yyy456xxx",
            "Name": "TestGatingRule",
            "RuleConfig": {
                "Inverted": false,
                "Threshold": 0,
                "Type": "OR"
            },
            "Status": "PENDING",
            "WaitPeriodMs": 5000
        }
    }
}
```

Come con altre risorse per il controllo del routing, è possibile descrivere, elencare o eliminare le regole di sicurezza dopo che si sono propagate sul piano dati.

Dopo aver impostato una o più regole di sicurezza, è possibile continuare a interagire con il cluster, impostare o recuperare lo stato dei controlli di routing. Se un'`set-routing-control-state`operazione viola una regola che hai creato, riceverai un'eccezione simile alla seguente:

```
Cannot modify control state for [0123456bbbbbbb0123456bbbbbb01234560123
abcdefg1234567] due to failed rule evaluation
0123456bbbbbbb0123456bbbbbb0123456333333444444
```

Il primo identificatore è l'ARN del pannello di controllo concatenato con l'ARN di controllo del routing. Il secondo identificatore è l'ARN del pannello di controllo concatenato con la regola di sicurezza ARN.

5. Create health checks

Per utilizzare i controlli di routing per il failover del traffico, crei controlli di integrità in Amazon Route 53, quindi associ i controlli di integrità ai tuoi record DNS. Per eseguire il failover del traffico, un controllo di routing ARC imposta il controllo di integrità in modo che Route 53 reindirizzi il traffico. (Il controllo dello stato non conferma lo stato dell'applicazione; viene semplicemente utilizzato come metodo per reindirizzare il traffico.)

Ad esempio, supponiamo che tu abbia due celle (regioni o zone di disponibilità). Ne configuri una come cella principale per l'applicazione e l'altra come secondaria, su cui eseguire il failover.

Per impostare i controlli di integrità per il failover, puoi fare quanto segue, ad esempio:

1. Utilizzate l'ARC CLI per creare un controllo di routing per ogni cella.
2. Utilizza la CLI Route 53 per creare un controllo di integrità ARC in Route 53 per ogni controllo di routing.
3. Utilizza la CLI di Route 53 per creare due record DNS di failover in Route 53 e associare un controllo dello stato a ciascuno di essi.

5a. Crea un controllo di routing per ogni cella.

```
aws route53-recovery-control-config --region us-west-2 create-routing-control \
        --routing-control-name RoutingControlCell1 \
        --cluster-arn arn:aws:route53-recovery-control::111122223333:cluster/5678abcd-
abcd-5678-abcd-5678abcdefgh
```

```
aws route53-recovery-control-config --region us-west-2 create-routing-control \
        --routing-control-name RoutingControlCell2 \
        --cluster-arn arn:aws:route53-recovery-control::111122223333:cluster/5678abcd-
abcd-5678-abcd-5678abcdefgh
```

5 b. Crea un controllo di integrità per ogni controllo di routing.

> **Note**
>
> Puoi creare controlli di integrità ARC utilizzando la CLI di Amazon Route 53.

```
aws route53 create-health-check --caller-reference RoutingControlCell1 \
        --health-check-config \
        Type=RECOVERY_CONTROL,RoutingControlArn=arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567
```

```
{
```

```
    "Location": "https://route53.amazonaws.com/2015-01-01/healthcheck/11111aaaa-bbbb-
cccc-dddd-ffffff22222",
    "HealthCheck": {
        "Id": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
        "CallerReference": "RoutingControlCell1",
        "HealthCheckConfig": {
            "Type": "RECOVERY_CONTROL",
            "Inverted": false,
            "Disabled": false,
            "RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567"
        },
        "HealthCheckVersion": 1
    }
}
```

```
aws route53 create-health-check --caller-reference RoutingControlCell2 \
    --health-check-config \
    Type=RECOVERY_CONTROL,RoutingControlArn=arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567
```

```
{
    "Location": "https://route53.amazonaws.com/2015-01-01/healthcheck/11111aaaa-bbbb-
cccc-dddd-ffffff22222",
    "HealthCheck": {
        "Id": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
        "CallerReference": "RoutingControlCell2",
        "HealthCheckConfig": {
            "Type": "RECOVERY_CONTROL",
            "Inverted": false,
            "Disabled": false,
            "RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567"
        },
        "HealthCheckVersion": 1
    }
}
```

5c. Crea due record DNS di failover e associa un controllo dello stato a ciascuno di essi.

È possibile creare record DNS di failover in Route 53 utilizzando la CLI di Route 53. Per creare i record, segui le istruzioni in Amazon Route 53 AWS CLI Command Reference per il change-resource-record-setscomando. Nei record, specifica il valore DNS per ogni cella insieme al `HealthCheckID` valore corrispondente che Route 53 ha creato per il controllo dello stato di salute (vedi 6b).

Per la cella principale:

```
{
    "Name": "myapp.yourdomain.com",
    "Type": "CNAME",
    "SetIdentifier": "primary",
    "Failover": "PRIMARY",
    "TTL": 0,
    "ResourceRecords": [
        {
            "Value": "cell1.yourdomain.com"
        }
    ],
    "HealthCheckId": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
}
```

Per la cella secondaria:

```
{
    "Name": "myapp.yourdomain.com",
    "Type": "CNAME",
    "SetIdentifier": "secondary",
    "Failover": "SECONDARY",
    "TTL": 0,
    "ResourceRecords": [
        {
            "Value": "cell2.yourdomain.com"
        }
    ],
    "HealthCheckId": "yyyyyy-yyyy-yyyy-yyyy-yyyyyyyyyyyy"
}
```

Ora, per eseguire il failover dalla cella principale alla cella secondaria, puoi seguire l'esempio CLI nel passaggio 4b per aggiornare lo stato di to e `RoutingControlCell1` to`OFF`. `RoutingControlCell2` `ON`

Elenca e aggiorna i controlli e gli stati del routing con il AWS CLI

Dopo aver creato le risorse Amazon Application Recovery Controller (ARC), come cluster, controlli di routing e pannelli di controllo, puoi interagire con il cluster per elencare e aggiornare gli stati di controllo del routing per il failover.

Per ogni cluster che crei, ARC ti fornisce un set di endpoint del cluster, uno su cinque. Regioni AWSÈ necessario specificare uno di questi endpoint regionali (l' Regione AWS e l'URL dell'endpoint) quando si effettuano chiamate al cluster per recuperare o impostare gli stati di controllo del routing su o. `On` `Off` Quando si utilizza AWS CLI, per ottenere o aggiornare gli stati di controllo del routing, oltre all'endpoint regionale, è necessario specificare anche l'endpoint regionale, come illustrato negli esempi `--region` di questa sezione.

È possibile utilizzare qualsiasi endpoint del cluster regionale. Consigliamo di far ruotare i sistemi tra gli endpoint regionali e di prepararsi a riprovare con ciascuno degli endpoint disponibili. Per esempi di codice che illustrano il tentativo degli endpoint del cluster in sequenza, vedi. Azioni per l'utilizzo di Application Recovery Controller AWS SDKs

Per ulteriori informazioni sull'utilizzo di AWS CLI, vedere AWS CLI Command Reference. Per un elenco delle azioni dell'API di controllo del routing e dei collegamenti a ulteriori informazioni, vedereOperazioni dell'API di controllo del routing.

> **Important**
>
> Sebbene sia possibile aggiornare uno stato di controllo del routing sulla console Amazon Route 53, consigliamo di aggiornare gli stati di controllo del routing utilizzando AWS CLI o un AWS SDK. ARC offre un'affidabilità estrema con il piano dati di controllo del routing ARC per il reindirizzamento del traffico e il failover tra le celle. Per ulteriori consigli sull'utilizzo di ARC per il failover, vedere. Le migliori pratiche per il controllo del routing in ARC

Quando si crea un controllo di routing, lo stato viene impostato su. `Off` Ciò significa che il traffico non viene indirizzato alla cella di destinazione per quel controllo di routing. È possibile verificare lo stato del controllo del routing eseguendo il comando. `get-routing-control-state`

Per determinare la regione e l'endpoint da specificare, esegui il `describe-clusters` comando per visualizzare il. `ClusterEndpoints` Ciascuno `ClusterEndpoint` include una regione e un endpoint corrispondente che è possibile utilizzare per ottenere o aggiornare gli stati di controllo del routing. DescribeClusterè un'operazione dell'API di configurazione del controllo del ripristino. Ti

consigliamo di conservare una copia locale degli endpoint del cluster ARC Regional, nei segnalibri o inserendola nel codice di automazione che usi per riprovare gli endpoint.

1. Elenca i controlli di routing

È possibile visualizzare i controlli e gli stati di controllo del routing utilizzando gli endpoint del piano dati ARC altamente affidabili.

1. Elenca i controlli di routing per un pannello di controllo specifico. Se non si specifica un pannello di controllo, `list-routing-controls` restituisce tutti i controlli di routing nel cluster.

```
aws route53-recovery-cluster list-routing-controls --control-panel-arn \
        arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456 \
        --region us-west-2 \
        --endpoint-url https://host-dddddd.us-west-2.example.com/v1
```

```
{
    "RoutingControls": [{
        "ControlPanelArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456",
        "ControlPanelName": "ExampleControlPanel",
        "RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567",
        "RoutingControlName": "RCOne",
        "RoutingControlState": "On"
    },
    {
        "ControlPanelArn": "arn:aws:route53-recovery-
control::023759465626:controlpanel/0123456bbbbbbb0123456bbbbbb0123456",
        "ControlPanelName": "ExampleControlPanel",
        "RoutingControlArn": "arn:aws:route53-recovery-
control::023759465626:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
zzzzxxxxyyyy123456",
        "RoutingControlName": "RCTwo",
        "RoutingControlState": "Off"
    }
]
```

2. Ottieni i controlli di routing

2. Ottieni uno stato di controllo del routing.

```
aws route53-recovery-cluster get-routing-control-state --routing-control-arn \
        arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567 \
        --region us-west-2 \
        --endpoint-url https://host-dddddd.us-west-2.example.com/v1
```

```
{"RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567",
    "RoutingControlName": "RCOne",
    "RoutingControlState": "On"
}
```

2. Aggiorna i controlli di routing

Per indirizzare il traffico verso l'endpoint di destinazione controllato dal controllo del routing, si aggiorna lo stato di controllo del routing a. 0n Aggiornate lo stato di controllo del routing eseguendo il comando. `update-routing-control-state` (Quando la richiesta ha esito positivo, la risposta è vuota.)

2a. Aggiornare uno stato di controllo del routing.

```
aws route53-recovery-cluster update-routing-control-state \
        --routing-control-arn \
        arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567 \
        --routing-control-state On \
        --region us-west-2 \
        --endpoint-url https://host-dddddd.us-west-2.example.com/v1
```

```
{}
```

Puoi aggiornare diversi controlli di routing contemporaneamente con una sola chiamata API:. `update-routing-control-states` (Quando la richiesta ha esito positivo, la risposta è vuota.)

2 b. Aggiorna più stati di controllo del routing contemporaneamente (aggiornamenti in batch).

```
aws route53-recovery-cluster update-routing-control-states \
```

```
        --update-routing-control-state-entries \
        '[{"RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567",
        "RoutingControlState": "Off"}, \
        {"RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
hijklmnop987654321",
        "RoutingControlState": "On"}]' \
        --region us-west-2 \
        --endpoint-url https://host-dddddd.us-west-2.example.com/v1
```

```
{}
```

Utilizzo dei componenti di controllo del routing in ARC

Argomenti

- Creazione di componenti di controllo del routing in ARC
- Visualizzazione e aggiornamento degli stati di controllo del routing in ARC
- Creazione di regole di sicurezza per il controllo del routing
- Supporta più account per i cluster in ARC

Creazione di componenti di controllo del routing in ARC

Questa sezione spiega come creare un cluster, controlli di routing, controlli di integrità e pannelli di controllo per lavorare con il controllo del routing in Amazon Application Recovery Controller (ARC).

Inizia creando un cluster, per ospitare i controlli di routing e i pannelli di controllo che usi per raggrupparli. Quindi crea controlli di routing e controlli di integrità in modo da reindirizzare il traffico per il failover da una cella all'altra, in modo che il traffico vada, ad esempio, alla tua replica di backup.

Tieni presente che ti viene addebitato un costo orario per ogni cluster che crei. In genere è sufficiente un solo cluster per ospitare i controlli di routing e i pannelli di controllo per la gestione del controllo del ripristino per un'applicazione. Inoltre, è possibile configurare la condivisione delle risorse utilizzando AWS Resource Access Manager, in modo che un cluster possa ospitare i controlli di routing e altre risorse ARC di proprietà di più utenti. Account AWS Per ulteriori informazioni sulla condivisione delle risorse in ARC,Supporta più account per i cluster in ARC. Per informazioni sui prezzi, consulta la pagina dei prezzi di Amazon Application Recovery Controller (ARC).

Per utilizzare i controlli di routing per il failover del traffico, crei controlli di integrità del controllo del routing che associ ai record DNS di Amazon Route 53 per le risorse della tua applicazione. Ad esempio, supponiamo che tu abbia due celle, una configurata come cella principale per l'applicazione e l'altra configurata come secondaria, su cui eseguire il failover.

Per configurare i controlli di integrità per il failover, procedi come segue:

1. Create un controllo di routing per ogni cella.
2. Crea un controllo di integrità per ogni controllo di routing.
3. Crea due record DNS, ad esempio due record di failover DNS, e associa un controllo dello stato a ciascuno di essi.

Un altro scenario in cui è possibile creare un controllo di routing è quando si crea una regola di sicurezza che è una regola di gating. In questo caso, non assocerai i controlli di integrità e i record DNS al controllo di routing perché lo utilizzerai come controllo di gating routing. Per ulteriori informazioni, consulta Creazione di regole di sicurezza per il controllo del routing.

I passaggi per creare i componenti per il controllo del routing sulla console ARC sono inclusi in queste sezioni. Per ulteriori informazioni sull'utilizzo delle operazioni dell'API di configurazione del controllo di ripristino con ARC, consulta laOperazioni dell'API di controllo del routing.

Creazione di un cluster in ARC

È necessario creare un cluster per ospitare i controlli di routing e i pannelli di controllo in ARC.

Un cluster è un insieme di endpoint regionali ridondanti su cui è possibile eseguire chiamate API per aggiornare o ottenere lo stato di uno o più controlli di routing. Un singolo cluster può ospitare diversi controlli di routing.

> **Important**
>
> Tieni presente che ti viene addebitato un costo orario per ogni cluster che crei. Un cluster può ospitare diversi controlli di routing e pannelli di controllo per la gestione del controllo del ripristino, in genere sufficienti per un'applicazione.

Come creare un cluster

1. Apri la console ARC all'indirizzohttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Scegli Cluster.
3. Scegli Crea, quindi inserisci un nome per il cluster.
4. Scegli Crea cluster.

Creazione di un controllo di routing in ARC

Crea un controllo di routing per ogni cella verso cui vuoi indirizzare il traffico. Ad esempio, se disponi di un'applicazione con risorse suddivise in silos per la ripristinabilità, potresti avere una cella per ciascuna e celle nidificate per ogni Regione AWS zona di disponibilità all'interno di ciascuna regione. In questo scenario, è necessario creare un controllo di routing per ogni cella e ogni cella annidata.

Quando create i controlli di routing, tenete presente che i nomi dei controlli di routing devono essere univoci all'interno di ogni pannello di controllo.

Dopo aver creato i controlli di routing da utilizzare per reindirizzare il traffico, associ ciascuno di essi a un controllo di integrità, che ti consente di indirizzare il traffico verso le celle, in base ai record DNS che hai associato a ciascuno di essi. Se stai impostando una regola di gating come regola di sicurezza e stai creando un controllo di gating routing, non aggiungi un controllo di integrità al controllo di routing.

Per creare un controllo di routing

1. Apri la console ARC all'indirizzohttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Scegli Routing control.
3. Nella pagina di controllo del routing, scegli Crea, quindi scegli un controllo di routing.
4. Inserisci un nome per il controllo del routing, scegli il cluster a cui aggiungere il controllo e scegli di aggiungerlo a un pannello di controllo esistente, incluso l'utilizzo del pannello di controllo predefinito. In alternativa, crea un nuovo pannello di controllo.
5. Se scegli di creare un nuovo pannello di controllo, scegli un cluster in cui creare il pannello di controllo, quindi inserisci un nome per il pannello.
6. Scegliete Crea controllo di routing.
7. Segui i passaggi per denominare e creare il controllo di routing.

Creazione di un controllo dello stato del routing in ARC

Si associa un controllo dello stato del controllo del routing a ciascun controllo di routing che si desidera utilizzare per reindirizzare il traffico. Quindi configuri ogni controllo di integrità con un record DNS di Amazon Route 53, ad esempio un record DNS di failover. Quindi puoi reindirizzare il traffico in Amazon Application Recovery Controller (ARC) semplicemente aggiornando lo stato del controllo di routing associato, impostandolo su o. `On` `Off`

> **Note**
>
> Non è possibile modificare un controllo di integrità del controllo di routing esistente per associarlo a un controllo di routing diverso.

Per creare un controllo dello stato del routing control

1. Apri la console ARC all'indirizzohttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Scegli Routing control.
3. Nella pagina Controllo del routing, scegli un controllo di routing.
4. Nella pagina dei dettagli del controllo del routing, scegli Crea controllo di integrità.
5. Inserisci un nome per il controllo dello stato, quindi scegli Crea.

Successivamente, crei i record DNS di Route 53 e associ i controlli di integrità del controllo del routing a ciascuno di essi. Ad esempio, supponiamo di voler utilizzare due record di failover DNS a cui associare i controlli di integrità del controllo del routing. Affinché ARC esegua correttamente il failover del traffico utilizzando i controlli di routing, inizia creando i due record di failover in Route 53: uno principale e uno secondario. Per ulteriori informazioni sulla configurazione dei record di failover DNS, vedere Health checking concepts.

Quando si crea il record di failover principale, i valori devono essere simili ai seguenti:

```
Name: myapp.yourdomain.com
Type: CNAME
Set Identifier: Primary
Failover: Primary
TTL: 0
```

```
Resource Records:
Value: cell1.yourdomain.com
Health Check ID: xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
```

I valori del record di failover secondario devono essere simili ai seguenti:

```
Name: myapp.yourdomain.com
Type: CNAME
Set Identifier: Secondary
Failover: Secondary
TTL: 0
Resource Records:
Value: cell2.yourdomain.com
Health Check ID: xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
```

Supponiamo ora di voler reindirizzare il traffico perché c'è un errore. A tale scopo, si aggiornano gli stati di controllo del routing associati per modificare lo stato di controllo del routing primario in `OFF` e lo stato di controllo del routing secondario in. `ON` Quando si esegue questa operazione, i controlli di integrità associati impediscono al traffico di passare alla replica principale e lo indirizzano invece alla replica secondaria. Per ulteriori informazioni sul failover del traffico con i controlli di routing, vedere. Ottenere e aggiornare gli stati di controllo del routing utilizzando l'API ARC (consigliato)

Per vedere esempi di AWS CLI comandi per la creazione di controlli di routing e i relativi controlli di integrità utilizzando le operazioni dell'API ARC, vedere. Esempi di utilizzo delle operazioni dell'API di controllo del routing ARC con AWS CLI

Creazione di un pannello di controllo in ARC

Un pannello di controllo in Amazon Application Recovery Controller (ARC) consente di raggruppare i controlli di routing correlati. Un pannello di controllo può avere controlli di routing che rappresentano un microservizio all'interno di un'applicazione, un'intera applicazione stessa o un gruppo di applicazioni, a seconda dell'ambito del failover. Un vantaggio del raggruppamento dei controlli di routing in un pannello di controllo è la possibilità di utilizzare le regole di sicurezza con un pannello di controllo per proteggere le modifiche al routing del traffico.

Quando si crea un cluster, ARC crea un pannello di controllo predefinito. È possibile utilizzare il pannello di controllo predefinito per i controlli di routing oppure creare uno o più pannelli di controllo per raggruppare i controlli di routing. Nota che per i nomi dei pannelli di controllo sono supportati solo i caratteri ASCII.

I passaggi per creare un pannello di controllo sulla console ARC sono inclusi in questa sezione. Per informazioni sull'utilizzo delle operazioni dell'API di configurazione del controllo di ripristino con ARC, consulta laOperazioni dell'API di controllo del routing.

Per creare un pannello di controllo

1. Apri la console ARC all'indirizzohttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Scegli Routing control.
3. Nella pagina di controllo del routing, scegli Crea, quindi scegli un pannello di controllo.
4. Scegliete un cluster su cui creare il pannello di controllo, quindi inserite un nome per il pannello.
5. Scegli Crea pannello di controllo.

Visualizzazione e aggiornamento degli stati di controllo del routing in ARC

Questa sezione descrive come visualizzare e aggiornare gli stati di controllo del routing in Amazon Application Recovery Controller (ARC). I controlli di routing sono semplici interruttori on-off che gestiscono il flusso di traffico verso le celle del gruppo di ripristino. Le celle sono in genere Regioni AWS, o talvolta zone di disponibilità, che includono le risorse dell'utente. Quando lo stato di controllo del routing è impostato su 00n, il traffico fluisce verso la cella controllata da quel controllo di routing.

I controlli di routing vengono raggruppati in pannelli di controllo, che sono raggruppamenti logici di failover. Quando si apre un pannello di controllo sulla console, ad esempio, è possibile visualizzare contemporaneamente tutti i controlli di routing per un raggruppamento, per vedere dove scorre il traffico.

È possibile aggiornare lo stato di controllo del routing sulla console ARC o utilizzando l'API ARC. Ti consigliamo di aggiornare gli stati di controllo del routing utilizzando l'API. Innanzitutto, ARC offre un'affidabilità estrema con l'API nel piano dati per eseguire queste azioni. Questo è importante quando si modificano questi stati, perché le modifiche allo stato di routing falliscono tra le celle reindirizzando il traffico delle applicazioni. Inoltre, utilizzando l'API, puoi provare a connetterti a diversi endpoint del cluster a rotazione, se necessario, se un endpoint del cluster a cui tenti di connetterti non è disponibile.

È possibile aggiornare uno stato di controllo del routing oppure aggiornare più stati di controllo del routing contemporaneamente. Ad esempio, potresti voler impostare uno stato di controllo del routing per impedire `0ff` al traffico di fluire verso una cella, ad esempio una zona di disponibilità

in cui un'applicazione presenta una maggiore latenza. Allo stesso tempo, potresti voler impostare un altro stato di controllo del routing per avviare il flusso del traffico 0n verso un'altra cella o zona di disponibilità. In questo scenario, puoi aggiornare entrambi gli stati di controllo del routing contemporaneamente, in modo che il traffico continui a fluire.

Argomenti

- Ottenere e aggiornare gli stati di controllo del routing utilizzando l'API ARC (consigliato)
- Ottenere e aggiornare gli stati di controllo del routing in Console di gestione AWS

Ottenere e aggiornare gli stati di controllo del routing utilizzando l'API ARC (consigliato)

Ti consigliamo di utilizzare le operazioni API di Amazon Application Recovery Controller (ARC) per ottenere o aggiornare gli stati di controllo del routing, utilizzando un AWS CLI comando o utilizzando il codice che hai sviluppato per utilizzare le operazioni dell'API ARC con uno dei AWS SDKs. Si consiglia di utilizzare le operazioni API, con la CLI o nel codice, per lavorare con gli stati di controllo del routing, anziché utilizzare il. Console di gestione AWS

ARC offre un'affidabilità estrema per il failover tra celle (Regioni AWS) aggiornando gli stati di controllo del routing utilizzando l'API, poiché i controlli di routing sono archiviati in un cluster ad alta disponibilità. ARC garantisce che almeno tre dei cinque endpoint del cluster regionale siano sempre accessibili all'utente per apportare modifiche allo stato di controllo del routing. Per ottenere o modificare uno stato di controllo del routing utilizzando l'API, ti connetti a uno degli endpoint del cluster regionale. Se l'endpoint non è disponibile, puoi provare a connetterti a un altro degli endpoint del cluster.

Puoi visualizzare l'elenco degli endpoint regionali del cluster per il tuo cluster nella console Route 53 o utilizzando un'azione API,. DescribeCluster Il processo di acquisizione e modifica degli stati di controllo del routing dovrebbe provare ogni endpoint a rotazione, se necessario, poiché gli endpoint del cluster vengono alternati tra gli stati disponibili e non disponibili per manutenzione e aggiornamenti regolari.

Forniamo informazioni dettagliate ed esempi di codice per l'utilizzo delle operazioni dell'API ARC per ottenere e aggiornare gli stati di controllo del routing e per utilizzare gli endpoint dei cluster regionali. Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per esempi di codice che spiegano come ruotare tra gli endpoint dei cluster regionali per ottenere e impostare gli stati di controllo del routing, consulta. Azioni per l'utilizzo di Application Recovery Controller AWS SDKs

- Per informazioni sull'utilizzo di per ottenere e aggiornare AWS CLI gli stati di controllo del routing, vedere. Elenca e aggiorna i controlli e gli stati del routing con il AWS CLI

Ottenere e aggiornare gli stati di controllo del routing in Console di gestione AWS

È possibile ottenere e aggiornare gli stati di controllo del routing in. Console di gestione AWS Tieni presente, tuttavia, che non puoi scegliere endpoint di cluster regionali diversi nella console. Cioè, non esiste un processo per la scelta e la rotazione degli endpoint del cluster nella console, come è possibile fare utilizzando l'API Amazon Application Recovery Controller (ARC). Inoltre, la console non è altamente disponibile mentre il piano dati ARC offre un'affidabilità estrema. Per questi motivi, consigliamo di utilizzare l'API ARC per ottenere e aggiornare gli stati di controllo del routing per le operazioni di produzione.

Per ulteriori consigli sull'utilizzo di ARC per il failover, consulta. Le migliori pratiche per il controllo del routing in ARC

Per visualizzare e aggiornare i controlli di routing nella console, segui i passaggi indicati nelle seguenti procedure.

Per ottenere gli stati di controllo del routing

1. Apri la console ARC all'indirizzohttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Scegli Routing control.
3. Dall'elenco, scegli un pannello di controllo e visualizza i controlli di routing.

Per aggiornare uno o più stati di controllo del routing

1. Apri la console Amazon Route 53 a https://console.aws.amazon.com/route53/casa.
2. In Application Recovery Controller, scegli Routing control.
3. Scegli Azione, quindi scegli Modifica il routing del traffico.
4. Aggiorna lo stato di uno o più controlli di routing impostandolo su `Off` o`On`, a seconda di dove desideri che il traffico fluisca o smetta di fluire per la tua applicazione.
5. Immetti `confirm` nella casella di testo.
6. Scegli Aggiorna il routing del traffico.

Creazione di regole di sicurezza per il controllo del routing

Quando si utilizzano più controlli di routing contemporaneamente, è possibile decidere di adottare misure di protezione per evitare conseguenze indesiderate. Ad esempio, potreste voler evitare che tutti i controlli di routing di un'applicazione vengano disattivati inavvertitamente, con il risultato di uno scenario di fail-open. Oppure potreste voler implementare un interruttore principale di accensione e spegnimento per disabilitare un set di controlli di routing, magari per impedire all'automazione di reindirizzare il traffico. Per stabilire protezioni come queste per il controllo del routing in ARC, create delle regole di sicurezza.

Le regole di sicurezza per il controllo del routing vengono configurate con una combinazione di controlli di routing, regole e altre opzioni specificate dall'utente. Ogni regola di sicurezza è associata a un singolo pannello di controllo, ma un pannello di controllo può avere più di una regola di sicurezza. Quando crei regole di sicurezza, tieni presente che i nomi delle regole di sicurezza devono essere univoci all'interno di ogni pannello di controllo.

Argomenti

- Tipi di regole di sicurezza
- Creazione di una regola di sicurezza sulla console
- Modifica o eliminazione di una regola di sicurezza sulla console
- Sostituire le regole di sicurezza per reindirizzare il traffico

Tipi di regole di sicurezza

Esistono due tipi di regole di sicurezza, regole di asserzione e regole di controllo, che è possibile utilizzare per proteggere il failover in diversi modi.

Regola di asserzione

Con una regola di asserzione, quando si modifica uno o più stati di controllo del routing, ARC impone che i criteri impostati durante la configurazione della regola siano soddisfatti, altrimenti gli stati di controllo del routing non vengono modificati.

Un esempio di quando ciò è utile è prevenire uno scenario di fail-open, ad esempio uno scenario in cui si impedisce al traffico di andare verso una cella ma non si avvia il flusso del traffico verso un'altra cella. Per evitare ciò, una regola di asserzione assicura che almeno un controllo di routing in un set di controlli di routing in un pannello di controllo sia presente in un dato momento.

0n Ciò garantisce che il traffico fluisca verso almeno una regione o zona di disponibilità per un'applicazione.

Per vedere un AWS CLI comando di esempio che crea una regola di asserzione per applicare questi criteri, vedi Creare regole di sicurezza in. Esempi di utilizzo delle operazioni dell'API di controllo del routing ARC con AWS CLI

Per informazioni dettagliate sulle proprietà operative dell'API della regola di asserzione, consulta AssertionRulela Routing Control API Reference Guide for Amazon Application Recovery Controller.

Regola di gating

Con una regola di gating, è possibile applicare un interruttore on/off generale su una serie di controlli di routing in modo che la possibilità di modificare tali stati di controllo del routing venga applicata in base a una serie di criteri specificati nella regola. Il criterio più semplice è se un singolo controllo di routing specificato come switch è impostato su o. `0N` `0FF`

A tal fine, è necessario creare un controllo di routing basato sul gateway, da utilizzare come switch generale, e utilizzare i controlli di routing di destinazione, per controllare il flusso di traffico verso diverse regioni o zone di disponibilità. Quindi, per evitare aggiornamenti manuali o automatici dello stato dei controlli di routing di destinazione configurati per la regola di gating, imposti lo stato di controllo del gating routing su. `0ff` Per consentire gli aggiornamenti, lo imposti su. `0n`

Per vedere un AWS CLI comando di esempio che crea una regola di gating che implementa questo tipo di switch generale, vedi Creare regole di sicurezza in. Esempi di utilizzo delle operazioni dell'API di controllo del routing ARC con AWS CLI

Per informazioni dettagliate sulle proprietà operative dell'API gating rule, consulta GatingRulela Routing Control API Reference Guide for Amazon Application Recovery Controller.

Creazione di una regola di sicurezza sulla console

I passaggi di questa sezione spiegano come creare una regola di sicurezza sulla console ARC. I passaggi sono simili sia che si crei una regola di asserzione che una regola di gating. Le differenze sono riportate nella procedura.

Per ulteriori informazioni sull'utilizzo delle operazioni API di ripristino e controllo del routing con Amazon Application Recovery Controller (ARC), consultaOperazioni dell'API di controllo del routing.

Per creare una regola di sicurezza

1. Apri la console ARC all'indirizzohttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Scegli Routing control.
3. Nella pagina di controllo del routing, scegli un pannello di controllo.
4. Nella pagina dei dettagli del pannello di controllo, scegli Azione, quindi scegli Aggiungi regola di sicurezza.
5. Scegli un tipo di regola da aggiungere: regola di asserzione o regola di Gating.
6. Scegli un nome e, facoltativamente, modifica il periodo di attesa.
7. Specificate le opzioni di configurazione per la regola di sicurezza.

   - Per una regola di asserzione, specifica i controlli di routing asseriti.
   - Per una regola di gating, specifica il controllo di gating routing e i controlli di destinazione di routing.

   Per entrambe le regole, specifica la configurazione della regola scegliendo il tipo e la soglia e se la regola è invertita.

   > **Note**
   >
   > Per ulteriori informazioni sulla specificazione di una regola di asserzione, consulta le informazioni fornite per il AssertionRulefunzionamento nella Routing Control API Reference Guide per Amazon Application Recovery Controller. Per ulteriori informazioni sulla specificazione di una regola di gating, consulta le informazioni fornite per l'GatingRuleoperazione nella Routing Control API Reference Guide for Amazon Application Recovery Controller.

8. Scegli Create (Crea).

Modifica o eliminazione di una regola di sicurezza sulla console

I passaggi di questa sezione spiegano come modificare o eliminare una regola di sicurezza sulla console ARC. È possibile apportare solo modifiche limitate a una regola di sicurezza, per cambiare il nome o aggiornare il periodo di attesa. Per apportare altre modifiche, elimina e ricrea la regola di sicurezza.

Per ulteriori informazioni sull'utilizzo delle operazioni API con Amazon Application Recovery Controller (ARC), consulta ilOperazioni dell'API di controllo del routing.

Per eliminare una regola di sicurezza

1. Apri la console ARC all'indirizzohttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Scegli Routing control.
3. Nella pagina di controllo del routing, scegli un pannello di controllo.
4. Nella pagina dei dettagli del pannello di controllo, scegli una regola di sicurezza, quindi scegli Elimina o Modifica.

Sostituire le regole di sicurezza per reindirizzare il traffico

In alcuni casi potresti voler aggirare le protezioni di controllo del routing applicate con le regole di sicurezza che hai configurato. Ad esempio, potresti voler eseguire rapidamente il failover per il disaster recovery e una o più regole di sicurezza potrebbero impedirti inaspettatamente di aggiornare lo stato di controllo del routing per reindirizzare il traffico. In uno scenario «break glass» come questo, è possibile ignorare una o più regole di sicurezza per modificare lo stato di controllo del routing e eseguire il failover dell'applicazione.

È possibile ignorare le regole di sicurezza quando si aggiorna uno stato di controllo del routing (o più stati di controllo del routing) utilizzando il comando `update-routing-control-state` o `update-routing-control-states` AWS CLI con il parametro. `safety-rules-to-override` Specificate il parametro con l'Amazon Resource Name (ARN) della regola di sicurezza che desiderate sostituire o specificate un elenco separato da virgole per sovrascrivere due o più regole ARNs di sicurezza.

Quando una regola di sicurezza blocca un aggiornamento dello stato di controllo del routing, il messaggio di errore include l'ARN della regola che ha bloccato l'aggiornamento. Quindi puoi prendere nota dell'ARN e quindi specificarlo in un comando CLI dello stato di controllo del routing con il parametro safety rule override.

> **Note**
>
> Poiché potrebbero essere in vigore più regole di sicurezza per i controlli di routing che stai aggiornando, puoi eseguire il comando CLI per aggiornare lo stato del controllo del routing sostituendo una regola di sicurezza, ma ricevi un errore che indica che un'altra regola di

sicurezza sta bloccando l'aggiornamento. Continua ad aggiungere la regola di sicurezza ARNs all'elenco delle regole da sostituire nel comando update, separate da virgole, fino al completamento corretto del comando di aggiornamento.

Per ulteriori informazioni sull'utilizzo della `SafetyRulesToOverride` proprietà con l'API e SDKs, consulta. UpdateRoutingControlState

Di seguito sono riportati due esempi di comandi CLI per sovrascrivere le regole di sicurezza per aggiornare gli stati di controllo del routing.

Ignora una regola di sicurezza

```
aws route53-recovery-cluster --region us-west-2 update-routing-control-state \
    --routing-control-arn \
    arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/
routingcontrol/abcdefg1234567 \
    --routing-control-state On \
    --safety-rules-to-override arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/safetyrule/
yyyyyyy8888888 \
    --endpoint-url https://host-dddddd.us-west-2.example.com/v1
```

Ignora due regole di sicurezza

```
aws route53-recovery-cluster --region us-west-2 update-routing-control-state \
    --routing-control-arn \
    arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/
routingcontrol/abcdefg1234567 \
    --routing-control-state On \
    --safety-rules-to-override "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/safetyrule/
yyyyyyy8888888" \
    "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/safetyrule/
qqqqqqq7777777"
    --endpoint-url https://host-dddddd.us-west-2.example.com/v1
```

Supporta più account per i cluster in ARC

Amazon Application Recovery Controller (ARC) si integra con AWS Resource Access Manager per abilitare la condivisione delle risorse. AWS RAM è un servizio che consente di condividere risorse con altri Account AWS o tramite AWS Organizations. Per il controllo del routing ARC, è possibile condividere la risorsa del cluster.

Con AWS RAM, condividi le risorse di tua proprietà creando una condivisione di risorse. Una condivisione di risorse specifica le risorse da condividere e i partecipanti con cui condividerle. I partecipanti possono includere:

- Specifico Account AWS all'interno o all'esterno dell'organizzazione del proprietario in AWS Organizations
- Un'unità organizzativa all'interno della sua organizzazione in AWS Organizations
- La sua intera organizzazione in AWS Organizations

Per ulteriori informazioni in merito AWS RAM, consulta la Guida AWS RAM per l'utente.

Utilizzando AWS Resource Access Manager per condividere le risorse del cluster tra gli account in ARC, è possibile utilizzare un cluster per ospitare pannelli di controllo e controlli di routing di proprietà di diversi Account AWS account. Quando si sceglie di condividere un cluster, Account AWS gli altri utenti specificati possono utilizzare il cluster per ospitare i propri pannelli di controllo e controlli di routing, garantendo maggiore controllo e flessibilità sulle funzionalità di routing tra team diversi.

AWS RAM è un servizio che aiuta AWS i clienti a condividere in modo sicuro le risorse tra i clienti. Account AWS Con AWS RAM, puoi condividere risorse all'interno di un'organizzazione o di unità organizzative (OUs) in AWS Organizations, utilizzando ruoli e utenti IAM. AWS RAM è un modo centralizzato e controllato per condividere un cluster.

Quando si condivide un cluster, è possibile ridurre il numero totale di cluster richiesti dall'organizzazione. Con un cluster condiviso, è possibile allocare il costo totale di gestione del cluster tra diversi team, per massimizzare i vantaggi di ARC a costi inferiori. (La creazione di risorse ospitate in un cluster non comporta costi aggiuntivi né per il proprietario né per i partecipanti.) La condivisione di cluster tra account può anche semplificare il processo di onboarding di più applicazioni su ARC, soprattutto se si dispone di un gran numero di applicazioni distribuite su più account e team operativi.

Per iniziare con la condivisione tra account in ARC, devi creare una condivisione di risorse in. AWS RAM La condivisione delle risorse specifica i partecipanti autorizzati a condividere il cluster

di proprietà del tuo account. I partecipanti possono quindi creare risorse, come pannelli di controllo e controlli di routing, nel cluster, utilizzando Console di gestione AWS o eseguendo operazioni API ARC utilizzando o. AWS Command Line Interface AWS SDKs

Questo argomento spiega come condividere le tue risorse e come utilizzare le risorse condivise con te.

Indice

- Prerequisiti per la condivisione dei cluster
- Condivisione di un cluster
- Annullamento della condivisione di un cluster condiviso
- Identificazione di un cluster condiviso
- Responsabilità e autorizzazioni per i cluster condivisi
- Costi di fatturazione
- Quote

Prerequisiti per la condivisione dei cluster

- Per condividere un cluster, devi possederlo nel tuo. Account AWS Ciò significa che la risorsa deve essere allocata o assegnata all'account. Non puoi condividere un cluster che è stato condiviso con te.
- Per condividere un cluster con la tua organizzazione o un'unità organizzativa AWS Organizations, devi abilitare la condivisione con AWS Organizations. Per ulteriori informazioni, consulta Abilitare la condivisione con AWS Organizations nella Guida per l'utente di AWS RAM .
- AWS RAM le condivisioni di risorse per risorse globali come i cluster devono essere create nella regione Stati Uniti orientali (Virginia settentrionale) (us-east-1).

Condivisione di un cluster

Quando condividi un cluster di tua proprietà, i partecipanti specificati per la condivisione del cluster possono creare e ospitare le proprie risorse ARC nel cluster.

Per condividere un cluster, è necessario aggiungerlo a una condivisione di risorse. Una condivisione di risorse è una risorsa AWS RAM che consente di condividere le risorse tra Account AWS. Una condivisione di risorse specifica le risorse da condividere e i partecipanti con cui vengono condivise. Per condividere un cluster è possibile creare una nuova condivisione di risorse o aggiungere la

risorsa a una condivisione di risorse esistente. Per creare una nuova condivisione di risorse, puoi utilizzare la AWS RAM console o utilizzare le operazioni AWS RAM API con AWS Command Line Interface o AWS SDKs.

Se fai parte di un'organizzazione AWS Organizations e la condivisione all'interno dell'organizzazione è abilitata, ai partecipanti dell'organizzazione viene automaticamente concesso l'accesso al cluster condiviso. In caso contrario, i partecipanti ricevono un invito a partecipare alla condivisione di risorse e ottengono l'accesso al cluster condiviso dopo aver accettato l'invito.

Puoi condividere un cluster di tua proprietà utilizzando la AWS RAM console o utilizzando le operazioni AWS RAM API con AWS CLI o SDKs.

Per condividere un cluster di tua proprietà utilizzando la AWS RAM console

Vedi Creazione di una condivisione di risorse nella Guida AWS RAM per l'utente.

Per condividere un cluster di tua proprietà utilizzando il AWS CLI

Utilizza il comando create-resource-share.

Concessione delle autorizzazioni per condividere i cluster

La condivisione di cluster tra account richiede le autorizzazioni per il principale IAM che condivide il cluster tramite. AWS RAM

Ti consigliamo di utilizzare la policy IAM `AmazonRoute53RecoveryControlConfigFullAccess` gestita per garantire che i tuoi responsabili IAM dispongano delle autorizzazioni necessarie per condividere e utilizzare i cluster condivisi.

La condivisione di un cluster utilizzando una policy IAM personalizzata richiede `route53-recovery-control-config:PutResourcePolicy` e `route53-recovery-control-config:DeleteResourcePolicy` autorizzazioni per quel cluster. `route53-recovery-control-config:GetResourcePolicy` `PutResourcePolicye` `DeleteResourcePolicy` sono azioni IAM soggette a solo autorizzazione. Il tentativo di condividere un cluster AWS RAM senza disporre di queste autorizzazioni genererà un errore.

Per ulteriori informazioni sul modo in cui AWS Resource Access Manager utilizza IAM, consulta How AWS Resource Access Manager uses IAM nella Guida per l'AWS RAM utente.

Annullamento della condivisione di un cluster condiviso

Quando annulli la condivisione di un cluster, ai partecipanti e ai proprietari si applica quanto segue:

- Le risorse correnti dei partecipanti continuano a esistere nel cluster non condiviso.
- I partecipanti possono continuare ad aggiornare gli stati di controllo del routing nel cluster non condiviso, per gestire il routing per il failover delle applicazioni.
- I partecipanti non possono più creare nuove risorse nel cluster non condiviso.
- Se i partecipanti dispongono ancora di risorse in un cluster non condiviso, il proprietario non può eliminare il cluster condiviso.

Per annullare la condivisione di un cluster condiviso di tua proprietà, rimuovilo dalla condivisione di risorse. Puoi farlo utilizzando la AWS RAM console o utilizzando le operazioni AWS RAM API con AWS CLI o SDKs.

Per annullare la condivisione di un cluster condiviso di tua proprietà utilizzando la console AWS RAM

Consulta Aggiornamento di una condivisione di risorse nella Guida per l'utente di AWS RAM .

Per annullare la condivisione di un cluster condiviso di tua proprietà utilizzando il AWS CLI

Utilizza il comando disassociate-resource-share.

Identificazione di un cluster condiviso

I proprietari e i partecipanti possono identificare i cluster condivisi visualizzando le informazioni in AWS RAM. Possono inoltre ottenere informazioni sulle risorse condivise utilizzando la console ARC e AWS CLI.

In generale, per saperne di più sulle risorse che hai condiviso o che sono state condivise con te, consulta le informazioni nella Guida per l' AWS Resource Access Manager utente:

- In qualità di proprietario, puoi visualizzare tutte le risorse che condividi con altri utilizzando AWS RAM. Per ulteriori informazioni, vedi Visualizzazione delle risorse condivise in AWS RAM.
- Come partecipante, puoi visualizzare tutte le risorse condivise con te utilizzando AWS RAM. Per ulteriori informazioni, vedi Visualizzazione delle risorse condivise in AWS RAM.

In qualità di proprietario, puoi determinare se stai condividendo un cluster visualizzando le informazioni nelle operazioni dell'API Console di gestione AWS o utilizzando le operazioni dell'API AWS Command Line Interface con ARC.

Per identificare se un cluster di tua proprietà è condiviso utilizzando la console

Nella Console di gestione AWS pagina dei dettagli di un cluster, vedi lo Stato di condivisione del cluster.

Per identificare se un cluster di tua proprietà è condiviso utilizzando il AWS CLI

Utilizza il comando get-resource-policy. Se esiste una politica delle risorse per un cluster, il comando restituisce informazioni sulla politica.

In qualità di partecipante, quando un cluster viene condiviso con te, in genere devi accettare la condivisione. Inoltre, il campo Proprietario del cluster contiene l'account del proprietario del cluster.

Responsabilità e autorizzazioni per i cluster condivisi

Autorizzazioni per i proprietari

Quando condividi un cluster di tua proprietà con altri Account AWS, i partecipanti autorizzati a utilizzare il cluster possono creare pannelli di controllo, controlli di routing e altre risorse nel cluster.

In qualità di proprietario del cluster, sei responsabile della creazione, della gestione e dell'eliminazione dei cluster. Non puoi modificare o eliminare le risorse create dai partecipanti, come i controlli di routing e le regole di sicurezza. Ad esempio, non è possibile aggiornare un controllo di routing creato da un partecipante per modificare lo stato del controllo di routing.

Tuttavia, puoi visualizzare i dettagli dei controlli di routing creati dai partecipanti a un cluster di tua proprietà. Ad esempio, è possibile visualizzare gli stati di controllo del routing chiamando un'operazione dell'API di controllo del routing ARC, utilizzando o. AWS Command Line Interface AWS SDKs

Se devi modificare le risorse create dai partecipanti, questi possono impostare un ruolo in IAM con l'autorizzazione ad accedere alle risorse e aggiungere il tuo account al ruolo.

Autorizzazioni per i partecipanti

In generale, i partecipanti possono creare e utilizzare pannelli di controllo, controlli di routing, regole di sicurezza e controlli di integrità creati in un cluster condiviso con loro. Possono visualizzare, modificare o eliminare le risorse del cluster nel cluster condiviso solo se sono proprietari delle risorse. Ad esempio, i partecipanti possono creare ed eliminare regole di sicurezza per i pannelli di controllo che hanno creato.

Ai partecipanti si applicano le seguenti restrizioni:

- I partecipanti non possono visualizzare, modificare o eliminare i pannelli di controllo creati da altri account utilizzando un cluster condiviso.
- I partecipanti non possono visualizzare, creare o modificare i controlli di routing, inclusi gli stati di controllo del routing, per le risorse create in un cluster condiviso da altri account.
- I partecipanti non possono creare, modificare o visualizzare le regole di sicurezza create da altri account in un cluster condiviso.
- I partecipanti non possono aggiungere risorse nel pannello di controllo predefinito di un cluster condiviso perché appartiene al proprietario del cluster.

Come indicato, i partecipanti non possono creare controlli di routing nel pannello di controllo predefinito per un cluster condiviso, poiché il proprietario del cluster possiede il pannello di controllo predefinito. Tuttavia, il proprietario del cluster può creare un ruolo IAM multiaccount che fornisce l'autorizzazione per accedere al pannello di controllo predefinito per il cluster. Quindi, il proprietario può concedere a un partecipante le autorizzazioni per assumere il ruolo, in modo che il partecipante possa accedere al pannello di controllo predefinito per utilizzarlo come specificato dal proprietario tramite le autorizzazioni del ruolo.

Costi di fatturazione

Al proprietario di un cluster in ARC vengono fatturati i costi associati al cluster. Non ci sono costi aggiuntivi, per i proprietari dei cluster o per i partecipanti, per la creazione di risorse ospitate in un cluster.

Per informazioni dettagliate ed esempi sui prezzi, consulta la pagina dei prezzi di Amazon Application Recovery Controller (ARC).

Quote

Tutte le risorse create in un cluster condiviso, incluse le risorse create da tutti i partecipanti con accesso al cluster condiviso, vengono conteggiate ai fini delle quote valide per il cluster e altre risorse, come i controlli di routing. Se gli account che condividono la risorsa del cluster hanno una quota superiore rispetto alle quote del proprietario del cluster, le quote del proprietario del cluster hanno la precedenza sulle quote degli account che condividono.

Per capire meglio come funziona, consulta i seguenti esempi. Per illustrare come funzionano le quote con la condivisione delle risorse, per questi esempi, supponiamo che il proprietario del cluster sia Proprietario e un account con cui il cluster è stato condiviso sia Partecipante.

Quota dei pannelli di controllo

Vengono applicate delle quote per il totale dei pannelli di controllo del proprietario per cluster.

Ad esempio, supponiamo che Owner abbia una quota di 50 per il numero di pannelli di controllo per cluster e abbia 13 pannelli di controllo nel cluster. Supponiamo ora che il Partecipante abbia la quota impostata su 150. In questo scenario, Participant può creare solo fino a 37 pannelli di controllo (ovvero 50-13) nel cluster condiviso.

Inoltre, se altri account che condividono il cluster creano anche pannelli di controllo, anche questi vengono conteggiati ai fini della quota complessiva del cluster di 50 pannelli di controllo.

Quote di controllo del routing

I controlli di routing hanno quote multiple: una quota per pannello di controllo, una quota per cluster e una quota per regola di sicurezza. Le quote del proprietario hanno la precedenza per tutte queste quote.

Ad esempio, supponiamo che Owner abbia una quota di 300 per il numero di controlli di routing per cluster e disponga già di 300 controlli di routing nel cluster. Supponiamo ora che Participant abbia questa quota impostata su 500. In questo scenario, Participant non può creare nuovi controlli di routing nel cluster condiviso.

Regole di sicurezza, quote

Le quote vengono applicate in base alle regole di sicurezza del proprietario per quota del pannello di controllo.

Ad esempio, supponiamo che il Proprietario abbia una quota di 20 per il numero di regole di sicurezza per pannello di controllo e il Partecipante abbia questa quota impostata su 80. In questo scenario, poiché il limite inferiore del proprietario ha la precedenza, il partecipante può creare solo fino a 20 regole di sicurezza in un pannello di controllo del cluster condiviso.

Per un elenco delle quote di controllo del routing, vedere. Quote per il controllo del routing

Registrazione e monitoraggio per il controllo del routing in Amazon Application Recovery Controller (ARC)

Puoi utilizzarlo AWS CloudTrail per monitorare il controllo del routing in Amazon Application Recovery Controller (ARC), per analizzare i modelli e aiutare a risolvere i problemi.

Argomenti

- Registrazione delle chiamate API ARC utilizzando AWS CloudTrail

Registrazione delle chiamate API ARC utilizzando AWS CloudTrail

Amazon Application Recovery Controller (ARC) è integrato con AWS CloudTrail un servizio che fornisce un registro delle azioni intraprese da un utente, ruolo o AWS servizio in ARC. CloudTrail acquisisce tutte le chiamate API per ARC come eventi. Le chiamate acquisite includono chiamate dalla console ARC e chiamate in codice alle operazioni dell'API ARC.

Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per ARC. 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, è possibile determinare la richiesta che è stata effettuata ad ARC, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e ulteriori dettagli.

Per ulteriori informazioni CloudTrail, consulta la Guida AWS CloudTrail per l'utente.

Informazioni ARC in CloudTrail

CloudTrail è abilitato sul tuo account al Account AWS momento della creazione dell'account. Quando si verifica un'attività in ARC, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi AWS di servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare eventi recenti in Account AWS. Per ulteriori informazioni, consulta Lavorare con la cronologia CloudTrail degli eventi.

Per una registrazione continua degli eventi del tuo Account AWS, compresi gli eventi per ARC, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando si crea un percorso nella console, questo sarà valido in tutte le Regioni AWS. Il trail registra gli eventi di tutte le regioni della AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica della creazione di un percorso
- CloudTrail servizi e integrazioni supportati

- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di CloudTrail registro da più regioni e ricezione di file di CloudTrail registro da più account

Tutte le azioni ARC vengono registrate CloudTrail e sono documentate nella Recovery Readiness API Reference Guide per Amazon Application Recovery Controller, nella Recovery Control Configuration API Reference Guide per Amazon Application Recovery Controller e nella Routing Control API Recovery Guide per Amazon Application Recovery Controller. Ad esempio, le chiamate `UpdateRoutingControlState` e le `CreateRecoveryGroup` azioni generano voci nei file di registro. `CreateCluster` CloudTrail

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con credenziali utente root o AWS Identity and Access Management (IAM).
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro AWS servizio.

Per ulteriori informazioni, consulta Elemento CloudTrail userIdentity.

Visualizzazione degli eventi ARC nella cronologia degli eventi

CloudTrail consente di visualizzare gli eventi recenti nella cronologia degli eventi. Per visualizzare gli eventi per le richieste API ARC, devi scegliere US West (Oregon) nel selettore di regione nella parte superiore della console. Per ulteriori informazioni, consulta Lavorare con la cronologia CloudTrail degli eventi nella Guida per l'AWS CloudTrail utente.

Comprendere le voci dei file di registro ARC

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'`CreateCluster`azione per configurare il controllo del routing.


```
{
  "eventVersion": "1.08",
   "userIdentity": {
     "type": "IAMUser",
     "principalId": "A1B2C3D4E5F6G7EXAMPLE",
     "arn": "arn:aws:iam::111122223333:user/smithj",
     "accountId": "111122223333",
     "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
     "sessionContext": {
          "sessionIssuer": {
              "type": "Role",
              "principalId": "A1B2C3D4E5F6G7EXAMPLE",
              "arn": "arn:aws:iam::111122223333:role/smithj",
              "accountId": "111122223333",
              "userName": "smithj"
          },
          "webIdFederationData": {},
          "attributes": {
              "mfaAuthenticated": "false",
              "creationDate": "2021-06-30T04:44:41Z"
          }
      }
  },
  "eventTime": "2021-06-30T04:45:46Z",
  "eventSource": "route53-recovery-control-config.amazonaws.com",
  "eventName": "CreateCluster",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "192.0.2.50",
  "userAgent": "aws-cli/2.0.0 Python/3.8.2 Darwin/19.6.0 botocore/2.0.0dev7",
  "requestParameters": {
      "ClientToken": "12345abcdef-1234-5678-abcd-12345abcdef",
      "ClusterName": "XYZCluster"
  },
  "responseElements": {
      "Cluster": {
          "Arn": "arn:aws:route53-recovery-control::012345678901:cluster/abc123456-
aa11-bb22-cc33-abc123456",
          "ClusterArn": "arn:aws:route53-recovery-control::012345678901:cluster/
abc123456-aa11-bb22-cc33-abc123456",
          "Name": "XYZCluster",
```

```
          "Status": "PENDING"
      }
  },
  "requestID": "6090509a-5a97-4be6-8e6a-7d73example",
  "eventID": "9cab44ef-0777-41e6-838f-f249example",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "111122223333"
}
```

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'`UpdateRoutingControlState`azione per il controllo del routing.

```
{
  "eventVersion": "1.08",
   "userIdentity": {
     "type": "AssumedRole",
     "principalId": "A1B2C3D4E5F6G7EXAMPLE",
     "arn": "arn:aws:sts::111122223333:assumed-role/admin/smithj",
     "accountId": "111122223333",
     "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
     "sessionContext": {
          "sessionIssuer": {
              "type": "Role",
              "principalId": "A1B2C3D4E5F6G7EXAMPLE",
              "arn": "arn:aws:iam::111122223333:role/admin",
              "accountId": "111122223333",
              "userName": "admin"
          },
          "webIdFederationData": {},
          "attributes": {
              "mfaAuthenticated": "false",
              "creationDate": "2021-06-30T04:44:41Z"
          }
      }
  },
  "eventTime": "2021-06-30T04:45:46Z",
  "eventSource": "route53-recovery-control-config.amazonaws.com",
  "eventName": "UpdateRoutingControl",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "192.0.2.50",
```

```
  "userAgent": "aws-cli/2.0.0 Python/3.8.2 Darwin/19.6.0 botocore/2.0.0dev7",
  "requestParameters": {
      "RoutingControlName": "XYZRoutingControl3",
      "RoutingControlArn": "arn:aws:route53-recovery-
control::012345678:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567"
  },
  "responseElements": {
      "RoutingControl": {
          "ControlPanelArn": "arn:aws:route53-recovery-
control::012345678:controlpanel/0123456bbbbbbb0123456bbbbbb0123456",
          "Name": "XYZRoutingControl3",
          "Status": "DEPLOYED",
          "RoutingControlArn": "arn:aws:route53-recovery-
control::012345678:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567"
      }
  },
  "requestID": "6090509a-5a97-4be6-8e6a-7d73example",
  "eventID": "9cab44ef-0777-41e6-838f-f249example",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "111122223333"
}
```


Identity and Access Management per il controllo del routing in

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

Indice

- Come funziona il controllo del routing in Amazon Application Recovery Controller (ARC) con IAM
- Esempi di policy basate sull'identità per il controllo del routing in ARC
- AWS politiche gestite per il controllo del routing in Amazon Application Recovery Controller (ARC)

Come funziona il controllo del routing in Amazon Application Recovery Controller (ARC) con IAM

Prima di utilizzare IAM per gestire l'accesso al controllo del routing in Amazon Application Recovery Controller (ARC), scopri quali funzionalità IAM sono disponibili per il controllo del routing.

Funzionalità IAM che puoi utilizzare con il controllo del routing in Amazon Application Recovery Controller (ARC)

Funzionalità IAM	Supporto per il controllo del routing
Policy basate sull'identità	Sì
Policy basate su risorse	No
Operazioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione delle policy	Sì
ACLs	No
ABAC (tag nelle policy)	Parziale
Credenziali temporanee	Sì
Autorizzazioni del principale	Sì
Ruoli di servizio	No
Ruoli collegati al servizio	No

Per avere una panoramica generale di alto livello su come AWS i 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 ARC

Supporta le policy basate sull'identità: sì

Le policy basate sull'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 di IAM.

Con le policy basate sull'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. 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 IAM.

Per visualizzare esempi di politiche ARC basate sull'identità per il controllo del routing, vedere. Esempi di policy basate sull'identità per il controllo del routing in ARC

Politiche basate sulle risorse nell'ambito del controllo del routing

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 di 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.

Azioni politiche per il controllo del routing

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

Per visualizzare un elenco di azioni ARC per il controllo del routing, consulta Azioni definite da Amazon Route 53 Recovery Controls e Azioni definite da Amazon Route 53 Recovery Cluster nel Service Authorization Reference.

Le azioni politiche in ARC per il controllo del routing utilizzano i seguenti prefissi prima dell'azione, a seconda dell'API con cui stai lavorando:

```
route53-recovery-control-config
```

```
route53-recovery-cluster
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola. Ad esempio, è possibile eseguire le operazioni seguenti:

```
"Action": [
      "route53-recovery-control-config:action1",
      "route53-recovery-control-config:action2"
         ]
```

È possibile specificare più azioni tramite caratteri jolly (*). Ad esempio, per specificare tutte le azioni che iniziano con la parola `Describe`, includi la seguente azione:

```
"Action": "route53-recovery-control-config:Describe*"
```

Per visualizzare esempi di politiche basate sull'identità ARC per il controllo del routing, consulta. Esempi di policy basate sull'identità per il controllo del routing in ARC

Risorse politiche per ARC

Supporta le risorse relative alle policy: sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità 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. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). Per le azioni che non supportano le autorizzazioni a livello di risorsa, si utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

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

Nel Service Authorization Reference, è possibile visualizzare le seguenti informazioni relative ad ARC:

Per visualizzare un elenco dei tipi di risorse e delle relative ARNs azioni e le azioni che è possibile specificare con l'ARN di ciascuna risorsa, vedere i seguenti argomenti nel Service Authorization Reference:

- Azioni definite da Amazon Route 53 Recovery Controls

- Azioni definite da Amazon Route 53 Recovery Cluster.

Per visualizzare esempi di politiche ARC basate sull'identità per il controllo del routing, consulta. Esempi di policy basate sull'identità per il controllo del routing in ARC

Chiavi relative alle condizioni delle policy per ARC

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 entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento `Condition` specifica quando le istruzioni vengono eseguite in base a criteri definiti. 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. 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 ARC per il controllo del routing, consulta i seguenti argomenti nel Service Authorization Reference:

- Chiavi di condizione per Amazon Route 53 Recovery Controls
- Chiavi di condizione per Amazon Route 53 Recovery Cluster

Per visualizzare le azioni e le risorse che puoi utilizzare con una chiave di condizione, consulta i seguenti argomenti nel Service Authorization Reference:

- Per visualizzare un elenco dei tipi di risorse e relativi ARNs, consulta Azioni definite da Amazon Route 53 Recovery Controls e Azioni definite da Amazon Route 53 Recovery Cluster.
- Per visualizzare un elenco delle azioni che puoi specificare con l'ARN di ogni risorsa, consulta Risorse definite da Amazon Route 53 Recovery Controls e Resources defined by Amazon Route 53 Recovery Cluster.

Per visualizzare esempi di politiche basate sull'identità ARC per il controllo del routing, consulta Esempi di policy basate sull'identità per il controllo del routing in ARC

Liste di controllo degli accessi () in ARC ACLs

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.

Controllo degli accessi basato sugli attributi (ABAC) con ARC

Supporta ABAC (tag nelle policy): parzialmente

Il controllo degli accessi basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi, chiamati tag. Puoi allegare tag a entità e AWS risorse IAM, quindi progettare politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag sulla risorsa.

Per controllare l'accesso basato su tag, fornire 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 Sì. Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per maggiori informazioni su ABAC, consulta Definizione delle autorizzazioni con autorizzazione ABAC nella Guida per l'utente di 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.

Il controllo del routing ARC include il seguente supporto per ABAC:

- Recovery Control Config supporta ABAC.
- Recovery Cluster non supporta ABAC.

Utilizzo di credenziali temporanee con ARC

Supporta le credenziali temporanee: sì

Le credenziali temporanee forniscono un accesso a breve termine alle AWS risorse e vengono create automaticamente quando si utilizza la federazione o si cambia ruolo. AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza temporanee in IAM e Servizi AWS compatibili con IAM nella Guida per l'utente IAM.

Autorizzazioni principali multiservizio per ARC

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

Quando utilizzi un'entità IAM (utente o ruolo) per eseguire azioni AWS, sei considerato un principale. Le policy concedono autorizzazioni a un'entità. Quando si utilizzano alcuni servizi, è possibile eseguire un'azione che attiva un'altra azione in un servizio diverso. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni.

Per vedere se un'azione richiede azioni dipendenti aggiuntive in una policy, consulta i seguenti argomenti nel Service Authorization Reference:

- Cluster di ripristino Amazon Route 53
- Controlli di ripristino di Amazon Route 53

Ruoli di servizio per ARC

Supporta i ruoli di servizio: no

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 Create a role to delegate permissions to an Servizio AWS nella Guida per l'utente IAM.

Ruoli collegati ai servizi per ARC

Supporta ruoli collegati ai servizi:

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'operazione per tuo conto. I ruoli collegati al servizio vengono visualizzati nell' AWS account e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati al servizio, ma non modificarle.

Il controllo del routing non utilizza ruoli collegati al servizio.

Esempi di policy basate sull'identità per il controllo del routing in ARC

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare risorse ARC. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM.

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 di IAM.

Per dettagli sulle azioni e sui tipi di risorse definiti da ARC, incluso il formato di ARNs per ogni tipo di risorsa, consulta Azioni, risorse e chiavi di condizione per Amazon Application Recovery Controller (ARC) nel Service Authorization Reference.

Argomenti

- Best practice per le policy
- Esempio: accesso alla console ARC per il controllo del routing
- Esempi: azioni dell'API ARC per la configurazione del controllo del routing

Best practice per le policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare le risorse ARC nel tuo account. Queste azioni possono comportare costi aggiuntivi per l' Account AWS. Quando si creano o modificano policy basate sull'identità, seguire 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 maggiori informazioni, consulta Policy gestite da AWS o Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente di IAM.
- Applicazione delle autorizzazioni con privilegio minimo - Quando si impostano le autorizzazioni con le policy IAM, concedere 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 privilegio minimo. Per maggiori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso - Per limitare l'accesso ad azioni e risorse è possibile aggiungere una condizione alle 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 CloudFormation. Per

maggiori informazioni, consultare la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente di IAM.

- Utilizzo dello strumento di analisi degli accessi IAM per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali - Lo strumento di analisi degli accessi IAM convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio (JSON) della policy IAM e alle best practice di IAM. Lo strumento di analisi degli accessi IAM offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per maggiori informazioni, consultare Convalida delle policy per il Sistema di analisi degli accessi IAM nella Guida per l'utente di 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, aggiungere le condizioni MFA alle policy. Per maggiori informazioni, consultare Protezione dell'accesso API con MFA nella Guida per l'utente di IAM.

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

Esempio: accesso alla console ARC per il controllo del routing

Per accedere alla console Amazon Application Recovery Controller (ARC), devi disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle risorse ARC 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 agli utenti che effettuano chiamate solo verso AWS CLI o l' AWS API. Al contrario, è opportuno concedere l'accesso solo alle azioni che corrispondono all'operazione API che stanno cercando di eseguire.

Per garantire che utenti e ruoli possano ancora utilizzare la console ARC quando consenti l'accesso solo a operazioni API specifiche, allega anche una policy `ReadOnly` AWS gestita per ARC alle entità. Per ulteriori informazioni, consulta la pagina delle politiche gestite di ARC ARC o Aggiungere autorizzazioni a un utente nella Guida per l'utente IAM.

Per consentire agli utenti l'accesso completo all'utilizzo delle funzionalità di controllo del routing ARC tramite la console, allega all'utente una policy come la seguente, per concedere all'utente le autorizzazioni complete per configurare le risorse e le operazioni di controllo del routing ARC:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                   "route53-recovery-cluster:GetRoutingControlState",
                   "route53-recovery-cluster:UpdateRoutingControlState",
                   "route53-recovery-cluster:UpdateRoutingControlStates",
                   "route53-recovery-control-config:CreateCluster",
                   "route53-recovery-control-config:CreateControlPanel",
                   "route53-recovery-control-config:CreateRoutingControl",
                   "route53-recovery-control-config:CreateSafetyRule",
                   "route53-recovery-control-config:DeleteCluster",
                   "route53-recovery-control-config:DeleteControlPanel",
                   "route53-recovery-control-config:DeleteRoutingControl",
                   "route53-recovery-control-config:DeleteSafetyRule",
                   "route53-recovery-control-config:DescribeCluster",
                   "route53-recovery-control-config:DescribeControlPanel",
                   "route53-recovery-control-config:DescribeSafetyRule",
                   "route53-recovery-control-config:DescribeRoutingControl",
                   "route53-recovery-control-
config:ListAssociatedRoute53HealthChecks",
                   "route53-recovery-control-config:ListClusters",
                   "route53-recovery-control-config:ListControlPanels",
                   "route53-recovery-control-config:ListRoutingControls",
                   "route53-recovery-control-config:ListSafetyRules",
                   "route53-recovery-control-config:UpdateControlPanel",
                   "route53-recovery-control-config:UpdateRoutingControl",
                   "route53-recovery-control-config:UpdateSafetyRule"
             ],
            "Resource": "*"
        },
                {
            "Effect": "Allow",
            "Action": [
                   "route53:GetHealthCheck",
                   "route53:CreateHealthCheck",
                   "route53:DeleteHealthCheck",
                   "route53:ChangeTagsForResource"
            ],
```

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

Esempi: azioni dell'API ARC per la configurazione del controllo del routing

Per garantire che un utente possa utilizzare le azioni dell'API ARC per lavorare con la configurazione del controllo del routing ARC, allega una policy che corrisponda alle operazioni API con cui l'utente deve lavorare, come descritto di seguito.

Per utilizzare le operazioni API per la configurazione del controllo del ripristino, allega all'utente una policy come la seguente:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                   "route53-recovery-control-config:CreateCluster",
                   "route53-recovery-control-config:CreateControlPanel",
                   "route53-recovery-control-config:CreateRoutingControl",
                   "route53-recovery-control-config:CreateSafetyRule",
                   "route53-recovery-control-config:DeleteCluster",
                   "route53-recovery-control-config:DeleteControlPanel",
                   "route53-recovery-control-config:DeleteRoutingControl",
                   "route53-recovery-control-config:DeleteSafetyRule",
                   "route53-recovery-control-config:DescribeCluster",
                   "route53-recovery-control-config:DescribeControlPanel",
                   "route53-recovery-control-config:DescribeSafetyRule",
                   "route53-recovery-control-config:DescribeRoutingControl",
                   "route53-recovery-control-config:GetResourcePolicy",
                   "route53-recovery-control-
config:ListAssociatedRoute53HealthChecks",
                   "route53-recovery-control-config:ListClusters",
                   "route53-recovery-control-config:ListControlPanels",
                   "route53-recovery-control-config:ListRoutingControls",
                   "route53-recovery-control-config:ListSafetyRules",
```

```
                "route53-recovery-control-config:ListTagsForResource",
                "route53-recovery-control-config:UpdateControlPanel",
                "route53-recovery-control-config:UpdateRoutingControl",
                "route53-recovery-control-config:UpdateSafetyRule",
                "route53-recovery-control-config:TagResource",
                "route53-recovery-control-config:UntagResource"
            ],
            "Resource": "*"
        }
    ]
}
```

Per eseguire attività di controllo del routing ARC con l'API del piano dati del cluster di ripristino, ad esempio l'aggiornamento degli stati di controllo del routing per il failover durante un evento di emergenza, puoi allegare una policy ARC IAM come la seguente al tuo utente IAM.

Il valore `AllowSafetyRuleOverride` booleano consente di ignorare le regole di sicurezza che hai configurato come protezione per i controlli di routing. Questa autorizzazione potrebbe essere richiesta negli scenari «break glass» per aggirare le misure di protezione in caso di disastri o altri scenari di failover urgenti. Ad esempio, un operatore potrebbe aver bisogno di eseguire rapidamente il failover per il disaster recovery e una o più regole di sicurezza potrebbero impedire inaspettatamente l'aggiornamento dello stato di controllo del routing necessario per reindirizzare il traffico. Questa autorizzazione consente all'operatore di specificare le regole di sicurezza da ignorare quando si effettuano chiamate API per aggiornare gli stati di controllo del routing. Per ulteriori informazioni, consulta Sostituire le regole di sicurezza per reindirizzare il traffico.

Se desideri consentire a un operatore di utilizzare l'API del piano dati del cluster di ripristino ma evitare di ignorare le regole di sicurezza, puoi allegare una politica come la seguente, con `AllowSafetyRuleOverrides` boolean to. `false` Per consentire all'operatore di ignorare le regole di sicurezza, imposta il valore booleano su. `AllowSafetyRuleOverrides` `true`

JSON

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

```
                "route53-recovery-cluster:GetRoutingControlState",
                "route53-recovery-cluster:ListRoutingControls"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "route53-recovery-cluster:UpdateRoutingControlStates",
                "route53-recovery-cluster:UpdateRoutingControlState"
            ],
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "route53-recovery-cluster:AllowSafetyRulesOverrides": "false"
                }
            }
        }
    ]
}
```

AWS politiche gestite per il controllo del routing in Amazon Application Recovery Controller (ARC)

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 Si consiglia pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente specifiche per i propri 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, consultare Policy gestite da AWS nella Guida per l'utente di IAM.

AWS politica gestita: AmazonRoute 53 RecoveryControlConfigFullAccess

È possibile collegare `AmazonRoute53RecoveryControlConfigFullAccess` alle entità IAM. Questa politica garantisce l'accesso completo alle azioni per l'utilizzo della configurazione del controllo di ripristino in ARC. Collegala agli utenti IAM e ad altri responsabili che necessitano dell'accesso completo alle azioni di configurazione del controllo del ripristino.

A tua discrezione, puoi aggiungere l'accesso ad altre azioni di Amazon Route 53 per consentire agli utenti di creare controlli di integrità per i controlli di routing. Ad esempio, potresti concedere l'autorizzazione per una o più delle seguenti azioni:`route53:GetHealthCheck`, `route53:CreateHealthCheckroute53:DeleteHealthCheck`, `eroute53:ChangeTagsForResource`.

Per visualizzare le autorizzazioni per questa politica, vedere AmazonRoute53 RecoveryControlConfigFullAccess nel AWS Managed Policy Reference.

AWS politica gestita: 53 AmazonRoute RecoveryControlConfigReadOnlyAccess

È possibile collegare `AmazonRoute53RecoveryControlConfigReadOnlyAccess` alle entità IAM. È utile per gli utenti che devono visualizzare il controllo del routing e le configurazioni delle regole di sicurezza. Questa politica garantisce l'accesso in sola lettura alle azioni per l'utilizzo della configurazione del controllo di ripristino in ARC. Questi utenti non possono creare, aggiornare o eliminare risorse per il controllo del ripristino.

Per visualizzare le autorizzazioni per questa politica, vedere AmazonRoute53 RecoveryControlConfigReadOnlyAccess nel AWS Managed Policy Reference.

AWS politica gestita: 53 AmazonRoute RecoveryClusterFullAccess

È possibile collegare `AmazonRoute53RecoveryClusterFullAccess` alle entità IAM. Questa politica garantisce il pieno accesso alle azioni per lavorare con il piano dati del cluster in ARC. Collegala agli utenti IAM e ad altri responsabili che necessitano dell'accesso completo all'aggiornamento e al recupero degli stati di controllo del routing.

Per visualizzare le autorizzazioni per questa policy, vedi AmazonRoute53 RecoveryClusterFullAccess nel Managed Policy Reference.AWS

AWS politica gestita: 53 AmazonRoute RecoveryClusterReadOnlyAccess

È possibile collegare `AmazonRoute53RecoveryClusterReadOnlyAccess` alle entità IAM. Questa politica garantisce l'accesso in sola lettura al piano dati del cluster in ARC. Questi utenti possono recuperare gli stati di controllo del routing ma non possono aggiornarli.

Per visualizzare le autorizzazioni per questa politica, vedere AmazonRoute53 RecoveryClusterReadOnlyAccess nel AWS Managed Policy Reference.

AWS politica gestita: AmazonApplicationRecoveryControllerRegionSwitchPlanExecutionPolicy

È possibile collegare `AmazonApplicationRecoveryControllerRegionSwitchPlanExecutionPolicy` alle entità IAM. Questa politica concede le autorizzazioni per l'esecuzione e la valutazione del piano di commutazione della regione ARC. Collegala ai ruoli IAM utilizzati per l'esecuzione del piano di cambio di regione.

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `arc-region-switch:GetPlan`— Consente ai responsabili di recuperare i dettagli di configurazione per un piano di switch di regione.
- `arc-region-switch:GetPlanExecution`— Consente ai responsabili di recuperare informazioni sull'esecuzione di un piano di cambio di regione specifico.
- `arc-region-switch:ListPlanExecutions`— Consente ai responsabili di elencare tutte le esecuzioni dei piani di cambio di regione.
- `iam:SimulatePrincipalPolicy`— Consente ai responsabili di simulare e valutare le azioni che un ruolo IAM può eseguire. Questa autorizzazione è limitata solo ai ruoli IAM e viene utilizzata durante la valutazione del piano per verificare che siano disponibili le autorizzazioni necessarie prima di eseguire un piano di cambio di regione.
- `cloudwatch:DescribeAlarms`— Consente ai responsabili di recuperare informazioni sugli allarmi Amazon CloudWatch .
- `cloudwatch:DescribeAlarmHistory`— Consente ai responsabili di recuperare le modifiche storiche dello stato degli allarmi Amazon CloudWatch .
- `cloudwatch:GetMetricStatistics`— Consente ai mandanti di recuperare dati statistici per le metriche di Amazon CloudWatch .

Per visualizzare ulteriori dettagli sulla policy, inclusa la versione più recente del documento di policy JSON, consulta AmazonApplicationRecoveryControllerRegionSwitchPlanExecutionPolicy nella Guida di riferimento alle policy gestite da AWS .

Aggiornamenti per le politiche AWS gestite per il controllo del routing

Per dettagli sugli aggiornamenti alle politiche AWS gestite per il controllo del routing in ARC da quando questo servizio ha iniziato a tenere traccia di queste modifiche, vedere. Aggiornamenti alle politiche AWS gestite per Amazon Application Recovery Controller (ARC) Per avvisi automatici sulle modifiche a questa pagina, iscriviti al feed RSS nella pagina della cronologia dei documenti ARC.

Quote per il controllo del routing

Il controllo del routing in Amazon Application Recovery Controller (ARC) è soggetto alle seguenti quote (precedentemente denominate limiti).

Entità	Quota
Numero di cluster per account	2
Numero di pannelli di controllo per cluster	50
Numero di controlli di routing per pannello di controllo	100
Numero totale di controlli di routing (in tutti i pannelli di controllo) per cluster	300
Numero di regole di sicurezza per pannello di controllo	20
Numero di controlli di routing per chiamata UpdateRoutingControlStatesoperativa	10
Numero di chiamate API mutanti a un endpoint del cluster, al secondo	3

Controllo di prontezza in ARC

> **Note**
>
> La funzionalità di controllo della disponibilità in Amazon Application Recovery Controller (ARC) non sarà più aperta ai nuovi clienti a partire dal 30 aprile 2026. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta Amazon Application Recovery Controller (ARC) readiness check availability change.

Con il Readiness Check in Amazon Application Recovery Controller (ARC), puoi capire se le tue applicazioni e risorse sono pronte per il ripristino. Dopo aver modellato l' AWS applicazione in ARC e creato i controlli di fattibilità, i controlli monitorano continuamente le informazioni sull'applicazione, come quote di AWS risorse, capacità e politiche di routing di rete. È quindi possibile scegliere di ricevere notifiche sulle modifiche che potrebbero influire sulla capacità di eseguire il failover su una replica dell'applicazione e di eseguire il ripristino in seguito a un evento. I controlli di fattibilità aiutano a garantire, su base continuativa, la possibilità di mantenere le applicazioni multiregionali in uno stato scalabile e configurato per gestire il traffico di failover.

Questo capitolo spiega come modellare l'applicazione in ARC per configurare la struttura che consente il funzionamento dei controlli di fattibilità, creando un gruppo di ripristino e celle che descrivano l'applicazione. Quindi, è possibile seguire i passaggi per aggiungere controlli di fattibilità e ambiti di fattibilità in modo che ARC possa verificare la disponibilità dell'applicazione.

Dopo aver creato i controlli di preparazione, è possibile monitorare lo stato di preparazione delle risorse. I controlli di fattibilità consentono di garantire che la replica dell'applicazione in standby e le relative risorse corrispondano costantemente alla replica di produzione, in base alla capacità, alle politiche di routing e ad altri dettagli di configurazione dell'applicazione di produzione. Se la replica non corrisponde, è possibile aggiungere capacità o modificare una configurazione in modo da allineare nuovamente le repliche delle applicazioni.

> **Important**
>
> I controlli di fattibilità sono particolarmente utili per verificare, su base continuativa, che le configurazioni delle repliche delle applicazioni e gli stati di runtime siano allineati. I controlli di fattibilità non devono essere utilizzati per indicare se la replica di produzione è integra, né

è necessario affidarsi ai controlli di fattibilità come fattore principale per il failover durante un evento di emergenza.

Cos'è il controllo di disponibilità in Amazon Application Recovery Controller (ARC)?

> **Note**
>
> La funzionalità di controllo della disponibilità in Amazon Application Recovery Controller (ARC) non sarà più aperta ai nuovi clienti a partire dal 30 aprile 2026. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta Amazon Application Recovery Controller (ARC) readiness check availability change.

Un controllo di disponibilità in ARC verifica continuamente (a intervalli di un minuto) la presenza di discrepanze nella capacità AWS fornita, nelle quote di servizio, nei limiti di accelerazione e nelle discrepanze di configurazione e versione delle risorse incluse nel controllo. I controlli di fattibilità consentono di segnalare tali differenze in modo da garantire che ogni replica abbia la stessa configurazione di configurazione e lo stesso stato di runtime. Sebbene i controlli di fattibilità garantiscano che le capacità configurate tra le repliche siano coerenti, non dovresti aspettarti che siano loro a decidere per tuo conto quale deve essere la capacità della replica. Ad esempio, è necessario comprendere i requisiti dell'applicazione in modo da dimensionare i gruppi di Auto Scaling con una capacità di buffer sufficiente in ogni replica per gestire se un'altra cella non è disponibile.

Per quanto riguarda le quote, quando ARC rileva una mancata corrispondenza con un controllo di disponibilità, può adottare misure per allineare le quote per le repliche aumentando la quota inferiore in modo che corrisponda alla quota più alta. Quando le quote corrispondono, viene visualizzato lo stato del controllo di disponibilità. `READY` (Tieni presente che questo non è un processo di aggiornamento immediato e il tempo totale dipende dal tipo di risorsa specifico e da altri fattori.)

Il primo passaggio consiste nell'impostare i controlli di fattibilità per creare un gruppo di ripristino che rappresenti l'applicazione. Ogni gruppo di ripristino include celle per ogni singola unità di contenimento dei guasti o replica dell'applicazione. Successivamente, si creano set di risorse per ogni tipo di risorsa dell'applicazione e si associano i controlli di fattibilità ai set di risorse. Infine, si associano le risorse agli ambiti di preparazione, in modo da poter conoscere lo stato di preparazione

delle risorse in un gruppo di ripristino (l'applicazione) o nelle singole celle (repliche, che sono regioni o zone di disponibilità ()). AZs

La disponibilità (ovvero, `READY` o`NOT READY`) si basa sulle risorse che rientrano nell'ambito del controllo di preparazione e sul set di regole per un tipo di risorsa. Esistono set di regole di preparazione per ogni tipo di risorsa, che i controlli ARC utilizzano per verificare la disponibilità delle risorse. Il fatto che una risorsa lo sia `READY` o meno dipende da come viene definita ogni regola di preparazione. Tutte le regole di preparazione valutano le risorse, ma alcune confrontano le risorse tra loro e altre esaminano informazioni specifiche su ciascuna risorsa del set di risorse.

Aggiungendo i controlli di preparazione, è possibile monitorare lo stato di preparazione in diversi modi: con EventBridge, all'interno o utilizzando le Console di gestione AWS azioni dell'API ARC. È inoltre possibile monitorare lo stato di preparazione delle risorse in diversi contesti, tra cui la disponibilità delle celle e la disponibilità dell'applicazione. Utilizzate la funzionalità di autorizzazione tra account di ARC per semplificare la configurazione e il monitoraggio delle risorse distribuite da un singolo account. AWS

Monitoraggio delle repliche delle applicazioni con controlli di fattibilità

ARC verifica le repliche delle applicazioni utilizzando controlli di fattibilità per garantire che ognuna abbia la stessa configurazione di configurazione e lo stesso stato di runtime. Un controllo di fattibilità verifica continuamente la capacità AWS delle risorse, la configurazione, le AWS quote e le politiche di routing di un'applicazione, informazioni che è possibile utilizzare per garantire che le repliche siano pronte per il failover. I controlli di fattibilità aiutano a garantire che l'ambiente di ripristino sia scalabile e configurato per il failover quando necessario.

Le sezioni seguenti forniscono ulteriori dettagli su come funziona il controllo di prontezza.

Controlli di fattibilità e repliche delle applicazioni

Per prepararsi al ripristino, è necessario mantenere sempre una capacità di riserva sufficiente nelle repliche per assorbire il traffico di failover proveniente da un'altra zona o regione di disponibilità. ARC ispeziona continuamente (una volta al minuto) l'applicazione per garantire che la capacità assegnata corrisponda in tutte le zone o regioni di disponibilità.

La capacità ispezionata da ARC include, ad esempio, il numero di istanze di Amazon EC2, le unità di capacità di lettura e scrittura di Aurora e le dimensioni del volume Amazon EBS. Se si aumenta la capacità della replica principale in base ai valori delle risorse ma si dimentica di aumentare anche i valori corrispondenti nella replica in standby, ARC rileva la mancata corrispondenza in modo da poter aumentare i valori in standby.

> **Important**
>
> I controlli di fattibilità sono particolarmente utili per verificare, su base continuativa, che le configurazioni delle repliche delle applicazioni e gli stati di runtime siano allineati. I controlli di fattibilità non devono essere utilizzati per indicare se la replica di produzione è integra, né è necessario affidarsi ai controlli di fattibilità come fattore principale per il failover durante un evento di emergenza.

In una configurazione in standby attivo, è necessario decidere se ripartire da o verso una cella in base ai sistemi di monitoraggio e controllo dello stato e considerare i controlli di fattibilità come servizio complementare a tali sistemi. I controlli di prontezza ARC non sono altamente disponibili, quindi non si dovrebbe dipendere dall'accessibilità dei controlli durante un'interruzione. Inoltre, le risorse controllate potrebbero non essere disponibili durante un evento di emergenza.

È possibile monitorare lo stato di disponibilità delle risorse dell'applicazione in celle specifiche (AWS regioni o zone di disponibilità) o per l'intera applicazione. È possibile ricevere una notifica quando lo stato di un controllo di conformità cambia, ad esempio`Not ready`, creando regole in. EventBridge Per ulteriori informazioni, consulta Utilizzo del Readiness Check in ARC con Amazon EventBridge. È inoltre possibile visualizzare lo stato di preparazione in o utilizzando operazioni API, ad esempio. Console di gestione AWS`get-recovery-readiness` Per ulteriori informazioni, consulta Operazioni dell'API per il controllo della prontezza.

Come funziona il controllo di prontezza

ARC verifica le repliche delle applicazioni utilizzando controlli di fattibilità per garantire che ognuna abbia la stessa configurazione di configurazione e lo stesso stato di runtime.

Per prepararsi al ripristino, ad esempio, è necessario mantenere sempre una capacità di riserva sufficiente per assorbire il traffico di failover proveniente da un'altra zona o regione di disponibilità. ARC ispeziona continuamente (una volta al minuto) l'applicazione per garantire che la capacità assegnata corrisponda in tutte le zone o regioni di disponibilità. La capacità ispezionata da ARC include, ad esempio, il numero di istanze di Amazon EC2, le unità di capacità di lettura e scrittura di Aurora e le dimensioni del volume Amazon EBS. Se si aumenta la capacità della replica principale in base ai valori delle risorse ma si dimentica di aumentare anche i valori corrispondenti nella replica in standby, ARC rileva la mancata corrispondenza in modo da poter aumentare i valori in standby.

> **Important**
>
> I controlli di fattibilità sono particolarmente utili per verificare, su base continuativa, che le configurazioni delle repliche delle applicazioni e gli stati di runtime siano allineati. I controlli di fattibilità non devono essere utilizzati per indicare se la replica di produzione è integra, né è necessario affidarsi ai controlli di fattibilità come fattore principale per il failover durante un evento di emergenza.

In una configurazione in standby attivo, è necessario decidere se ripartire da o verso una cella in base ai sistemi di monitoraggio e controllo dello stato e considerare i controlli di fattibilità come servizio complementare a tali sistemi. I controlli di prontezza ARC non sono altamente disponibili, quindi non si dovrebbe dipendere dall'accessibilità dei controlli durante un'interruzione. Inoltre, le risorse controllate potrebbero non essere disponibili durante un evento di emergenza.

È possibile monitorare lo stato di disponibilità delle risorse dell'applicazione in celle specifiche (AWS regioni o zone di disponibilità) o per l'intera applicazione. È possibile ricevere una notifica quando lo stato di un controllo di conformità cambia, ad esempio`Not ready`, creando regole in. EventBridge Per ulteriori informazioni, consulta Utilizzo del Readiness Check in ARC con Amazon EventBridge. È inoltre possibile visualizzare lo stato di preparazione in o utilizzando operazioni API, ad esempio. Console di gestione AWS`get-recovery-readiness` Per ulteriori informazioni, consulta Operazioni dell'API per il controllo della prontezza.

In che modo le regole di preparazione determinano lo stato di preparazione

> **Note**
>
> La funzionalità di controllo della disponibilità in Amazon Application Recovery Controller (ARC) non sarà più aperta ai nuovi clienti a partire dal 30 aprile 2026. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta Amazon Application Recovery Controller (ARC) readiness check availability change.

I controlli di preparazione ARC determinano lo stato di preparazione in base alle regole predefinite per ogni tipo di risorsa e al modo in cui tali regole sono definite. ARC include un gruppo di regole per ogni tipo di risorsa che supporta. Ad esempio, ARC dispone di gruppi di regole di preparazione per i cluster Amazon Aurora, i gruppi di Auto Scaling e così via. Alcune regole di preparazione confrontano

tra loro le risorse di un set e altre esaminano informazioni specifiche su ciascuna risorsa del set di risorse.

Non è possibile aggiungere, modificare o rimuovere regole di preparazione o gruppi di regole. Tuttavia, puoi creare un CloudWatch allarme Amazon e creare un controllo di disponibilità per monitorare lo stato dell'allarme. Ad esempio, puoi creare un CloudWatch allarme personalizzato per monitorare i servizi container Amazon EKS e creare un controllo di disponibilità per verificare lo stato di disponibilità dell'allarme.

Puoi visualizzare tutte le regole di preparazione per ogni tipo di risorsa Console di gestione AWS quando crei un set di risorse oppure puoi visualizzare le regole di preparazione in un secondo momento accedendo alla pagina dei dettagli di un set di risorse. È inoltre possibile visualizzare le regole di preparazione nella sezione seguente:. Regole di preparazione in ARC

Quando un controllo di preparazione verifica un insieme di risorse con un insieme di regole, il modo in cui viene definita ciascuna regola determina se il risultato sarà `READY` o `NOT READY` per tutte le risorse o se il risultato sarà diverso per risorse diverse. Inoltre, è possibile visualizzare lo stato di preparazione in diversi modi. Ad esempio, è possibile visualizzare lo stato di preparazione di un gruppo di risorse in un set di risorse o visualizzare un riepilogo dello stato di preparazione per un gruppo di ripristino o una cella (ovvero una AWS regione o una zona di disponibilità, a seconda di come è stato impostato il gruppo di ripristino).

La formulazione contenuta nella descrizione di ogni regola spiega come vengono valutate le risorse per determinare lo stato di disponibilità quando viene applicata la regola. Viene definita una regola per ispezionare ogni risorsa o per ispezionare tutte le risorse di un set di risorse per determinarne la disponibilità. Nello specifico, le regole funzionano come segue:

- La regola controlla ogni risorsa del set di risorse per verificare una condizione.
  - Se tutte le risorse hanno esito positivo, tutte le risorse vengono impostate come`READY`.
  - Se una risorsa fallisce, quella risorsa viene impostata come `NOT READY` e le altre celle rimangono`READY`.

  Ad esempio: MskClusterState:ispeziona ogni cluster Amazon MSK per assicurarsi che sia in uno `ACTIVE` stato.
- La regola ispeziona tutte le risorse del set di risorse per verificare una condizione.
  - Se la condizione è garantita, tutte le risorse sono impostate come. `READY`
  - Se una di esse non soddisfa la condizione, tutte le risorse vengono impostate come`NOT READY`.

Ad esempio: VpcSubnetCount:ispeziona tutte le VPC sottoreti per assicurarsi che abbiano lo stesso numero di sottoreti.

- Regola non critica: la regola ispeziona tutte le risorse del set di risorse per verificare una condizione.
  - Se una di esse fallisce, lo stato di preparazione rimane invariato. Una regola con questo comportamento ha una nota nella descrizione.

  Ad esempio: ElbV2CheckAzCount:ispeziona ogni Network Load Balancer per assicurarsi che sia collegato a una sola zona di disponibilità. Nota: questa regola non influisce sullo stato di preparazione.

Inoltre, ARC compie un ulteriore passo avanti per quanto riguarda le quote. Se un controllo di conformità rileva una mancata corrispondenza tra le celle per quanto riguarda le quote di servizio (il valore massimo per la creazione e le operazioni delle risorse) per qualsiasi risorsa supportata, ARC aumenta automaticamente la quota per la risorsa con la quota inferiore. Questo vale solo per le quote (limiti). Per quanto riguarda la capacità, è necessario aggiungere capacità aggiuntiva in base alle esigenze dell'applicazione.

Puoi anche impostare una EventBridge notifica Amazon per i controlli di disponibilità, ad esempio, quando lo stato di un controllo di disponibilità cambia in. `NOT READY` Quindi, quando viene rilevata una mancata corrispondenza della configurazione, ti EventBridge invia una notifica e puoi intraprendere azioni correttive per assicurarti che le repliche delle applicazioni siano allineate e preparate per il ripristino. Per ulteriori informazioni, consulta Utilizzo del Readiness Check in ARC con Amazon EventBridge.

Come interagiscono i controlli di prontezza, i set di risorse e gli ambiti di preparazione

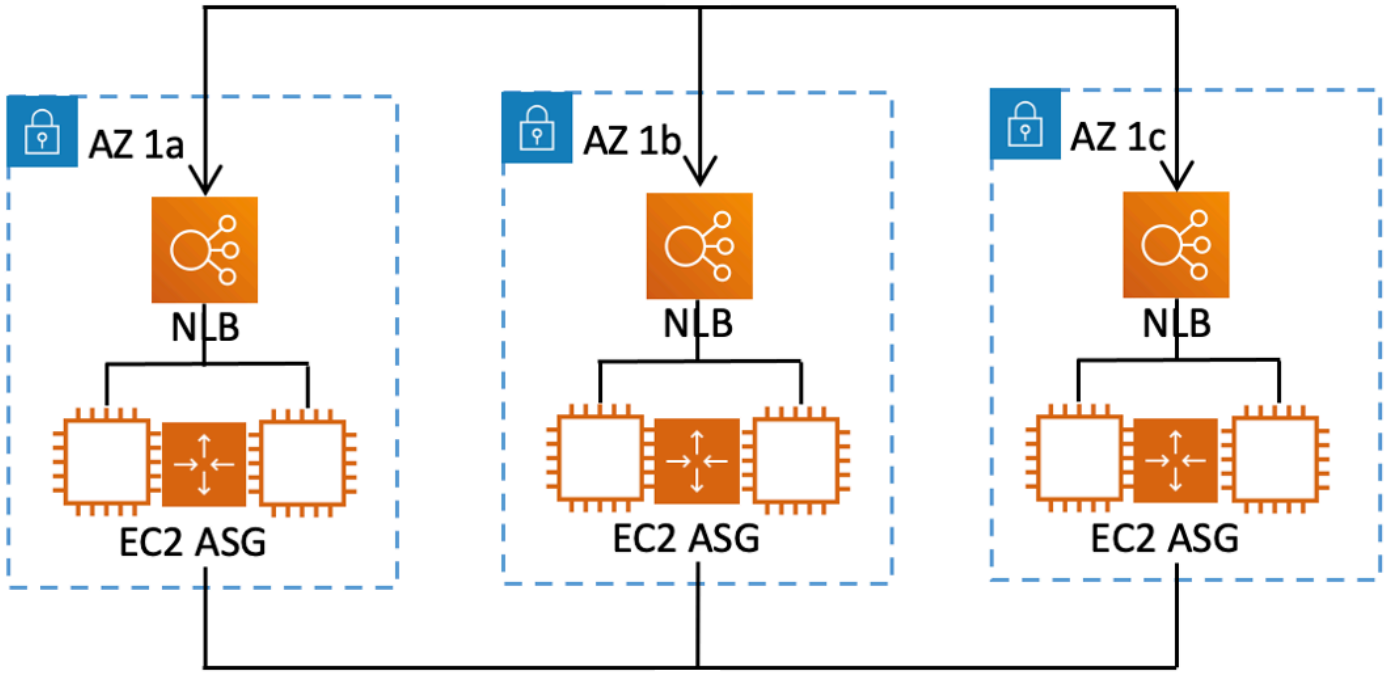
> **Note**
>
> La funzionalità di controllo della disponibilità in Amazon Application Recovery Controller (ARC) non sarà più aperta ai nuovi clienti a partire dal 30 aprile 2026. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta Amazon Application Recovery Controller (ARC) readiness check availability change.

I controlli di fattibilità controllano sempre i gruppi di risorse nei set di risorse. È possibile creare set di risorse (separatamente o durante la creazione di un controllo di disponibilità) per raggruppare le

risorse presenti nelle celle (zone di disponibilità o AWS regioni) del gruppo di ripristino ARC, in modo da poter definire i controlli di preparazione. Un set di risorse è in genere un gruppo dello stesso tipo di risorse (come Network Load Balancer), ma può anche essere costituito da risorse di destinazione DNS, per i controlli di fattibilità dell'architettura.

In genere si crea un set di risorse e si verifica la disponibilità per ogni tipo di risorsa dell'applicazione. Per verificare la fattibilità dell'architettura, si creano una risorsa di destinazione DNS di primo livello e un set di risorse globale (a livello di gruppo di ripristino), quindi si creano risorse di destinazione DNS a livello di cella per un set di risorse separato.

Il diagramma seguente mostra un esempio di gruppo di ripristino con tre celle (Availability Zones), ognuna con un Network Load Balancer (NLB) e un gruppo Auto Scaling (ASG).



In questo scenario, si creerebbe un set di risorse e un controllo di fattibilità per i tre Network Load Balancer e un set di risorse e un controllo di fattibilità per i tre gruppi di Auto Scaling. Ora è disponibile un controllo di disponibilità per ogni set di risorse per il gruppo di ripristino, per tipo di risorsa.

Creando ambiti di preparazione per le risorse, è possibile aggiungere riepiloghi dei controlli di preparazione per celle o gruppi di ripristino. Per specificare un ambito di disponibilità per una risorsa, si associa l'ARN della cella o del gruppo di ripristino a ciascuna risorsa in un set di risorse. È possibile eseguire questa operazione quando si crea un controllo di disponibilità per un set di risorse.

Ad esempio, quando si aggiunge un controllo di fattibilità per un set di risorse per i Network Load Balancer per questo gruppo di ripristino, è possibile aggiungere contemporaneamente ambiti di preparazione a ciascun NLB. In questo caso, si assocerebbe l'ARN di AZ 1a al NLB in AZ 1a, l'ARN di al NLB e l'ARN `AZ 1b` del NLB in. `AZ 1b` `AZ 1c` `AZ 1c` Quando si crea un controllo di fattibilità per i gruppi Auto Scaling, si fa lo stesso, assegnando ambiti di preparazione a ciascuno di essi quando si crea il controllo di fattibilità per il set di risorse del gruppo Auto Scaling.

È facoltativo associare gli ambiti di prontezza quando si crea un controllo di prontezza, tuttavia si consiglia vivamente di impostarli. Gli ambiti di fattibilità consentono ad ARC di mostrare lo stato corretto `READY` o di prontezza per i controlli riepilogativi di `NOT READY` prontezza dei gruppi di ripristino e i controlli di riepilogo di prontezza a livello di cella. A meno che non si impostino gli ambiti di preparazione, ARC non può fornire questi riepiloghi.

Tieni presente che quando aggiungi una risorsa a livello di applicazione o globale, ad esempio una politica di routing DNS, non scegli un gruppo o una cella di ripristino per l'ambito di preparazione. Invece, scegli una risorsa globale (nessuna cella).

Controlli di idoneità delle risorse di destinazione DNS: verifica della disponibilità della resilienza

> **Note**
>
> La funzionalità di controllo della disponibilità in Amazon Application Recovery Controller (ARC) non sarà più aperta ai nuovi clienti a partire dal 30 aprile 2026. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta Amazon Application Recovery Controller (ARC) readiness check availability change.

Con i controlli di idoneità delle risorse di destinazione DNS in ARC, puoi verificare la disponibilità dell'architettura e della resilienza della tua applicazione. Questo tipo di controllo di conformità analizza continuamente l'architettura dell'applicazione e le politiche di routing di Amazon Route 53 per verificare le dipendenze tra zone e regioni.

Un'applicazione orientata al ripristino dispone di più repliche suddivise in zone o AWS regioni di disponibilità, in modo che le repliche possano fallire indipendentemente l'una dall'altra. Se l'applicazione deve essere adattata per essere inserita correttamente in silos, ARC suggerirà le modifiche da apportare, se necessario, per aggiornare l'architettura per garantire che sia resiliente e pronta per il failover.

ARC rileva automaticamente il numero e l'ambito delle celle (che rappresentano repliche o unità di contenimento dei guasti) nell'applicazione e se le celle sono suddivise in silos per zona di disponibilità o per regione. Quindi, ARC identifica e fornisce informazioni sulle risorse dell'applicazione nelle celle, per determinare se sono correttamente suddivise in silos in zone o regioni. Ad esempio, se le celle sono limitate a zone specifiche, i controlli di fattibilità consentono di verificare se anche i sistemi di bilanciamento del carico e i relativi obiettivi si trovano in silos in tali zone.

Con queste informazioni, è possibile determinare se è necessario apportare modifiche per allineare le risorse nelle celle alle zone o alle regioni corrette.

Per iniziare, create risorse DNS target per la vostra applicazione, oltre a set di risorse e controlli di fattibilità per esse. Per ulteriori informazioni, consulta Ottenere consigli sull'architettura in ARC.

Controlli di fattibilità e scenari di disaster recovery

> **Note**
>
> La funzionalità di controllo della disponibilità in Amazon Application Recovery Controller (ARC) non sarà più aperta ai nuovi clienti a partire dal 30 aprile 2026. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta Amazon Application Recovery Controller (ARC) readiness check availability change.

I controlli di fattibilità ARC ti consentono di capire se le tue applicazioni e risorse sono pronte per il ripristino, aiutandoti a garantire che le tue applicazioni siano scalabili per gestire il traffico di failover. Gli stati del controllo di fattibilità non devono essere utilizzati come segnale per indicare che una replica di produzione è integra. Tuttavia, è possibile utilizzare i controlli di fattibilità come complemento al monitoraggio delle applicazioni e dell'infrastruttura o ai sistemi di controllo dello stato di integrità per determinare se eseguire o meno un errore da una replica.

In una situazione urgente o in caso di interruzione, utilizzate una combinazione di controlli di integrità e altre informazioni per verificare che il sistema di standby sia ottimizzato, funzionante e pronto per il failover del traffico di produzione. Ad esempio, controllate se i canarini che funzionano contro la vostra cella di standby soddisfano i criteri di successo, oltre a verificare che lo stato del controllo di prontezza per la cella di standby sia corretto. `READY`

Tieni presente che i controlli di idoneità ARC si svolgono in un'unica AWS regione, Stati Uniti occidentali (Oregon), e durante un'interruzione o un disastro, le informazioni sui controlli di prontezza

potrebbero diventare obsolete o i controlli potrebbero non essere disponibili. Per ulteriori informazioni, consulta Piani di controllo e dati per il controllo del routing.

AWS Disponibilità regionale per il controllo di idoneità

> **Note**
>
> La funzionalità di controllo della disponibilità in Amazon Application Recovery Controller (ARC) non sarà più aperta ai nuovi clienti a partire dal 30 aprile 2026. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta Amazon Application Recovery Controller (ARC) readiness check availability change.

Per informazioni dettagliate sul supporto regionale e sugli endpoint di servizio per Amazon Application Recovery Controller (ARC), consulta gli endpoint e le quote di Amazon Application Recovery Controller (ARC) nel riferimento generale di Amazon Web Services.

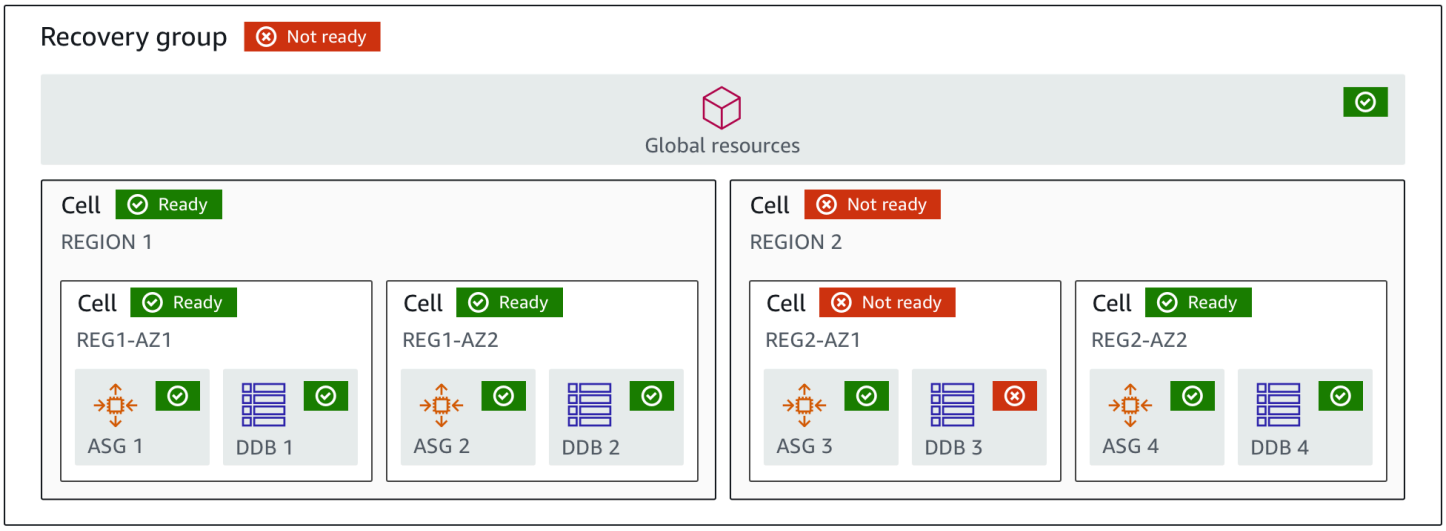
> **Note**
>
> Il controllo di conformità in Amazon Application Recovery Controller (ARC) è una funzionalità globale. Tuttavia, le risorse per il controllo di fattibilità si trovano nella regione Stati Uniti occidentali (Oregon), quindi è necessario specificare la regione Stati Uniti occidentali (Oregon) (specificare il parametro`--region us-west-2`) nei AWS CLI comandi ARC regionali, ad esempio, quando si creano risorse come set di risorse e controlli di fattibilità.

Componenti per il controllo di fattibilità

> **Note**
>
> La funzionalità di controllo della disponibilità in Amazon Application Recovery Controller (ARC) non sarà più aperta ai nuovi clienti a partire dal 30 aprile 2026. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta Amazon Application Recovery Controller (ARC) readiness check availability change.

Il diagramma seguente illustra un esempio di gruppo di ripristino configurato per supportare la funzionalità di controllo della disponibilità. Le risorse in questo esempio sono raggruppate in celle

(per Regione AWS) e celle nidificate (per zone di disponibilità) in un gruppo di ripristino. Esiste uno stato di disponibilità generale per il gruppo di ripristino (applicazione), nonché stati di disponibilità individuali per ogni cella (Regione) e cella nidificata (Zona di disponibilità).



Di seguito sono riportati i componenti della funzionalità di controllo della fattibilità di ARC.

Cella

Una cella definisce le repliche dell'applicazione o le unità di failover indipendenti. Raggruppa tutte le AWS risorse necessarie per l'esecuzione indipendente dell'applicazione all'interno della replica. Ad esempio, è possibile disporre di un set di risorse in una cella principale e un altro set in una cella di standby. Siete voi a determinare il limite di ciò che include una cella, ma in genere le celle rappresentano una zona di disponibilità o una regione. È possibile avere più celle (celle nidificate) all'interno di una cella, ad esempio AZs all'interno di una regione. Ogni cella nidificata rappresenta un'unità isolata di failover.

Gruppo di ripristino

Le cellule vengono raccolte in un gruppo di recupero. Un gruppo di ripristino rappresenta un'applicazione o un gruppo di applicazioni per cui si desidera verificare la preparazione al failover. È costituito da due o più celle, o repliche, che corrispondono tra loro in termini di funzionalità. Ad esempio, se si dispone di un'applicazione Web replicata su us-east-1a e us-east-1b, dove us-east-1b è l'ambiente di failover, è possibile rappresentare questa applicazione in ARC come gruppo di ripristino con due celle: una in us-east-1a e una in us-east-1b. Un gruppo di ripristino può anche includere una risorsa globale, ad esempio un controllo dello stato della Route 53.

Risorse e identificatori di risorse

Quando crei componenti per i controlli di fattibilità in ARC, specifichi una risorsa, come una tabella Amazon DynamoDB, un Network Load Balancer o una risorsa di destinazione DNS, utilizzando un identificatore di risorsa. Un identificatore di risorsa è l'Amazon Resource Name (ARN) della risorsa o, per una risorsa di destinazione DNS, l'identificatore che ARC genera quando crea la risorsa.

Risorsa di destinazione DNS

Una risorsa di destinazione DNS è la combinazione del nome di dominio dell'applicazione e di altre informazioni DNS, ad esempio la AWS risorsa a cui punta il dominio. L'inclusione di una AWS risorsa è facoltativa, ma se la fornisci, deve essere un record di risorse Route 53 o un Network Load Balancer. Quando fornisci la AWS risorsa, puoi ottenere consigli architetturali più dettagliati che possono aiutarti a migliorare la resilienza di ripristino dell'applicazione. È possibile creare set di risorse in ARC per le risorse di destinazione DNS e quindi creare un controllo di conformità per il set di risorse in modo da ottenere consigli sull'architettura per l'applicazione. Il controllo di conformità monitora anche la politica di routing DNS per l'applicazione, in base alle regole di fattibilità per le risorse di destinazione DNS.

Set di risorse

Un set di risorse è un insieme di risorse, incluse risorse o AWS risorse di destinazione DNS, che si estendono su più celle. Ad esempio, potresti avere un load balancer in us-east-1a e un altro in us-east-1b. Per monitorare la preparazione al ripristino dei sistemi di bilanciamento del carico, è possibile creare un set di risorse che includa entrambi i sistemi di bilanciamento del carico e quindi creare un controllo di fattibilità per il set di risorse. ARC verificherà continuamente la disponibilità delle risorse del set. È inoltre possibile aggiungere un ambito di disponibilità per associare le risorse di un set di risorse al gruppo di ripristino creato per l'applicazione.

Regola di prontezza

Le regole di preparazione sono controlli eseguiti da ARC su un insieme di risorse in un set di risorse. ARC dispone di una serie di regole di preparazione per ogni tipo di risorsa per cui supporta i controlli di disponibilità. Ogni regola include un ID e una descrizione che spiega per cosa ARC ispeziona le risorse.

Controllo di prontezza

Un controllo di fattibilità monitora un set di risorse nell'applicazione, ad esempio un set di istanze Amazon Aurora, per cui ARC sta verificando la preparazione al ripristino. I controlli di fattibilità possono includere il controllo, ad esempio, delle configurazioni di capacità, delle quote o delle

politiche di routing. AWS Ad esempio, se desideri verificare lo stato di preparazione dei tuoi gruppi Amazon EC2 Auto Scaling in due zone di disponibilità, puoi creare un controllo di disponibilità per un set di risorse con due ARNs risorse, una per ogni gruppo di Auto Scaling. Quindi, per assicurarsi che ogni gruppo sia scalato allo stesso modo, ARC monitora continuamente i tipi di istanze e i conteggi nei due gruppi.

Ambito di prontezza

Un ambito di preparazione identifica il raggruppamento di risorse compreso in uno specifico controllo di prontezza. L'ambito di un controllo di fattibilità può essere un gruppo di ripristino (ovvero globale per l'intera applicazione) o una cella (ovvero una regione o una zona di disponibilità). Per una risorsa che è una risorsa globale per ARC, imposta l'ambito di disponibilità a livello di gruppo di ripristino o risorsa globale. Ad esempio, un controllo dello stato di Route 53 è una risorsa globale in ARC perché non è specifico per una regione o una zona di disponibilità.

Piani di dati e controllo per il controllo di prontezza

> **Note**
>
> La funzionalità di controllo della disponibilità in Amazon Application Recovery Controller (ARC) non sarà più aperta ai nuovi clienti a partire dal 30 aprile 2026. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta Amazon Application Recovery Controller (ARC) readiness check availability change.

Quando pianifichi il failover e il disaster recovery, considera la resilienza dei tuoi meccanismi di failover. Ti consigliamo di assicurarti che i meccanismi da cui dipendi durante il failover siano altamente disponibili, in modo da poterli utilizzare quando ne hai bisogno in uno scenario di emergenza. In genere, è consigliabile utilizzare le funzioni del piano dati per i meccanismi ogni volta che è possibile, per la massima affidabilità e tolleranza ai guasti. In quest'ottica, è importante capire in che modo la funzionalità di un servizio è suddivisa tra piani di controllo e piani dati e quando è possibile contare su un'aspettativa di estrema affidabilità con il piano dati di un servizio.

Come per la maggior parte dei AWS servizi, la funzionalità di verifica della fattibilità è supportata da piani di controllo e piani dati. Sebbene entrambi siano progettati per essere affidabili, un piano di controllo è ottimizzato per la coerenza dei dati, mentre un piano dati è ottimizzato per la disponibilità. Un piano dati è progettato per la resilienza in modo da poter mantenere la disponibilità anche durante eventi di interruzione, quando un piano di controllo potrebbe non essere disponibile.

In generale, un piano di controllo consente di eseguire funzioni di gestione di base, come creare, aggiornare ed eliminare risorse nel servizio. Un piano dati fornisce le funzionalità principali di un servizio.

Per il controllo della fattibilità, esiste un'unica API, l'API Recovery Readiness, sia per il piano di controllo che per il piano dati. I controlli di prontezza e le risorse di preparazione sono disponibili solo nella regione degli Stati Uniti occidentali (Oregon) (us-west-2). Il piano di controllo per il controllo della prontezza e il piano dati sono affidabili ma non altamente disponibili.

Per ulteriori informazioni sui piani dati, sui piani di controllo e su come AWS crea servizi per soddisfare gli obiettivi di alta disponibilità, consulta il paper Static stability using Availability Zones in Amazon Builders' Library.

Etichettatura per il controllo di disponibilità in Amazon Application Recovery Controller (ARC)

> **Note**
>
> La funzionalità di controllo della disponibilità in Amazon Application Recovery Controller (ARC) non sarà più aperta ai nuovi clienti a partire dal 30 aprile 2026. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta Amazon Application Recovery Controller (ARC) readiness check availability change.

I tag sono parole o frasi (metadati) che usi per identificare e organizzare le tue AWS risorse. È possibile aggiungere più tag a ogni risorsa e ogni tag include una chiave e un valore che definisci. Ad esempio, la chiave potrebbe essere l'ambiente e il valore potrebbe essere la produzione. Puoi cercare e filtrare le tue risorse in base ai tag che aggiungi.

Puoi taggare le seguenti risorse in Readiness Check in ARC:

- Set di risorse
- Controlli di prontezza

L'etichettatura in ARC è disponibile solo tramite l'API, ad esempio utilizzando il. AWS CLI

Di seguito sono riportati alcuni esempi di verifica della disponibilità dei tag utilizzando. AWS CLI

```
aws route53-recovery-readiness --region us-west-2 create-resource-
set --resource-set-name dynamodb_resource_set --resource-set-type
AWS::DynamoDB::Table --resources ReadinessScopes=arn:aws:aws-recovery-
readiness::111122223333:cell/PDXCell,ResourceArn=arn:aws:dynamodb:us-
west-2:111122223333:table/PDX_Table ReadinessScopes=arn:aws:aws-recovery-
readiness::111122223333:cell/IADCell,ResourceArn=arn:aws:dynamodb:us-
east-1:111122223333:table/IAD_Table --tags Stage=Prod

aws route53-recovery-readiness --region us-west-2 create-readiness-
check --readiness-check-name dynamodb_readiness_check --resource-set-name
dynamodb_resource_set --tags Stage=Prod
```

Per ulteriori informazioni, consulta TagResourcela Recovery Readiness API Readiness Reference Guide per Amazon Application Recovery Controller (ARC).

Prezzi per Readiness Check in ARC

> **Note**
>
> La funzionalità di controllo della disponibilità in Amazon Application Recovery Controller (ARC) non sarà più aperta ai nuovi clienti a partire dal 30 aprile 2026. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta Amazon Application Recovery Controller (ARC) readiness check availability change.

Paghi un costo orario per ogni verifica di disponibilità effettuata.

Per informazioni dettagliate sui prezzi di ARC ed esempi di prezzi, consulta ARC Pricing.

Imposta un processo di ripristino resiliente per la tua applicazione

Per utilizzare Amazon Application Recovery Controller (ARC) con AWS applicazioni che si trovano in più AWS regioni, ci sono linee guida da seguire per configurare le applicazioni per la resilienza, in modo da poter supportare efficacemente la preparazione al ripristino. Quindi, puoi creare controlli di fattibilità per la tua applicazione e configurare controlli di routing per reindirizzare il traffico per il failover. È inoltre possibile consultare i consigli forniti da ARC sull'architettura dell'applicazione in grado di migliorare la resilienza.

> **Note**
>
> Se disponi di un'applicazione isolata per zone di disponibilità, valuta la possibilità di utilizzare lo spostamento zonale o lo spostamento automatico di zona per il ripristino in caso di failover. Non è necessaria alcuna configurazione per utilizzare lo spostamento zonale o lo spostamento automatico di zona per ripristinare in modo affidabile le applicazioni in caso di problemi relativi alla zona di disponibilità.
> Per allontanare il traffico da una zona di disponibilità per le risorse del load balancer, avvia uno spostamento di zona nella console ARC o nella console Elastic Load Balancing. In alternativa, puoi utilizzare l' AWS SDK AWS Command Line Interface o con azioni API di spostamento zonale. Per ulteriori informazioni, consulta Zonal shift in ARC.

Per ulteriori informazioni su come iniziare a utilizzare configurazioni di failover resilienti, consulta. Guida introduttiva al ripristino multiregionale in Amazon Application Recovery Controller (ARC)

Le migliori pratiche per il controllo di idoneità in ARC

> **Note**
>
> La funzionalità di controllo della disponibilità in Amazon Application Recovery Controller (ARC) non sarà più aperta ai nuovi clienti a partire dal 30 aprile 2026. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta Amazon Application Recovery Controller (ARC) readiness check availability change.

Consigliamo le seguenti best practice per il controllo di idoneità in Amazon Application Recovery Controller (ARC).

Aggiungi notifiche per le modifiche allo stato di preparazione

Imposta una regola in Amazon EventBridge per inviare una notifica ogni volta che lo stato di un controllo di disponibilità cambia, ad esempio da `READY` a`NOT READY`. Quando ricevi una notifica, puoi indagare e risolvere il problema, per assicurarti che l'applicazione e le risorse siano pronte per il failover quando previsto.

È possibile impostare EventBridge regole per inviare notifiche per diverse modifiche allo stato del controllo di prontezza, ad esempio per il gruppo di ripristino (per l'applicazione), per una cella (ad esempio una AWS regione) o per un controllo di disponibilità per un set di risorse.

Per ulteriori informazioni, consulta Utilizzo del Readiness Check in ARC con Amazon EventBridge.

Operazioni dell'API per il controllo della prontezza

> **Note**
>
> La funzionalità di controllo della disponibilità in Amazon Application Recovery Controller (ARC) non sarà più aperta ai nuovi clienti a partire dal 30 aprile 2026. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta Amazon Application Recovery Controller (ARC) readiness check availability change.

La tabella seguente elenca le operazioni ARC che puoi utilizzare per la preparazione al ripristino (controllo di preparazione), con collegamenti alla documentazione pertinente.

Per esempi di come utilizzare le comuni operazioni dell'API di preparazione al ripristino con, vedere. AWS Command Line InterfaceEsempi di utilizzo delle operazioni dell'API ARC Readiness Check con AWS CLI

Azione	Utilizzo della console ARC	Utilizzando l'API ARC
Crea una cella	Consulta Creazione, aggiornamento ed eliminazione di gruppi di ripristino in ARC.	Consulta la sezione CreateCell
Procurati una cella	Consulta Creazione, aggiornamento ed eliminazione di gruppi di ripristino in ARC.	Consulta la sezione GetCell
Eliminare una cella	Consulta Creazione, aggiornamento ed eliminazione di gruppi di ripristino in ARC.	Consulta la sezione DeleteCell
Aggiornare una cella	N/D	Per informazioni, consultare UpdateCell.

Azione	Utilizzo della console ARC	Utilizzando l'API ARC
Elenca le celle di un account	Consulta Creazione, aggiornamento ed eliminazione di gruppi di ripristino in ARC.	Consulta la sezione ListCells
Crea un gruppo di ripristino	Consulta Creazione, aggiornamento ed eliminazione di gruppi di ripristino in ARC.	Consulta la sezione CreateRecoveryGroup
Crea un gruppo di ripristino	Consulta Creazione, aggiornamento ed eliminazione di gruppi di ripristino in ARC.	Consulta la sezione GetRecoveryGroup
Aggiorna un gruppo di ripristino	Consulta Creazione, aggiornamento ed eliminazione di gruppi di ripristino in ARC.	Consulta la sezione UpdateRecoveryGroup
Eliminare un gruppo di ripristino	Consulta Creazione, aggiornamento ed eliminazione di gruppi di ripristino in ARC.	Consulta la sezione DeleteRecoveryGroup
Elenca i gruppi di ripristino	Consulta Creazione, aggiornamento ed eliminazione di gruppi di ripristino in ARC.	Consulta la sezione ListRecoveryGroups
Crea un set di risorse	Consulta Creazione e aggiornamento dei controlli di idoneità in ARC.	Consulta la sezione CreateResourceSet

Azione	Utilizzo della console ARC	Utilizzando l'API ARC
Ottieni un set di risorse	Consulta Creazione e aggiornamento dei controlli di idoneità in ARC.	Consulta la sezione GetResourceSet
Aggiorna un set di risorse	Consulta Creazione e aggiornamento dei controlli di idoneità in ARC.	Consulta la sezione UpdateResourceSet
Eliminare un set di risorse	Consulta Creazione e aggiornamento dei controlli di idoneità in ARC.	Consulta la sezione DeleteResourceSet
Elenca i set di risorse	Consulta Creazione e aggiornamento dei controlli di idoneità in ARC.	Consulta la sezione ListResourceSets
Crea un controllo di prontezza	Consulta Creazione e aggiornamento dei controlli di idoneità in ARC.	Consulta la sezione CreateReadinessCheck
Richiedi un controllo di disponibilità	Consulta Creazione e aggiornamento dei controlli di idoneità in ARC.	Consulta la sezione GetReadinessCheck
Aggiorna un controllo di disponibilità	Consulta Creazione e aggiornamento dei controlli di idoneità in ARC.	Consulta la sezione UpdateReadinessCheck
Eliminare un controllo di disponibilità	Consulta Creazione e aggiornamento dei controlli di idoneità in ARC.	Consulta la sezione DeleteReadinessCheck
Elenca i controlli di prontezza	Consulta Creazione e aggiornamento dei controlli di idoneità in ARC.	Consulta la sezione ListReadinessChecks

Azione	Utilizzo della console ARC	Utilizzando l'API ARC
Elenca le regole di preparazione	Consulta Descrizioni delle regole di preparazione in ARC.	Consulta la sezione ListRules
Verifica lo stato di un intero controllo di prontezza	Consulta Monitoraggio dello stato di preparazione in ARC.	Consulta la sezione GetReadinessCheckStatus
Verifica lo stato di una risorsa	Consulta Monitoraggio dello stato di preparazione in ARC.	Consulta la sezione GetReadinessCheckResourceStatus
Controlla lo stato di una cella	Consulta Monitoraggio dello stato di preparazione in ARC.	Consulta la sezione GetCellReadinessSummary
Controlla lo stato di un gruppo di ripristino	Consulta Monitoraggio dello stato di preparazione in ARC.	Consulta la sezione GetRecoveryGroupReadinessSummary

Esempi di utilizzo delle operazioni dell'API ARC Readiness Check con AWS CLI

> **Note**
>
> La funzionalità di controllo della disponibilità in Amazon Application Recovery Controller (ARC) non sarà più aperta ai nuovi clienti a partire dal 30 aprile 2026. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta Amazon Application Recovery Controller (ARC) readiness check availability change.

Questa sezione illustra semplici esempi di applicazioni, utilizzando le funzionalità AWS Command Line Interface di verifica della fattibilità di Amazon Application Recovery Controller (ARC) utilizzando le operazioni API. Gli esempi hanno lo scopo di aiutarvi a sviluppare una comprensione di base su come utilizzare le funzionalità di controllo della prontezza utilizzando la CLI.

Il controllo di fattibilità in ARC verifica la presenza di mancate corrispondenze tra le risorse nelle repliche delle applicazioni. Per impostare i controlli di fattibilità per l'applicazione, è necessario

configurare, o modellare, le risorse dell'applicazione in celle ARC allineate alle repliche create per l'applicazione. Quindi impostate controlli di fattibilità per controllare queste repliche, per assicurarvi che la replica dell'applicazione in standby e le relative risorse corrispondano alla replica di produzione, su base continuativa

Esaminiamo un caso semplice in cui si dispone di un'applicazione denominata Simple-Service attualmente in esecuzione nella regione Stati Uniti orientali (Virginia settentrionale) (us-east-1). È inoltre disponibile una copia in standby dell'applicazione nella regione Stati Uniti occidentali (Oregon) (us-west-2). In questo esempio, configureremo i controlli di fattibilità per confrontare queste due versioni dell'applicazione. Questo ci consente di garantire che la regione di standby, Stati Uniti occidentali (Oregon), sia pronta a ricevere traffico, se necessario in uno scenario di failover.

Per ulteriori informazioni sull'utilizzo di AWS CLI, vedere Command Reference.AWS CLI Per un elenco delle azioni dell'API Readiness e i collegamenti a ulteriori informazioni, vedereOperazioni dell'API per il controllo della prontezza.

Le celle in ARC rappresentano i limiti di errore (come le zone di disponibilità o le regioni) e vengono raccolte in gruppi di ripristino. Un gruppo di ripristino rappresenta un'applicazione per la quale si desidera verificare la preparazione al failover. Per ulteriori informazioni sui componenti del controllo di fattibilità, vedere. Componenti per il controllo di fattibilità

> **Note**
>
> ARC è un servizio globale che supporta più endpoint, Regioni AWS ma è necessario specificare la regione Stati Uniti occidentali (Oregon) (ovvero specificare il parametro`--region us-west-2`) nella maggior parte dei comandi ARC CLI. Ad esempio, per creare risorse come gruppi di ripristino o controlli di preparazione.

Per il nostro esempio di applicazione, inizieremo creando una cella per ogni regione in cui disponiamo di risorse. Quindi creeremo un gruppo di ripristino e completeremo la configurazione per un controllo di prontezza.

1. Crea celle

1a. Crea una cella us-east-1.

```
aws route53-recovery-readiness --region us-west-2 create-cell \
    --cell-name east-cell
```

```
{
    "CellArn": "arn:aws:route53-recovery-readiness::111122223333:cell/east-cell",
    "CellName": "east-cell",
    "Cells": [],
    "ParentReadinessScopes": [],
    "Tags": {}
}
```

1b. Crea una cella us-west-1.

```
aws route53-recovery-readiness --region us-west-2 create-cell \
    --cell-name west-cell
```

```
{
    "CellArn": "arn:aws:route53-recovery-readiness::111122223333:cell/west-cell",
    "CellName": "west-cell",
    "Cells": [],
    "ParentReadinessScopes": [],
    "Tags": {}
}
```

1c. Ora abbiamo due celle. Puoi verificare che esistano chiamando l'`list-cells`API.

```
aws route53-recovery-readiness --region us-west-2 list-cells
```

```
{
    "Cells": [
        {
            "CellArn": "arn:aws:route53-recovery-readiness::111122223333:cell/east-
cell",
            "CellName": "east-cell",
            "Cells": [],
            "ParentReadinessScopes": [],
            "Tags": {}
        },
        {
            "CellArn": "arn:aws:route53-recovery-readiness::111122223333:cell/west-
cell",
            "CellName": "west-cell"
            "Cells": [],
```

```
            "ParentReadinessScopes": [],
            "Tags": {}
        }
    ]
}
```

2. Crea un gruppo di ripristino

I gruppi di ripristino sono la risorsa di primo livello per la preparazione al ripristino in ARC. Un gruppo di ripristino rappresenta un'applicazione nel suo insieme. In questo passaggio, creeremo un gruppo di ripristino per modellare un'applicazione complessiva, quindi aggiungeremo le due celle che abbiamo creato.

2a. Crea un gruppo di ripristino.

```
aws route53-recovery-readiness --region us-west-2 create-recovery-group \
    --recovery-group-name simple-service-recovery-group \
       --cells "arn:aws:route53-recovery-readiness::111122223333:cell/east-cell"\
       "arn:aws:route53-recovery-readiness::111122223333:cell/west-cell"
```

```
{
    "Cells": [],
    "RecoveryGroupArn": "arn:aws:route53-recovery-readiness::111122223333:recovery-
group/simple-service-recovery-group",
    "RecoveryGroupName": "simple-service-recovery-group",
    "Tags": {}
}
```

2 b. (Facoltativo) È possibile verificare che il gruppo di ripristino sia stato creato correttamente chiamando l'`list-recovery-groups` API.

```
aws route53-recovery-readiness --region us-west-2 list-recovery-groups
```

```
{
    "RecoveryGroups": [
        {
            "Cells": [
                "arn:aws:route53-recovery-readiness::111122223333:cell/east-cell",
                "arn:aws:route53-recovery-readiness::111122223333:cell/west-cell"
            ],
```

```
            "RecoveryGroupArn": "arn:aws:route53-recovery-
readiness::111122223333:recovery-group/simple-service-recovery-group",
            "RecoveryGroupName": "simple-service-recovery-group",
            "Tags": {}
        }
    ]
}
```

Ora che abbiamo un modello per la nostra applicazione, aggiungiamo le risorse da monitorare. In ARC, un gruppo di risorse che si desidera monitorare è chiamato set di risorse. I set di risorse contengono risorse tutte dello stesso tipo. Confrontiamo tra loro le risorse di un set di risorse per determinare la disponibilità di una cella al failover.

3. Crea un set di risorse

Supponiamo che la nostra Simple-Service applicazione sia davvero molto semplice e utilizzi solo tabelle DynamoDB. Ha una tabella DynamoDB in us-east-1 e un'altra in us-west-2. Un set di risorse contiene anche un ambito di preparazione, che identifica la cella in cui è contenuta ogni risorsa.

3a. Crea un set di risorse che rifletta le risorse della nostra Simple-Service applicazione.

```
aws route53-recovery-readiness --region us-west-2 create-resource-set \
    --resource-set-name ImportantInformationTables \
    --resource-set-type AWS::DynamoDB::Table \
    --resources
    ResourceArn="arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsWest2",ReadinessScopes="arn:aws:route53-recovery-readiness::111122223333:cell/
west-cell"
    ResourceArn="arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsEast1",ReadinessScopes="arn:aws:route53-recovery-readiness::111122223333:cell/
east-cell"
```

```
{
    "ResourceSetArn": "arn:aws:route53-recovery-readiness::111122223333:resource-set/
sample-resource-set",
    "ResourceSetName": "ImportantInformationTables",
    "Resources": [
        {
            "ReadinessScopes": [
                "arn:aws:route53-recovery-readiness::111122223333:cell/west-cell"
            ],
```

```
            "ResourceArn": "arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsWest2"
        },
        {
            "ReadinessScopes": [
                "arn:aws:route53-recovery-readiness::111122223333:cell/east-cell"
            ],
            "ResourceArn": "arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsEast1"
        }
    ],
    "Tags": {}
}
```

3b. (Facoltativo) Puoi verificare cosa è incluso nel set di risorse chiamando l'`list-resource-sets`API. Questo elenca tutti i set di risorse per un AWS account. Qui puoi vedere che abbiamo solo un set di risorse che abbiamo creato sopra.

```
aws route53-recovery-readiness --region us-west-2 list-resource-sets
```

```
{
    "ResourceSets": [
        {
            "ResourceSetArn": "arn:aws:route53-recovery-
readiness::111122223333:resource-set/ImportantInformationTables",
            "ResourceSetName": "ImportantInformationTables",
            "Resources": [
                {
                    "ReadinessScopes": [
                        "arn:aws:route53-recovery-readiness::111122223333:cell/west-
cell"
                    ],
                    "ResourceArn": "arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsWest2"
                },
                {
                    "ReadinessScopes": [
                        "arn:aws:route53-recovery-readiness::111122223333:cell/east-
cell"
                    ],
                    "ResourceArn": "arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsEast1"
```

```
                }
            ],
            "Tags": {}
        }
    ]
}{
    "ResourceSets": [
        {
            "ResourceSetArn": "arn:aws:route53-recovery-
readiness::111122223333:resource-set/ImportantInformationTables",
            "ResourceSetName": "ImportantInformationTables",
            "Resources": [
                {
                    "ReadinessScopes": [
                        "arn:aws:route53-recovery-readiness::111122223333:cell/west-
cell"
                    ],
                    "ResourceArn": "arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsWest2"
                },
                {
                    "ReadinessScopes": [
                        "arn:aws:route53-recovery-
readiness::&ExampleAWSAccountNo1;:cell/east-cell"
                    ],
                    "ResourceArn": "arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsEast1"
                }
            ],
            "Tags": {}
        }
    ]
}
```

Ora abbiamo creato le celle, il gruppo di ripristino e il set di risorse per modellare l'Simple-Serviceapplicazione in ARC. Successivamente, imposteremo i controlli di idoneità per monitorare la disponibilità delle risorse al failover.

4. Crea un controllo di prontezza

Un controllo di idoneità applica un set di regole a ciascuna risorsa del set di risorse allegato al controllo. Le regole sono specifiche per ogni tipo di risorsa. Cioè, esistono regole diverse per `AWS::DynamoDB::TableAWS::EC2::Instance`, e così via. Le regole controllano diverse

dimensioni di una risorsa, tra cui la configurazione, la capacità (se disponibile e applicabile), i limiti (se disponibili e applicabili) e le configurazioni di routing.

> **Note**
>
> Per visualizzare le regole applicate a una risorsa durante un controllo di fattibilità, puoi utilizzare l'`get-readiness-check-resource-status`API, come descritto nel passaggio 5. Per visualizzare un elenco di tutte le regole di preparazione in ARC, usa `list-rules` o vedi. Descrizioni delle regole di preparazione in ARC ARC ha un set specifico di regole che esegue per ogni tipo di risorsa; al momento non sono personalizzabili.

4a. Crea un controllo di idoneità per il set di risorse,ImportantInformationTables.

```
aws route53-recovery-readiness --region us-west-2 create-readiness-check \
    --readiness-check-name ImportantInformationTableCheck --resource-set-name
 ImportantInformationTables
```

```
{
    "ReadinessCheckArn": "arn:aws:route53-recovery-readiness::111122223333:readiness-
check/ImportantInformationTableCheck",
    "ReadinessCheckName": "ImportantInformationTableCheck",
    "ResourceSet": "ImportantInformationTables",
    "Tags": {}
}
```

4 b. (Facoltativo) Per verificare che il controllo di disponibilità sia stato creato correttamente, esegui l'`list-readiness-checks`API. Questa API mostra tutti i controlli di disponibilità in un account.

```
aws route53-recovery-readiness --region us-west-2 list-readiness-checks
```

```
{
    "ReadinessChecks": [
        {
            "ReadinessCheckArn": "arn:aws:route53-recovery-
readiness::111122223333:readiness-check/ImportantInformationTableCheck",
            "ReadinessCheckName": "ImportantInformationTableCheck",
            "ResourceSet": "ImportantInformationTables",
            "Tags": {}
```

```
        }
    ]
}
```

5. Monitora i controlli di prontezza

Ora che abbiamo modellato l'applicazione e aggiunto un controllo di fattibilità, siamo pronti a monitorare le risorse. È possibile modellare la preparazione dell'applicazione su quattro livelli: il livello di controllo della disponibilità (un gruppo di risorse), il livello di risorsa individuale, il livello di cella (tutte le risorse in una zona o regione di disponibilità) e il livello di gruppo di ripristino (l'applicazione nel suo insieme). Di seguito sono riportati i comandi per ottenere ciascuno di questi tipi di stati di prontezza.

5a. Visualizza lo stato del tuo controllo di disponibilità.

```
aws route53-recovery-readiness --region us-west-2 get-readiness-check-status\
    --readiness-check-name ImportantInformationTableCheck
```

```
{
    "Readiness": "READY",
    "Resources": [
        {
            "LastCheckedTimestamp": "2021-01-07T00:53:39Z",
            "Readiness": "READY",
            "ResourceArn": "arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsWest2"
        },
        {
            "LastCheckedTimestamp": "2021-01-07T00:53:39Z",
            "Readiness": "READY",
            "ResourceArn": "arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsEast2"
    ]
}
```

5 b. Visualizza lo stato di preparazione dettagliato di una singola risorsa in un controllo di disponibilità, incluso lo stato di ogni regola verificata.

```
aws route53-recovery-readiness --region us-west-2 get-readiness-check-resource-status \
    --readiness-check-name ImportantInformationTableCheck \
```

```
    --resource-identifier "arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsWest2"
```


```
{"Readiness": "READY",
    "Rules": [
        {
            "LastCheckedTimestamp": "2021-01-07T00:55:41Z",
            "Messages": [],
            "Readiness": "READY",
            "RuleId": "DynamoTableStatus"
        },
        {
            "LastCheckedTimestamp": "2021-01-07T00:55:41Z",
            "Messages": [],
            "Readiness": "READY",
            "RuleId": "DynamoCapacity"
        },
        {
            "LastCheckedTimestamp": "2021-01-07T00:55:41Z",
            "Messages": [],
            "Readiness": "READY",
            "RuleId": "DynamoPeakRcuWcu"
        },
        {
            "LastCheckedTimestamp": "2021-01-07T00:55:41Z",
            "Messages": [],
            "Readiness": "READY",
            "RuleId": "DynamoGSIsPeakRcuWcu"
        },
        {
            "LastCheckedTimestamp": "2021-01-07T00:55:41Z",
            "Messages": [],
            "Readiness": "READY",
            "RuleId": "DynamoGSIsConfig"
        },
        {
            "LastCheckedTimestamp": "2021-01-07T00:55:41Z",
            "Messages": [],
            "Readiness": "READY",
            "RuleId": "DynamoGSIsStatus"
        },
        {
            "LastCheckedTimestamp": "2021-01-07T00:55:41Z",
```

```
            "Messages": [],
            "Readiness": "READY",
            "RuleId": "DynamoGSIsCapacity"
        },
        {
            "LastCheckedTimestamp": "2021-01-07T00:55:41Z",
            "Messages": [],
            "Readiness": "READY",
            "RuleId": "DynamoReplicationLatency"
        },
        {
            "LastCheckedTimestamp": "2021-01-07T00:55:41Z",
            "Messages": [],
            "Readiness": "READY",
            "RuleId": "DynamoAutoScalingConfiguration"
        },
        {
            "LastCheckedTimestamp": "2021-01-07T00:55:41Z",
            "Messages": [],
            "Readiness": "READY",
            "RuleId": "DynamoLimits"
        }
    ]
}
```

5c. Visualizza la disponibilità complessiva di una cella.

```
aws route53-recovery-readiness --region us-west-2 get-cell-readiness-summary \
    --cell-name west-cell
```

```
{
    "Readiness": "READY",
    "ReadinessChecks": [
        {
            "Readiness": "READY",
            "ReadinessCheckName": "ImportantTableCheck"
        }
    ]
}
```

5d. Infine, verificate la massima preparazione della vostra applicazione, a livello di gruppo di ripristino.

```
aws route53-recovery-readiness --region us-west-2 get-recovery-group-readiness-summary
 \
    --recovery-group-name simple-service-recovery-group
```

```
{
    "Readiness": "READY",
    "ReadinessChecks": [
        {
            "Readiness": "READY",
            "ReadinessCheckName": "ImportantTableCheck"
        }
    ]
}
```

Utilizzo dei gruppi di ripristino e dei controlli di fattibilità

> **Note**
>
> La funzionalità di controllo della disponibilità in Amazon Application Recovery Controller (ARC) non sarà più aperta ai nuovi clienti a partire dal 30 aprile 2026. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta Amazon Application Recovery Controller (ARC) readiness check availability change.

Questa sezione descrive e fornisce le procedure per i gruppi di ripristino e i controlli di fattibilità, tra cui la creazione, l'aggiornamento e l'eliminazione di queste risorse.

Creazione, aggiornamento ed eliminazione di gruppi di ripristino in ARC

> **Note**
>
> La funzionalità di controllo della disponibilità in Amazon Application Recovery Controller (ARC) non sarà più aperta ai nuovi clienti a partire dal 30 aprile 2026. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta Amazon Application Recovery Controller (ARC) readiness check availability change.

Un gruppo di ripristino rappresenta la tua applicazione in Amazon Application Recovery Controller (ARC). In genere è costituito da due o più celle che sono repliche l'una dell'altra in termini di risorse

e funzionalità, in modo da poter eseguire il failover dall'una all'altra. Ogni cella include gli Amazon Resource Names (ARNs) per le risorse attive per una AWS regione o zona di disponibilità. Le risorse potrebbero essere un sistema di bilanciamento del carico Elastic Load Balancing, un gruppo Auto Scaling o altre risorse. Una cella corrispondente che rappresenta un'altra zona o regione contiene risorse di standby dello stesso tipo presenti nella cella attiva: un sistema di bilanciamento del carico, un gruppo Auto Scaling e così via.

Una cella rappresenta le repliche dell'applicazione. I controlli di fattibilità in ARC consentono di determinare se l'applicazione è pronta per il failover da una replica all'altra. Tuttavia, è necessario decidere se affidarsi o meno a una replica in base ai sistemi di monitoraggio e controllo dello stato di salute e considerare i controlli di fattibilità come un servizio complementare a tali sistemi.

I controlli di prontezza controllano le risorse per determinarne la disponibilità in base a una serie di regole predefinite per quel tipo di risorsa. Dopo aver creato il gruppo di ripristino con le repliche, aggiungi i controlli di fattibilità ARC per le risorse dell'applicazione, in modo che ARC possa contribuire a garantire che le repliche abbiano la stessa configurazione e configurazione nel tempo.

Argomenti

- Creazione di gruppi di ripristino
- Aggiornamento ed eliminazione di gruppi e celle di ripristino

Creazione di gruppi di ripristino

I passaggi di questa sezione spiegano come creare un gruppo di ripristino sulla console ARC. Per ulteriori informazioni sull'utilizzo delle operazioni API di preparazione al ripristino con Amazon Application Recovery Controller (ARC), consultaOperazioni dell'API per il controllo della prontezza.

Per creare un gruppo di ripristino

1. Apri la console ARC all'indirizzohttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Scegli Readiness check.
3. Nella pagina Recovery Recovery Recovery Recovery, scegli Crea, quindi scegli un gruppo di Recovery.
4. Inserisci un nome per il gruppo di recupero, quindi scegli Avanti.
5. Scegli Crea celle, quindi scegli Aggiungi cella.

6. Inserisci un nome per la cella. Ad esempio, se disponi di una replica dell'applicazione negli Stati Uniti occidentali (California settentrionale), puoi aggiungere una cella denominata. `MyApp-us-west-1`
7. Scegli Aggiungi cella e aggiungi un nome per una seconda cella. Ad esempio, se hai una replica negli Stati Uniti orientali (Ohio), puoi aggiungere una cella denominata. `MyApp-us-east-2`
8. Se desideri aggiungere celle nidificate (repliche nelle zone di disponibilità all'interno delle regioni), scegli Azione, scegli Aggiungi cella nidificata e quindi inserisci un nome.
9. Dopo aver aggiunto tutte le celle e le celle nidificate per le repliche delle applicazioni, scegli Avanti.
10. Controlla il tuo gruppo di ripristino, quindi scegli Crea gruppo di ripristino.

Aggiornamento ed eliminazione di gruppi e celle di ripristino

I passaggi di questa sezione spiegano come aggiornare ed eliminare un gruppo di ripristino ed eliminare una cella sulla console ARC. Per ulteriori informazioni sull'utilizzo delle operazioni API di preparazione al ripristino con Amazon Application Recovery Controller (ARC), consultaOperazioni dell'API per il controllo della prontezza.

Per aggiornare o eliminare un gruppo di ripristino o eliminare una cella

1. Apri la console ARC all'indirizzohttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Scegli Readiness check.
3. Nella pagina Recovery Readiness, scegli un gruppo di ripristino.
4. Per lavorare con un gruppo di ripristino, scegli Azione, quindi scegli Modifica gruppo di ripristino o Elimina gruppo di ripristino.
5. Quando modifichi un gruppo di recupero, puoi aggiungere o rimuovere celle o celle annidate.
   - Per aggiungere una cella, scegli Aggiungi cella.
   - Per rimuovere una cella, nell'etichetta Azione accanto alla cella, scegli Elimina cella.

Creazione e aggiornamento dei controlli di idoneità in ARC

> **Note**
>
> La funzionalità di controllo della disponibilità in Amazon Application Recovery Controller (ARC) non sarà più aperta ai nuovi clienti a partire dal 30 aprile 2026. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta Amazon Application Recovery Controller (ARC) readiness check availability change.

Questa sezione fornisce le procedure per i controlli di fattibilità e i set di risorse, tra cui la creazione, l'aggiornamento e l'eliminazione di queste risorse.

Creazione e aggiornamento di un controllo di idoneità

I passaggi di questa sezione spiegano come creare un controllo di idoneità sulla console ARC. Per ulteriori informazioni sull'utilizzo delle operazioni API di preparazione al ripristino con Amazon Application Recovery Controller (ARC), consultaOperazioni dell'API per il controllo della prontezza.

Per aggiornare un controllo di prontezza, puoi modificare il set di risorse per il controllo di prontezza, aggiungere o rimuovere risorse o modificare l'ambito di preparazione di una risorsa.

Per creare un controllo di prontezza

1. Apri la console ARC all'indirizzohttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Scegli Readiness check.
3. Nella pagina Readiness, scegli Crea, quindi scegli un controllo di Readiness.
4. Immettete un nome per il controllo di disponibilità, scegliete il tipo di risorsa che desiderate controllare, quindi scegliete Avanti.
5. Aggiungi un set di risorse per il controllo di idoneità. Un set di risorse è un gruppo di risorse dello stesso tipo in repliche diverse. Seleziona una delle seguenti opzioni:

   - Crea un controllo di fattibilità con le risorse di un set di risorse che hai già creato.
   - Crea un nuovo set di risorse.

   Se scegli di creare un nuovo set di risorse, inserisci un nome e scegli Aggiungi.

6. Copia e incolla Amazon Resource Names (ARNs) uno per uno per ogni risorsa che desideri includere nel set, quindi scegli Avanti.

   > **Tip**
   >
   > Per esempi e ulteriori informazioni sul formato ARN previsto da ARC per ogni tipo di risorsa, vedere. Tipi di risorse e formati ARN in ARC

7. Se lo desideri, visualizza le regole di preparazione che verranno utilizzate quando ARC verifica il tipo di risorsa che hai incluso in questo controllo di disponibilità. Quindi scegli Successivo.
8. (Facoltativo) In Nome del gruppo di ripristino, scegliete un gruppo di ripristino a cui associare il controllo di prontezza e quindi, per ogni ARN di risorsa, scegliete una cella (Regione o Zona di disponibilità) dal menu a discesa in cui si trova la risorsa. Se si tratta di una risorsa a livello di applicazione, ad esempio una politica di routing DNS, scegli risorsa globale (nessuna cella).

   Questo specifica gli ambiti di disponibilità per le risorse oggetto del controllo di fattibilità.

   > **Important**
   >
   > Sebbene questo passaggio sia facoltativo, è necessario aggiungere degli ambiti di preparazione per ottenere informazioni riepilogative sulla preparazione per il gruppo e le celle di ripristino. Se si salta questo passaggio e non si associa il controllo di fattibilità alle risorse del gruppo di ripristino selezionando qui gli ambiti di preparazione, ARC non può restituire informazioni riassuntive sulla disponibilità per il gruppo o le celle di ripristino.

9. Scegli Next (Successivo).
10. Controlla le informazioni nella pagina di conferma, quindi scegli Crea controllo di fattibilità.

Per eliminare un controllo di idoneità

1. Apri la console ARC all'indirizzohttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Scegli Readiness check.
3. Scegliete un controllo di conformità e, in Azioni, scegliete Elimina.

Creazione e modifica di set di risorse

In genere, si crea un set di risorse come parte della creazione di un controllo di disponibilità, ma è possibile creare un set di risorse anche separatamente. È inoltre possibile modificare un set di risorse per aggiungere o rimuovere risorse. I passaggi di questa sezione spiegano come creare o modificare un set di risorse sulla console ARC. Per ulteriori informazioni sull'utilizzo delle operazioni API di preparazione al ripristino con Amazon Application Recovery Controller (ARC), consultaOperazioni dell'API per il controllo della prontezza.

Per creare un set di risorse

1. Apri la console Route 53 a https://console.aws.amazon.com/route53/casa.
2. In Application Recovery Controller, scegli Resource sets.
3. Scegli Create (Crea).
4. Immettete un nome per il set di risorse, quindi scegliete il tipo di risorsa da includere nel set.
5. Scegli Aggiungi, quindi inserisci l'Amazon Resource Name (ARN) per la risorsa da aggiungere al set.
6. Dopo aver finito di aggiungere risorse, scegli Crea set di risorse.

Per modificare un set di risorse

1. Apri la console ARC all'indirizzohttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Scegli Readiness check.
3. In Set di risorse, scegli Azione, quindi scegli Modifica.
4. Esegui una delle seguenti operazioni:
   - Per rimuovere una risorsa dal set, scegliete Rimuovi.
   - Per aggiungere una risorsa al set, scegli Aggiungi, quindi inserisci l'Amazon Resource Name (ARN) per la risorsa.
5. Puoi anche modificare l'ambito di disponibilità della risorsa, per associare la risorsa a una cella diversa per il controllo di disponibilità.
6. Scegli Save (Salva).

Monitoraggio dello stato di preparazione in ARC

> **Note**
>
> La funzionalità di controllo della disponibilità in Amazon Application Recovery Controller (ARC) non sarà più aperta ai nuovi clienti a partire dal 30 aprile 2026. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta Amazon Application Recovery Controller (ARC) readiness check availability change.

Puoi verificare lo stato di preparazione della tua applicazione in Amazon Application Recovery Controller (ARC) ai seguenti livelli:

- Il livello di verifica della disponibilità delle risorse in un set di risorse
- Il livello di risorsa individuale
- Il livello di cella (replica dell'applicazione) per tutte le risorse in una zona o AWS regione di disponibilità
- Il livello del gruppo di ripristino per l'intera applicazione

È possibile ricevere notifiche sulle modifiche dello stato di preparazione oppure è possibile monitorare le modifiche allo stato di prontezza nella console Route 53 o utilizzando i comandi ARC CLI.

Notifica dello stato di prontezza

Puoi utilizzare Amazon EventBridge per configurare regole basate sugli eventi per monitorare le risorse ARC e informarti sui cambiamenti nello stato di preparazione. Per ulteriori informazioni, consulta Utilizzo del Readiness Check in ARC con Amazon EventBridge.

Monitoraggio dello stato di preparazione nella console ARC

La procedura seguente descrive come monitorare la preparazione al ripristino in. Console di gestione AWS

1. Apri la console ARC all'indirizzohttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Scegli Readiness check.
3. Nella pagina Readiness, in Recovery group, visualizza lo stato di preparazione del gruppo di ripristino per ogni gruppo di ripristino (applicazione).

È inoltre possibile visualizzare la disponibilità di celle specifiche o di singole risorse.

Monitoraggio dello stato di preparazione utilizzando i comandi CLI

Questa sezione fornisce esempi di AWS CLI comandi da utilizzare per verificare lo stato di disponibilità dell'applicazione e delle risorse a diversi livelli.

Disponibilità per un set di risorse

Lo stato di un controllo di disponibilità creato per un set di risorse (un gruppo di risorse).

```
aws route53-recovery-readiness --region us-west-2 get-readiness-check-status --readiness-check-name ReadinessCheckName
```

Disponibilità per una singola risorsa

Per ottenere lo stato di una singola risorsa in un controllo di disponibilità, incluso lo stato di ogni regola di preparazione verificata, specificare il nome del controllo di disponibilità e l'ARN della risorsa. Esempio:

```
aws route53-recovery-readiness --region us-west-2 get-readiness-check-status --readiness-check-name ReadinessCheckName --resource-arn "arn:aws:dynamodb:us-west-2:111122223333:table/TableName"
```

Disponibilità per una cella

Lo stato di una singola cella, ovvero una regione o una zona di disponibilità.

```
aws route53-recovery-readiness --region us-west-2 get-cell-readiness-summary --cell-name CellName
```

Disponibilità per un'applicazione

Lo stato dell'applicazione complessiva, a livello di gruppo di ripristino.

```
aws route53-recovery-readiness --region us-west-2 get-recovery-group-readiness-summary --recovery-group-name RecoveryGroupName
```

Ottenere consigli sull'architettura in ARC

> **Note**
>
> La funzionalità di controllo della disponibilità in Amazon Application Recovery Controller (ARC) non sarà più aperta ai nuovi clienti a partire dal 30 aprile 2026. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta Amazon Application Recovery Controller (ARC) readiness check availability change.

Se disponi di un'applicazione esistente, Amazon Application Recovery Controller (ARC) può valutare l'architettura dell'applicazione e le politiche di routing per fornire consigli per modificare il design per migliorare la resilienza di ripristino dell'applicazione. Dopo aver creato un gruppo di ripristino in ARC che rappresenta la tua applicazione, segui i passaggi di questa sezione per ottenere consigli sull'architettura dell'applicazione.

Ti consigliamo di specificare una risorsa di destinazione per la risorsa di destinazione DNS per il tuo gruppo di ripristino, se non ne hai ancora specificata una, in modo da poter fornire consigli più dettagliati. Quando fornisci informazioni aggiuntive, ARC può fornirti consigli migliori. Ad esempio, se inserisci un record di risorse Amazon Route 53 o un Network Load Balancer come risorsa di destinazione, ARC può fornire informazioni sul fatto che tu abbia creato il numero ottimale di celle per il tuo gruppo di ripristino.

Tieni presente quanto segue per le risorse di destinazione DNS:

- Specificare solo un record di risorse Route 53 o Network Load Balancer per una risorsa di destinazione.
- Crea solo una risorsa di destinazione DNS per ogni gruppo di ripristino.
- Consigliato: crea una risorsa di destinazione DNS per ogni cella.
- Raggruppa le risorse di destinazione DNS in un unico set di risorse con un controllo di disponibilità.

La procedura seguente spiega come creare risorse di destinazione DNS e ottenere consigli sull'architettura per l'applicazione.

Per ricevere consigli per l'aggiornamento dell'architettura

1. Apri la console ARC all'indirizzohttps://console.aws.amazon.com/route53recovery/home#/dashboard.

2. Scegli Readiness check.
3. In Nome del gruppo di ripristino, scegli il gruppo di ripristino che rappresenta la tua applicazione.
4. Nella pagina dei dettagli del gruppo di ripristino, nel menu Azione, scegli Ottieni consigli sull'architettura per questo gruppo di ripristino.
5. Se non hai ancora creato un controllo di idoneità delle risorse di destinazione DNS, creane uno in modo che ARC possa fornire consigli sull'architettura. Scegli Crea una risorsa di destinazione DNS.

   Per ulteriori informazioni sulle risorse di destinazione DNS, consulta. Componenti per il controllo di fattibilità
6. Per creare un set di risorse per una risorsa di destinazione DNS, è necessario creare un controllo di conformità. Immettete un nome per il controllo di conformità e quindi, per il tipo di controllo di conformità, scegliete la risorsa di destinazione DNS.
7. Immettete un nome per il set di risorse.
8. Inserisci gli attributi per la tua applicazione, tra cui il nome DNS, l'ARN della zona ospitata e l'ID del set di record.

   > **Tip**
   >
   > Per visualizzare il formato di una zona ospitata ARN, vedere Formato ARN per una zona ospitata in. Tipi di risorse e formati ARN in ARC

   Facoltativamente, ma fortemente consigliato, scegli Aggiungi attributo opzionale e fornisci un ARN Network Load Balancer o il record di risorse Route 53 del tuo dominio.
9. (Facoltativo) Nella configurazione del gruppo di ripristino, scegli una cella per la risorsa di destinazione DNS per impostare l'ambito di disponibilità.
10. Scegli Crea set di risorse.
11. Nella pagina dei dettagli del gruppo di ripristino, scegli Ottieni consigli sull'architettura. ARC visualizza una serie di consigli sulla pagina.

Consulta l'elenco dei consigli. Potrai quindi decidere se e come apportare modifiche per migliorare la resilienza di ripristino della tua app.

Creazione di autorizzazioni per più account in ARC

> **Note**
>
> La funzionalità di controllo della disponibilità in Amazon Application Recovery Controller (ARC) non sarà più aperta ai nuovi clienti a partire dal 30 aprile 2026. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta Amazon Application Recovery Controller (ARC) readiness check availability change.

Potresti avere le tue risorse distribuite su più AWS account, il che può rendere difficile ottenere una visione completa dello stato dell'applicazione. Può anche rendere difficile ottenere le informazioni necessarie per prendere decisioni rapide. Per semplificare il controllo di idoneità in Amazon Application Recovery Controller (ARC), puoi utilizzare l'autorizzazione tra account.

L'autorizzazione tra più account in ARC funziona con la funzione di controllo della disponibilità. Con l'autorizzazione su più account, puoi utilizzare un AWS account centrale per monitorare le risorse che si trovano in più account. AWS In ogni account con risorse che desideri monitorare, autorizzi l'account centrale ad avere accesso a tali risorse. L'account centrale può quindi creare controlli di idoneità per le risorse di tutti gli account e, dall'account centrale, è possibile monitorare la disponibilità al failover.

> **Note**
>
> La configurazione dell'autorizzazione tra account non è disponibile nella console. Utilizza invece le operazioni dell'API ARC per configurare e utilizzare l'autorizzazione tra account. Per aiutarti a iniziare, questa sezione fornisce esempi di AWS CLI comandi.

Supponiamo che un'applicazione disponga di un account con risorse nella regione Stati Uniti occidentali (Oregon) (us-west-2) e che esista anche un account con risorse che desideri monitorare nella regione Stati Uniti orientali (Virginia settentrionale) (us-east-1). ARC può consentire l'accesso per monitorare entrambi i set di risorse da un account, us-west-2, utilizzando l'autorizzazione tra account.

Ad esempio, supponiamo che tu abbia i seguenti account: AWS

- Account USA-Ovest: 9999

- Conto negli Stati Uniti orientali: 1111

Nell'account us-east-1 (1111), possiamo abilitare l'autorizzazione tra account per consentire l'accesso all'account us-west-2 (9999) specificando l'Amazon Resource Name (ARN) per l'utente (root) nell'account IAM us-west-2:. `arn:aws:iam::999999999999:root` Dopo aver creato l'autorizzazione, l'account us-west-2 può aggiungere risorse di proprietà di us-east-1 ai set di risorse e creare controlli di fattibilità da eseguire sui set di risorse.

L'esempio seguente illustra l'impostazione dell'autorizzazione tra più account per un account. È necessario abilitare l'autorizzazione su più account in ogni account aggiuntivo che dispone di AWS risorse che si desidera aggiungere e monitorare in ARC.

> **Note**
>
> ARC è un servizio globale che supporta gli endpoint in più AWS regioni, ma è necessario specificare la regione Stati Uniti occidentali (Oregon) (ovvero specificare il parametro`--region us-west-2`) nella maggior parte dei comandi ARC CLI.

Il AWS CLI comando seguente mostra come impostare l'autorizzazione tra account per questo esempio:

```
aws route53-recovery-readiness --region us-west-2 --profile profile-in-us-east-1-
account \
    create-cross-account-authorization --cross-account-authorization
 arn:aws:iam::999999999999:root
```

Per disabilitare questa autorizzazione, procedi come segue:

```
aws route53-recovery-readiness --region us-west-2 --profile profile-in-us-east-1-
account \
    delete-cross-account-authorization --cross-account-authorization
 arn:aws:iam::999999999999:root
```

Per archiviare in un account specifico tutti gli account per i quali hai fornito l'autorizzazione per più account, usa il `list-cross-account-authorizations` comando. Tieni presente che al momento non puoi effettuare il check-in nella direzione opposta. Cioè, non esiste un'operazione API che puoi utilizzare con un profilo di account per elencare tutti gli account per i quali è stata concessa l'autorizzazione di aggiungere e monitorare risorse su più account.

```
aws route53-recovery-readiness --region us-west-2 --profile profile-in-us-east-1-account \
    list-cross-account-authorizations
```

```
{
    "CrossAccountAuthorizations": [
        "arn:aws:iam::999999999999:root"
    ]
}
```

Regole di preparazione, tipi di risorse e ARNS

> **Note**
>
> La funzionalità di controllo della disponibilità in Amazon Application Recovery Controller (ARC) non sarà più aperta ai nuovi clienti a partire dal 30 aprile 2026. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta Amazon Application Recovery Controller (ARC) readiness check availability change.

Questa sezione include informazioni di riferimento sulle regole di preparazione, le descrizioni, i tipi di risorse supportati e il formato per Amazon Resource Names (ARNs) che usi per i set di risorse.

Descrizioni delle regole di preparazione in ARC

> **Note**
>
> La funzionalità di controllo della disponibilità in Amazon Application Recovery Controller (ARC) non sarà più aperta ai nuovi clienti a partire dal 30 aprile 2026. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta Amazon Application Recovery Controller (ARC) readiness check availability change.

Questa sezione elenca le descrizioni delle regole di preparazione per tutti i tipi di risorse supportate da Amazon Application Recovery Controller (ARC). Per visualizzare un elenco dei tipi di risorse supportati da ARC, consultaTipi di risorse e formati ARN in ARC.

È inoltre possibile visualizzare le descrizioni delle regole di preparazione sulla console ARC o utilizzando un'operazione API, effettuando le seguenti operazioni:

- Per visualizzare le regole di preparazione nella console, segui i passaggi della procedura seguente:. Visualizza le regole di preparazione sulla console
- Per visualizzare le regole di preparazione utilizzando l'API, consulta l'ListRulesoperazione.

Argomenti

- Regole di preparazione in ARC
- Visualizza le regole di preparazione sulla console

Regole di preparazione in ARC

Questa sezione elenca l'insieme di regole di preparazione per ogni tipo di risorsa supportato da ARC.

Esaminando le descrizioni delle regole, è possibile notare che la maggior parte di esse include i termini Ispeziona tutto o Ispeziona ciascuno. Per comprendere in che modo questi termini spiegano il funzionamento di una regola nel contesto di un controllo di idoneità e altri dettagli su come ARC imposta lo stato di preparazione, vedi Come le regole di preparazione determinano lo stato di preparazione.

Regole di preparazione

ARC verifica le risorse utilizzando le seguenti regole di preparazione.

Amazon API Gateway versione 1, fasi

- ApiGwV1ApiKeyCount: ispeziona tutte le fasi dell'API Gateway per garantire che abbiano lo stesso numero di chiavi API collegate.
- ApiGwV1ApiKeySource: ispeziona tutte le fasi dell'API Gateway per assicurarsi che abbiano lo stesso valore per`API Key Source`.
- ApiGwV1BasePath: ispeziona tutte le fasi dell'API Gateway per garantire che siano collegate allo stesso percorso di base.
- ApiGwV1BinaryMediaTypes: ispeziona tutte le fasi dell'API Gateway per garantire che supportino gli stessi tipi di supporti binari.
- ApiGwV1CacheClusterEnabled: ispeziona tutte le fasi dell'API Gateway per assicurarsi che tutte siano state `Cache Cluster` abilitate o nessuna.
- ApiGwV1CacheClusterSize: ispeziona tutte le fasi dell'API Gateway per assicurarsi che siano le stesse`Cache Cluster Size`. Se uno ha un valore maggiore, gli altri sono contrassegnati come NOT READY.

- ApiGwV1CacheClusterStatus: ispeziona tutte le fasi dell'API Gateway per garantire che `Cache Cluster` sia nello stato DISPONIBILE.
- ApiGwV1DisableExecuteApiEndpoint: ispeziona tutte le fasi dell'API Gateway per assicurarsi che tutte siano `Execute API Endpoint` disabilitate o che nessuna lo sia.
- ApiGwV1DomainName: ispeziona tutte le fasi dell'API Gateway per garantire che siano collegate allo stesso nome di dominio.
- ApiGwV1EndpointConfiguration: ispeziona tutte le fasi dell'API Gateway per garantire che siano collegate a un dominio con la stessa configurazione dell'endpoint.
- ApiGwV1EndpointDomainNameStatus: ispeziona tutte le fasi dell'API Gateway per garantire che il nome di dominio a cui sono collegate sia nello stato AVAILABLE.
- ApiGwV1MethodSettings: ispeziona tutte le fasi dell'API Gateway per assicurarsi che abbiano lo stesso valore per`Method Settings`.
- ApiGwV1MutualTlsAuthentication: ispeziona tutte le fasi dell'API Gateway per assicurarsi che abbiano lo stesso valore per`Mutual TLS Authentication`.
- ApiGwV1Policy: ispeziona tutte le fasi dell'API Gateway per garantire che tutte utilizzino politiche a livello di API o che nessuna lo faccia.
- ApiGwV1RegionalDomainName: ispeziona tutte le fasi dell'API Gateway per garantire che siano collegate allo stesso nome di dominio regionale. Nota: questa regola non influisce sullo stato di preparazione.
- ApiGwV1ResourceMethodConfigs: ispeziona tutte le fasi dell'API Gateway per garantire che abbiano una gerarchia di risorse simile, incluse le relative configurazioni.
- ApiGwV1SecurityPolicy: ispeziona tutte le fasi dell'API Gateway per assicurarsi che abbiano lo stesso valore per`Security Policy`.
- ApiGwV1Quotas: ispeziona tutti i gruppi di API Gateway per garantire che siano conformi alle quote (limiti) gestite da Service Quotas.
- ApiGwV1UsagePlans: ispeziona tutte le fasi dell'API Gateway per garantire che siano collegate `Usage Plans` con la stessa configurazione.

Amazon API Gateway versione 2 fasi

- ApiGwV2ApiKeySelectionExpression: ispeziona tutte le fasi dell'API Gateway per verificare che abbiano lo stesso valore per`API Key Selection Expression`.
- ApiGwV2ApiMappingSelectionExpression: ispeziona tutte le fasi dell'API Gateway per assicurarsi che abbiano lo stesso valore per`API Mapping Selection Expression`.

- ApiGwV2CorsConfiguration: ispeziona tutte le fasi dell'API Gateway per garantire che abbiano la stessa configurazione relativa a CORS.
- ApiGwV2DomainName: ispeziona tutte le fasi dell'API Gateway per garantire che siano collegate allo stesso nome di dominio.
- ApiGwV2DomainNameStatus: ispeziona tutte le fasi dell'API Gateway per garantire che il nome di dominio sia nello stato DISPONIBILE.
- ApiGwV2EndpointType: ispeziona tutte le fasi dell'API Gateway per assicurarsi che abbiano lo stesso valore per`Endpoint Type`.
- ApiGwV2Quotas: ispeziona tutti i gruppi di API Gateway per garantire che siano conformi alle quote (limiti) gestite da Service Quotas.
- ApiGwV2MutualTlsAuthentication: ispeziona tutte le fasi dell'API Gateway per assicurarsi che abbiano lo stesso valore per`Mutual TLS Authentication`.
- ApiGwV2ProtocolType: ispeziona tutte le fasi dell'API Gateway per assicurarsi che abbiano lo stesso valore per`Protocol Type`.
- ApiGwV2RouteConfigs: ispeziona tutte le fasi dell'API Gateway per garantire che abbiano la stessa gerarchia di rotte con la stessa configurazione.
- ApiGwV2RouteSelectionExpression: ispeziona tutte le fasi dell'API Gateway per assicurarsi che abbiano lo stesso valore per`Route Selection Expression`.
- ApiGwV2RouteSettings: ispeziona tutte le fasi dell'API Gateway per assicurarsi che abbiano lo stesso valore per`Default Route Settings`.
- ApiGwV2SecurityPolicy: ispeziona tutte le fasi dell'API Gateway per assicurarsi che abbiano lo stesso valore per`Security Policy`.
- ApiGwV2StageVariables: ispeziona tutte le fasi dell'API Gateway per garantire che abbiano tutte le `Stage Variables` stesse fasi delle altre.
- ApiGwV2ThrottlingBurstLimit: ispeziona tutte le fasi dell'API Gateway per assicurarsi che abbiano lo stesso valore per`Throttling Burst Limit`.
- ApiGwV2ThrottlingRateLimit: ispeziona tutte le fasi dell'API Gateway per assicurarsi che abbiano lo stesso valore per`Throttling Rate Limit`.

Cluster Amazon Aurora

- RdsClusterStatus: ispeziona ogni cluster Aurora per verificare che abbia uno stato di `AVAILABLE` uno o. `BACKING-UP`
- RdsEngineMode: ispeziona tutti i cluster Aurora per assicurarsi che abbiano lo stesso valore. `Engine Mode`

- RdsEngineVersion: ispeziona tutti i cluster Aurora per assicurarsi che abbiano lo stesso valore. `Major Version`
- RdsGlobalReplicaLag: ispeziona ogni cluster Aurora per assicurarsi che abbia meno `Global Replica Lag` di 30 secondi.
- RdsNormalizedCapacity: ispeziona tutti i cluster Aurora per garantire che abbiano una capacità normalizzata entro il 15% del massimo nel set di risorse.
- RdsInstanceType: ispeziona tutti i cluster Aurora per assicurarsi che abbiano gli stessi tipi di istanze.
- RdsQuotas: ispeziona tutti i cluster Aurora per garantire che siano conformi alle quote (limiti) gestite da Service Quotas.

Gruppi Auto Scaling

- AsgMinSizeAndMaxSize: ispeziona tutti i gruppi di Auto Scaling per garantire che abbiano le stesse dimensioni minime e massime dei gruppi.
- AsgAZCount: ispeziona tutti i gruppi di Auto Scaling per garantire che abbiano lo stesso numero di zone di disponibilità.
- AsgInstanceTypes: ispeziona tutti i gruppi di Auto Scaling per assicurarsi che abbiano gli stessi tipi di istanze. Nota: questa regola non influisce sullo stato di preparazione.
- AsgInstanceSizes: ispeziona tutti i gruppi di Auto Scaling per assicurarsi che abbiano le stesse dimensioni delle istanze.
- AsgNormalizedCapacity: ispeziona tutti i gruppi di Auto Scaling per garantire che abbiano una capacità normalizzata entro il 15% del massimo del set di risorse.
- AsgQuotas: ispeziona tutti i gruppi di Auto Scaling per garantire che siano conformi alle quote (limiti) gestite da Service Quotas.

CloudWatch allarmi

- CloudWatchAlarmState: Ispeziona gli CloudWatch allarmi per assicurarsi che ciascuno non sia nello `ALARM` stato o. `INSUFFICIENT_DATA`

Gateway per i clienti

- CustomerGatewayIpAddress: ispeziona tutti i gateway dei clienti per assicurarsi che abbiano lo stesso indirizzo IP.
- CustomerGatewayState: ispeziona i gateway dei clienti per garantire che ciascuno si trovi nello stato in cui si trova. `AVAILABLE`
- CustomerGatewayVPNType: ispeziona tutti i gateway dei clienti per assicurarsi che abbiano lo stesso tipo di VPN.

DNS target resources

- DnsTargetResourceHostedZoneConfigurationRule: ispeziona tutte le risorse di destinazione DNS per garantire che abbiano lo stesso ID di zona ospitata di Amazon Route 53 e che ogni zona ospitata non sia privata. Nota: questa regola non influisce sullo stato di preparazione.
- DnsTargetResourceRecordSetConfigurationRule: ispeziona tutte le risorse di destinazione DNS per assicurarsi che abbiano lo stesso record di risorse TTL (Resource Record Cache Time to Live) e che TTLs siano inferiori o uguali a 300.
- DnsTargetResourceRoutingRule: ispeziona ogni risorsa di destinazione DNS associata a un set di record di risorse alias per garantire che indirizzi il traffico verso il nome DNS configurato sulla risorsa di destinazione. Nota: questa regola non influisce sullo stato di preparazione.
- DnsTargetResourceHealthCheckRule: ispeziona tutte le risorse di destinazione DNS per garantire che i controlli di integrità siano associati ai relativi set di record di risorse, quando appropriato e non altrimenti. Nota: questa regola non influisce sullo stato di preparazione.

Tabelle Amazon DynamoDB

- DynamoConfiguration: ispeziona tutte le tabelle DynamoDB per assicurarsi che abbiano le stesse chiavi, attributi, crittografia lato server e configurazioni di stream.
- DynamoTableStatus: ispeziona ogni tabella DynamoDB per assicurarsi che abbia lo stato ACTIVE.
- DynamoCapacity: ispeziona tutte le tabelle DynamoDB per garantire che le capacità di lettura e scrittura assegnate rientrino nel 20% delle capacità massime del set di risorse.
- DynamoPeakRcuWcu: ispeziona ogni tabella DynamoDB per assicurarsi che abbia avuto un traffico di picco simile a quello delle altre tabelle, per assicurare la capacità assegnata.
- DynamoGsiPeakRcuWcu: ispeziona ogni tabella DynamoDB per assicurarsi che abbia una capacità massima di lettura e scrittura simile a quella delle altre tabelle, per assicurare la capacità assegnata.
- DynamoGsiConfig: ispeziona tutte le tabelle DynamoDB con indici secondari globali per garantire che utilizzino lo stesso indice, schema chiave e proiezione.
- DynamoGsiStatus: ispeziona tutte le tabelle DynamoDB con indici secondari globali per garantire che gli indici secondari globali abbiano uno stato ATTIVO.
- DynamoGsiCapacity: ispeziona tutte le tabelle DynamoDB con indici secondari globali per garantire che le tabelle abbiano fornito capacità di lettura GSI e capacità di scrittura GSI entro il 20% delle capacità massime del set di risorse.
- DynamoReplicationLatency: ispeziona tutte le tabelle DynamoDB che sono tabelle globali per garantire che abbiano la stessa latenza di replica.

- DynamoAutoScalingConfiguration: ispeziona tutte le tabelle DynamoDB con Auto Scaling abilitato per garantire che abbiano le stesse capacità di lettura e scrittura minime, massime e target.
- DynamoQuotas: ispeziona tutte le tabelle DynamoDB per garantire che siano conformi alle quote (limiti) gestite da Service Quotas.

Elastic Load Balancing (sistemi di bilanciamento del carico classici)

- ElbV1CheckAzCount: ispeziona ogni Classic Load Balancer per assicurarsi che sia collegato a una sola zona di disponibilità. Nota: questa regola non influisce sullo stato di preparazione.
- ElbV1AnyInstances: ispeziona tutti i Classic Load Balancer per assicurarsi che abbiano almeno un'istanza EC2.
- ElbV1AnyInstancesHealthy: Ispeziona tutti i Classic Load Balancer per assicurarsi che abbiano almeno un'istanza EC2 integra.
- ElbV1Scheme: Ispeziona tutti i Classic Load Balancer per assicurarsi che abbiano lo stesso schema di bilanciamento del carico.
- ElbV1HealthCheckThreshold: Ispeziona tutti i Classic Load Balancer per assicurarsi che abbiano lo stesso valore di soglia di controllo dello stato.
- ElbV1HealthCheckInterval: Ispeziona tutti i Classic Load Balancer per garantire che abbiano lo stesso valore dell'intervallo di controllo dello stato.
- ElbV1CrossZoneRoutingEnabled: Ispeziona tutti i Classic Load Balancer per assicurarsi che abbiano lo stesso valore per il bilanciamento del carico tra zone (ABILITATO o DISABILITATO).
- ElbV1AccessLogsEnabledAttribute: Ispeziona tutti i Classic Load Balancer per assicurarsi che abbiano lo stesso valore per i log di accesso (ABILITATO o DISABILITATO).
- ElbV1ConnectionDrainingEnabledAttribute: Ispeziona tutti i Classic Load Balancer per assicurarsi che abbiano lo stesso valore per il drenaggio della connessione (ABILITATO o DISABILITATO).
- ElbV1ConnectionDrainingTimeoutAttribute: Ispeziona tutti i Classic Load Balancer per assicurarsi che abbiano lo stesso valore di timeout di esaurimento della connessione.
- ElbV1IdleTimeoutAttribute: Ispeziona tutti i Classic Load Balancer per assicurarsi che abbiano lo stesso valore per il timeout di inattività.
- ElbV1ProvisionedCapacityLcuCount: Ispeziona tutti i Classic Load Balancer con una LCU assegnata superiore a 10 per garantire che rientrino nel 20% della LCU più fornita nel set di risorse.

- ElbV1ProvisionedCapacityStatus: controlla lo stato della capacità assegnata su ogni Classic Load Balancer per assicurarsi che non abbia un valore di DISABLED o PENDING.

Volumi Amazon EBS

- EbsVolumeEncryption: ispeziona tutti i EBS volumi per assicurarsi che abbiano lo stesso valore di crittografia (ABILITATO o DISABILITATO).
- EbsVolumeEncryptionDefault: ispeziona tutti i EBS volumi per assicurarsi che abbiano lo stesso valore di crittografia per impostazione predefinita (ENABLED o DISABLED).
- EbsVolumeIops: ispeziona tutti i EBS volumi per garantire che abbiano input/output le stesse operazioni al secondo (IOPS).
- EbsVolumeKmsKeyId: ispeziona tutti i EBS volumi per assicurarsi che abbiano lo stesso ID di chiave predefinito AWS KMS .
- EbsVolumeMultiAttach: ispeziona tutti i EBS volumi per assicurarsi che abbiano lo stesso valore per il collegamento multiplo (ABILITATO o DISABILITATO).
- EbsVolumeQuotas: ispeziona tutti i EBS volumi per garantire che siano conformi alle quote (limiti) stabilite da Service Quotas.
- EbsVolumeSize: ispeziona tutti i EBS volumi per assicurarsi che abbiano le stesse dimensioni leggibili.
- EbsVolumeState: ispeziona tutti i EBS volumi per assicurarsi che abbiano lo stesso stato di volume.
- EbsVolumeType: ispeziona tutti i EBS volumi per assicurarsi che abbiano lo stesso tipo di volume.

AWS Lambda funzioni

- LambdaMemorySize: ispeziona tutte le funzioni Lambda per assicurarsi che abbiano la stessa dimensione di memoria. Se una ha più memoria, le altre vengono contrassegnate. `NOT READY`
- LambdaFunctionTimeout: ispeziona tutte le funzioni Lambda per assicurarsi che abbiano lo stesso valore di timeout. Se una ha un valore maggiore, le altre vengono contrassegnate. `NOT READY`
- LambdaFunctionRuntime: ispeziona tutte le funzioni Lambda per garantire che abbiano tutte lo stesso tempo di esecuzione.
- LambdaFunctionReservedConcurrentExecutions: ispeziona tutte le funzioni Lambda per assicurarsi che abbiano tutte lo stesso valore per. `Reserved Concurrent Executions` Se una ha un valore maggiore, le altre vengono contrassegnate. `NOT READY`

- LambdaFunctionDeadLetterConfig: ispeziona tutte le funzioni Lambda per assicurarsi che abbiano tutte `Dead Letter Config` una definizione o che nessuna di esse ne abbia una.
- LambdaFunctionProvisionedConcurrencyConfig: ispeziona tutte le funzioni Lambda per assicurarsi che abbiano lo stesso valore per. `Provisioned Concurrency`
- LambdaFunctionSecurityGroupCount: ispeziona tutte le funzioni Lambda per assicurarsi che abbiano lo stesso valore per. `Security Groups`
- LambdaFunctionSubnetIdCount: ispeziona tutte le funzioni Lambda per assicurarsi che abbiano lo stesso valore per. `Subnet Ids`
- LambdaFunctionEventSourceMappingMatch: ispeziona tutte le funzioni Lambda per garantire che tutte le proprietà `Event Source Mapping` scelte corrispondano tra loro.
- LambdaFunctionLimitsRule: ispeziona tutte le funzioni Lambda per garantire che siano conformi alle quote (limiti) gestite da Service Quotas.

Network Load Balancer e Application Load Balancer

- ElbV2CheckAzCount: ispeziona ogni Network Load Balancer per assicurarsi che sia collegato a una sola zona di disponibilità. Nota: questa regola non influisce sullo stato di preparazione.
- ElbV2TargetGroupsCanServeTraffic: ispeziona ogni Network Load Balancer e Application Load Balancer per assicurarsi che abbia almeno un'istanza Amazon EC2 integra.
- ElbV2State: ispeziona ogni Network Load Balancer e Application Load Balancer per assicurarsi che sia nello stato corretto. `ACTIVE`
- ElbV2IpAddressType: ispeziona tutti i Network Load Balancer e gli Application Load Balancer per assicurarsi che abbiano gli stessi tipi di indirizzi IP.
- ElbV2Scheme: ispeziona tutti i Network Load Balancer e gli Application Load Balancer per assicurarsi che abbiano lo stesso schema.
- ElbV2Type: Ispeziona tutti i Network Load Balancer e gli Application Load Balancer per assicurarsi che siano dello stesso tipo.
- ElbV2S3LogsEnabled: ispeziona tutti i Network Load Balancer e gli Application Load Balancer per garantire che abbiano lo stesso valore per i log di accesso al server Amazon S3 (ABILITATO o DISABILITATO).
- ElbV2DeletionProtection: ispeziona tutti i Network Load Balancer e gli Application Load Balancer per garantire che abbiano lo stesso valore per la protezione da eliminazione (ABILITATO o DISABILITATO).
- ElbV2IdleTimeoutSeconds: Ispeziona tutti i Network Load Balancer e gli Application Load Balancer per garantire che abbiano lo stesso valore nei secondi di inattività.

- ElbV2HttpDropInvalidHeaders: ispeziona tutti i Network Load Balancer e gli Application Load Balancer per assicurarsi che abbiano lo stesso valore per le intestazioni HTTP drop non valide.
- ElbV2Http2Enabled: ispeziona tutti i Network Load Balancer e gli Application Load Balancer per verificare che abbiano lo stesso valore di (ENABLED o DISABLED). HTTP2
- ElbV2CrossZoneEnabled: ispeziona tutti i Network Load Balancer e gli Application Load Balancer per garantire che abbiano lo stesso valore per il bilanciamento del carico tra zone (ABILITATO o DISABILITATO).
- ElbV2ProvisionedCapacityLcuCount: Ispeziona tutti i Network Load Balancer e gli Application Load Balancer con una LCU assegnata superiore a 10 per garantire che rientrino nel 20% della LCU più fornita nel set di risorse.
- ElbV2ProvisionedCapacityEnabled: verifica lo stato di capacità assegnato a tutti i Network Load Balancer e Application Load Balancer per verificare che non sia impostato il valore DISABLED o PENDING.

Cluster Amazon MSK

- MskClusterClientSubnet: ispeziona ogni cluster MSK per assicurarsi che abbia solo due o solo tre sottoreti client.
- MskClusterInstanceType: ispeziona tutti i cluster MSK per assicurarsi che abbiano lo stesso tipo di istanza Amazon EC2.
- MskClusterSecurityGroups: ispeziona tutti i cluster MSK per assicurarsi che abbiano gli stessi gruppi di sicurezza.
- MskClusterStorageInfo: ispeziona tutti i cluster MSK per assicurarsi che abbiano le stesse dimensioni del volume di storage EBS. Se uno ha un valore maggiore, gli altri sono contrassegnati come NOT READY.
- MskClusterACMCertificate: ispeziona tutti i cluster MSK per assicurarsi che abbiano lo stesso elenco di certificati di autorizzazione del client. ARNs
- MskClusterServerProperties: ispeziona tutti i cluster MSK per assicurarsi che abbiano lo stesso valore per. `Current Broker Software Info`
- MskClusterKafkaVersion: Ispeziona tutti i cluster MSK per assicurarsi che abbiano la stessa versione di Kafka.
- MskClusterEncryptionInTransitInCluster: Ispeziona tutti i cluster MSK per assicurarsi che abbiano lo stesso valore per. `Encryption In Transit In Cluster`
- MskClusterEncryptionInClientBroker: Ispeziona tutti i cluster MSK per assicurarsi che abbiano lo stesso valore di. `Encryption In Transit Client Broker`

- MskClusterEnhancedMonitoring: Ispeziona tutti i cluster MSK per assicurarsi che abbiano lo stesso valore di. `Enhanced Monitoring`
- MskClusterOpenMonitoringInJmx: Ispeziona tutti i cluster MSK per assicurarsi che abbiano lo stesso valore di. `Open Monitoring JMX Exporter`
- MskClusterOpenMonitoringInNode: Ispeziona tutti i cluster MSK per assicurarsi che abbiano lo stesso valore per `Open Monitoring Not Exporter.`
- MskClusterLoggingInS3: Ispeziona tutti i cluster MSK per assicurarsi che abbiano lo stesso valore di. `Is Logging in S3`
- MskClusterLoggingInFirehose: Ispeziona tutti i cluster MSK per assicurarsi che abbiano lo stesso valore di. `Is Logging In Firehose`
- MskClusterLoggingInCloudWatch: Ispeziona tutti i cluster MSK per assicurarsi che abbiano lo stesso valore di. `Is Logging Available In CloudWatch Logs`
- MskClusterNumberOfBrokerNodes: Ispeziona tutti i cluster MSK per assicurarsi che abbiano lo stesso valore di. `Number of Broker Nodes` Se uno ha un valore maggiore, gli altri sono contrassegnati come NOT READY.
- MskClusterState: ispeziona ogni cluster MSK per assicurarsi che sia in uno stato ATTIVO.
- MskClusterLimitsRule: ispeziona tutte le funzioni Lambda per garantire che siano conformi alle quote (limiti) gestite da Service Quotas.

Controlli sanitari di Amazon Route 53

- R53HealthCheckType: esamina ogni controllo dello stato della Route 53 per verificare che non sia di tipo CALCOLATO e che tutti i controlli siano dello stesso tipo.
- R53HealthCheckDisabled: ispeziona ogni controllo dello stato di salute della Route 53 per verificare che non sia stato DISABILITATO.
- R53HealthCheckStatus: ispeziona ogni controllo dello stato di salute della Route 53 per verificare che abbia lo stato SUCCESS.
- R53HealthCheckRequestInterval: ispeziona tutti i controlli di integrità della Route 53 per assicurarsi che abbiano tutti lo stesso valore per`Request Interval`.
- R53HealthCheckFailureThreshold: ispeziona tutti i controlli di integrità della Route 53 per assicurarsi che abbiano tutti lo stesso valore per `Failure Threshold.`
- R53HealthCheckEnableSNI: ispeziona tutti i controlli di integrità della Route 53 per assicurarsi che abbiano tutti lo stesso valore per `Enable SNI.`
- R53HealthCheckSearchString: ispeziona tutti i controlli di integrità della Route 53 per assicurarsi che abbiano tutti lo stesso valore per `Search String.`

- R53HealthCheckRegions: esamina tutti i controlli sanitari della Route 53 per assicurarsi che abbiano tutti lo stesso elenco di AWS regioni.
- R53HealthCheckMeasureLatency: ispeziona tutti i controlli di integrità della Route 53 per assicurarsi che abbiano tutti lo stesso valore per`Measure Latency`.
- R53HealthCheckInsufficientDataHealthStatus: ispeziona tutti i controlli di integrità della Route 53 per assicurarsi che abbiano tutti lo stesso valore per`Insufficient Data Health Status`.
- R53HealthCheckInverted: esamina tutti i controlli di integrità della Route 53 per assicurarsi che siano tutti invertiti o non siano tutti invertiti.
- R53HealthCheckResourcePath: ispeziona tutti i controlli di integrità della Route 53 per assicurarsi che abbiano tutti lo stesso valore per`Resource Path`.
- R53HealthCheckCloudWatchAlarm: ispeziona tutti i controlli di integrità della Route 53 per garantire che gli CloudWatch allarmi ad essi associati abbiano le stesse impostazioni e configurazioni.

Abbonamenti Amazon SNS

- SnsSubscriptionProtocol: Ispeziona tutti gli abbonamenti SNS per assicurarsi che abbiano lo stesso protocollo.
- SnsSubscriptionSqsLambdaEndpoint: ispeziona tutti gli abbonamenti SNS che dispongono di endpoint Lambda o SQS per assicurarsi che abbiano endpoint diversi.
- SnsSubscriptionNonAwsEndpoint: ispeziona tutti gli abbonamenti SNS che hanno un tipo di endpoint non di AWS servizio, ad esempio e-mail, per garantire che abbiano lo stesso endpoint.
- SnsSubscriptionPendingConfirmation: Ispeziona tutti gli abbonamenti SNS per assicurarsi che abbiano lo stesso valore per «Conferme in sospeso».
- SnsSubscriptionDeliveryPolicy: ispeziona tutti gli abbonamenti SNS utilizzati per garantire che abbiano lo stesso valore HTTP/S per «Periodo di consegna effettivo».
- SnsSubscriptionRawMessageDelivery: ispeziona tutti gli abbonamenti SNS per assicurarsi che abbiano lo stesso valore per «Raw Message Delivery».
- SnsSubscriptionFilter: ispeziona tutti gli abbonamenti SNS per assicurarsi che abbiano lo stesso valore per 'Filter Policy'.
- SnsSubscriptionRedrivePolicy: ispeziona tutti gli abbonamenti SNS per assicurarsi che abbiano lo stesso valore per 'Redrive Policy'.
- SnsSubscriptionEndpointEnabled: ispeziona tutti gli abbonamenti SNS per assicurarsi che abbiano lo stesso valore per «Endpoint Enabled».

- SnsSubscriptionLambdaEndpointValid: ispeziona tutti gli abbonamenti SNS che dispongono di endpoint Lambda per assicurarsi che abbiano endpoint Lambda validi.
- SnsSubscriptionSqsEndpointValidRule: ispeziona tutti gli abbonamenti SNS che utilizzano endpoint SQS per assicurarsi che dispongano di endpoint SQS validi.
- SnsSubscriptionQuotas: ispeziona tutti gli abbonamenti SNS per garantire che siano conformi alle quote (limiti) gestite da Service Quotas.

Argomenti di Amazon SNS

- SnsTopicDisplayName: esamina tutti gli argomenti SNS per assicurarsi che abbiano lo stesso valore per. `Display Name`
- SnsTopicDeliveryPolicy: controlla tutti gli argomenti SNS che hanno abbonati HTTPS per assicurarsi che abbiano lo stesso. `EffectiveDeliveryPolicy`
- SnsTopicSubscription: esamina tutti gli argomenti SNS per assicurarsi che abbiano lo stesso numero di abbonati per ciascuno dei relativi protocolli.
- SnsTopicAwsKmsKey: esamina tutti gli argomenti SNS per assicurarsi che tutti gli argomenti o nessuno di essi abbiano una chiave. AWS KMS
- SnsTopicQuotas: esamina tutti gli argomenti SNS per garantire che siano conformi alle quote (limiti) gestite da Service Quotas.

Code Amazon SQS

- SqsQueueType: Ispeziona tutte le code SQS per assicurarsi che abbiano tutte lo stesso valore. `Type`
- SqsQueueDelaySeconds: Ispeziona tutte le code SQS per assicurarsi che abbiano tutte lo stesso valore di. `Delay Seconds`
- SqsQueueMaximumMessageSize: Ispeziona tutte le code SQS per assicurarsi che abbiano tutte lo stesso valore di. `Maximum Message Size`
- SqsQueueMessageRetentionPeriod: Ispeziona tutte le code SQS per assicurarsi che abbiano tutte lo stesso valore di. `Message Retention Period`
- SqsQueueReceiveMessageWaitTimeSeconds: Ispeziona tutte le code SQS per assicurarsi che abbiano tutte lo stesso valore di. `Receive Message Wait Time Seconds`
- SqsQueueRedrivePolicyMaxReceiveCount: Ispeziona tutte le code SQS per assicurarsi che abbiano tutte lo stesso valore di. `Redrive Policy Max Receive Count`
- SqsQueueVisibilityTimeout: Ispeziona tutte le code SQS per assicurarsi che abbiano tutte lo stesso valore di. `Visibility Timeout`

- SqsQueueContentBasedDeduplication: Ispeziona tutte le code SQS per assicurarsi che abbiano tutte lo stesso valore di. `Content-Based Deduplication`
- SqsQueueQuotas: ispeziona tutte le code SQS per garantire che siano conformi alle quote (limiti) gestite da Service Quotas.

Amazon VPCs

- VpcCidrBlock: VPCs Ispeziona tutti per assicurarsi che abbiano tutti lo stesso valore per la dimensione della rete a blocchi CIDR.
- VpcCidrBlocksSameProtocolVersion: ispeziona tutti i VPCs blocchi CIDR con gli stessi blocchi CIDR per assicurarsi che abbiano lo stesso valore per il numero di versione del protocollo Internet Stream.
- VpcCidrBlocksStateInAssociationSets: Ispeziona tutti i set di associazioni di blocchi CIDR VPCs per assicurarsi che tutti abbiano blocchi CIDR che si trovano in uno stato. `ASSOCIATED`
- VpcIpv6CidrBlocksStateInAssociationSets: Ispeziona tutti i set di associazioni di blocchi CIDR VPCs per assicurarsi che abbiano tutti blocchi CIDR con lo stesso numero di indirizzi.
- VpcCidrBlocksInAssociationSets: Ispeziona tutti i set di associazioni di blocchi CIDR VPCs per assicurarsi che abbiano tutti la stessa dimensione.
- VpcIpv6CidrBlocksInAssociationSets: Ispeziona tutti i set di associazioni di blocchi IPv6 CIDR VPCs per assicurarsi che abbiano le stesse dimensioni.
- VpcState: ispeziona ogni VPC per assicurarsi che sia in `AVAILABLE` uno stato.
- VpcInstanceTenancy: VPCs Ispeziona tutti per assicurarsi che abbiano tutti lo stesso valore per. `Instance Tenancy`
- VpcIsDefault: VPCs Ispeziona tutti per assicurarsi che abbiano lo stesso valore per `Is Default.`
- VpcSubnetState: ispeziona ogni sottorete VPC per assicurarsi che sia in uno stato DISPONIBILE.
- VpcSubnetAvailableIpAddressCount: ispeziona ogni sottorete VPC per verificare che abbia un numero di indirizzi IP disponibili superiore a zero.
- VpcSubnetCount: ispeziona tutte le sottoreti VPC per assicurarsi che abbiano lo stesso numero di sottoreti.
- VpcQuotas: ispeziona tutte le sottoreti VPC per garantire che siano conformi alle quote (limiti) gestite da Service Quotas.

Site-to-Site VPN connessioni

- VpnConnectionsRouteCount: Ispeziona tutte le connessioni VPN per assicurarsi che abbiano almeno un percorso e lo stesso numero di percorsi.
- VpnConnectionsEnableAcceleration: Ispeziona tutte le connessioni VPN per assicurarsi che abbiano lo stesso valore per. `Enable Accelerations`
- VpnConnectionsStaticRoutesOnly: Ispeziona tutte le connessioni VPN per assicurarsi che abbiano lo stesso valore per `Static Routes Only.`
- VpnConnectionsCategory: Ispeziona tutte le connessioni VPN per assicurarsi che abbiano una categoria di. `VPN`
- VpnConnectionsCustomerConfiguration: Ispeziona tutte le connessioni VPN per assicurarsi che abbiano lo stesso valore per. `Customer Gateway Configuration`
- VpnConnectionsCustomerGatewayId: ispeziona ogni connessione VPN per assicurarsi che sia collegato un gateway per il cliente.
- VpnConnectionsRoutesState: ispeziona tutte le connessioni VPN per assicurarsi che siano in uno `AVAILABLE` stato.
- VpnConnectionsVgwTelemetryStatus: Ispeziona ogni connessione VPN per assicurarsi che abbia uno stato VGW pari a. `UP`
- VpnConnectionsVgwTelemetryIpAddress: Ispeziona ogni connessione VPN per assicurarsi che abbia un indirizzo IP esterno diverso per ogni telemetria VGW.
- VpnConnectionsTunnelOptions: Ispeziona tutte le connessioni VPN per assicurarsi che abbiano le stesse opzioni di tunnel.
- VpnConnectionsRoutesCidr: Ispeziona tutte le connessioni VPN per assicurarsi che abbiano gli stessi blocchi CIDR di destinazione.
- VpnConnectionsInstanceType: Ispeziona tutte le connessioni VPN per assicurarsi che abbiano le stesse. `Instance Type`

Site-to-Site VPN gateway

- VpnGatewayState: Ispeziona tutti i gateway VPN per assicurarsi che siano in uno stato DISPONIBILE.
- VpnGatewayAsn: Ispeziona tutti i gateway VPN per assicurarsi che abbiano lo stesso ASN.
- VpnGatewayType: Ispeziona tutti i gateway VPN per assicurarsi che abbiano lo stesso tipo.
- VpnGatewayAttachment: Ispeziona tutti i gateway VPN per assicurarsi che abbiano le stesse configurazioni di allegati.

Visualizza le regole di preparazione sulla console

È possibile visualizzare le regole di preparazione su Console di gestione AWS, elencate per ogni tipo di risorsa.

Per visualizzare le regole di preparazione sulla console

1. Apri la console ARC all'indirizzohttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Scegli Readiness check.
3. In Tipo di risorsa, scegli il tipo di risorsa per cui desideri visualizzare le regole.

Tipi di risorse e formati ARN in ARC

> **Note**
>
> La funzionalità di controllo della disponibilità in Amazon Application Recovery Controller (ARC) non sarà più aperta ai nuovi clienti a partire dal 30 aprile 2026. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta Amazon Application Recovery Controller (ARC) readiness check availability change.

Quando crei un set di risorse in Amazon Application Recovery Controller (ARC), specifichi il tipo di risorsa da includere nel set e Amazon Resource Names (ARNs) per ciascuna delle risorse da includere. ARC prevede un formato ARN specifico per ogni tipo di risorsa. Questa sezione elenca i tipi di risorse supportati da ARC e i formati ARN associati per ciascuno di essi.

Il formato specifico dipende dalla risorsa. Quando fornisci un ARN, sostituisci il *`italicized`* testo con le informazioni specifiche della risorsa.

> **Note**
>
> Tieni presente che il formato ARN richiesto da ARC per le risorse potrebbe differire dal formato ARN richiesto dal servizio stesso per le sue risorse. Ad esempio, i formati ARN descritti nelle sezioni Tipo di risorsa per ogni servizio nel Service Authorization Reference potrebbero non includere l' Account AWS ID o altre informazioni di cui ARC ha bisogno per supportare le funzionalità del servizio ARC.

AWS::ApiGateway::Stage

Una fase di Amazon API Gateway versione 1.

- Formato ARN: `arn:partition:apigateway:region:account:/restapis/api-id/stages/stage-name`

  Ad esempio: `arn:aws:apigateway:us-east-1:111122223333:/restapis/123456789/stages/ExampleStage`

  Per ulteriori informazioni, consulta API Gateway Amazon Resource Name (ARN) reference.

AWS::ApiGatewayV2::Stage

Una fase di Amazon API Gateway versione 2.

- Formato ARN: `arn:partition:apigateway:region:account:/apis/api-id/stages/stage-name`

  Ad esempio: `arn:aws:apigateway:us-east-1:111122223333:/apis/123456789/stages/ExampleStage`

  Per ulteriori informazioni, consulta API Gateway Amazon Resource Name (ARN) reference.

AWS::CloudWatch::Alarm

Un CloudWatch allarme Amazon.

- Formato ARN: `arn:partition:cloudwatch:region:account:alarm:alarm-name`

  Ad esempio: `arn:aws:cloudwatch:us-west-2:111122223333:alarm:test-alarm-1`

  Per ulteriori informazioni, consulta Tipi di risorse definiti da Amazon CloudWatch.

AWS::DynamoDB::Table

Una tabella Amazon DynamoDB.

- Formato ARN: `arn:partition:dynamodb:region:account:table/table-name`

  Ad esempio: `arn:aws:dynamodb:us-west-2:111122223333:table/BigTable`

  Per ulteriori informazioni, consulta Risorse e operazioni di DynamoDB.

AWS::EC2::CustomerGateway

Un dispositivo gateway per i clienti.

- Formato ARN: `arn:`*`partition`*`:ec2:`*`region`*`:`*`account`*`:customer-gateway/`*`CustomerGatewayId`*

  Ad esempio: `arn:aws:ec2:us-west-2:111122223333:customer-gateway/vcg-123456789`

  Per ulteriori informazioni, consulta Tipi di risorse definiti da Amazon EC2.

AWS::EC2::Volume

Un volume Amazon EBS.

- Formato ARN: `arn:`*`partition`*`:ec2:`*`region`*`:`*`account`*`:volume/`*`VolumeId`*

  Ad esempio: `arn:aws:ec2:us-west-2:111122223333:volume/volume-of-cylinder-is-pi`

  Per ulteriori informazioni, consulta API Gateway Amazon Resource Name (ARN) reference.

AWS::ElasticLoadBalancing::LoadBalancer

Un Load Balancer classico.

- Formato ARN: `arn:`*`partition`*`:elasticloadbalancing:`*`region`*`:`*`account`*`:loadbalancer/`*`LoadBalancerN`

  Ad esempio: `arn:aws:elasticloadbalancing:us-west-2:111122223333:loadbalancer/123456789abcbdeCLB`

  Per ulteriori informazioni, consulta le risorse di Elastic Load Balancing.

AWS::ElasticLoadBalancingV2::LoadBalancer

Un Network Load Balancer o un Application Load Balancer.

- Formato ARN per Network Load Balancer: `arn:`*`partition`*`:elasticloadbalancing:`*`region`*`:`*`account`*`:loadbalancer/net/`*`LoadBalancerName`*

  Esempio di Network Load Balancer: `arn:aws:elasticloadbalancing:us-west-2:111122223333:loadbalancer/net/sandbox-net/123456789acbdeNLB`
- Formato ARN per Application Load Balancer: `arn:`*`partition`*`:elasticloadbalancing:`*`region`*`:`*`account`*`:loadbalancer/app/`*`LoadBalancerName`*

Esempio di Application Load Balancer: `arn:aws:elasticloadbalancing:us-west-2:111122223333:loadbalancer/app/sandbox-alb/123456789acbdeALB`

Per ulteriori informazioni, consulta le risorse di Elastic Load Balancing.

AWS::Lambda::Function

Una AWS Lambda funzione.

- Formato ARN: `arn:`*`partition`*`:lambda:`*`region`*`:`*`account`*`:function:`*`FunctionName`*

  Ad esempio: `arn:aws:lambda:us-west-2:111122223333:function:my-function`

  Per ulteriori informazioni, consulta Risorse e condizioni per le azioni Lambda.

AWS::MSK::Cluster

UN cluster Amazon MSK.

- Formato ARN: `arn:`*`partition`*`:kafka:`*`region`*`:`*`account`*`:cluster/`*`ClusterName`*`/`*`UUID`*

  Ad esempio: `arn:aws:kafka:us-east-1:111122223333:cluster/demo-cluster-1/123456-1111-2222-3333`

  Per ulteriori informazioni, consulta Tipi di risorse definiti da Amazon Managed Streaming for Apache Kafka.

AWS::RDS::DBCluster

Un cluster Aurora DB.

- Formato ARN: `arn:`*`partition`*`:rds:`*`region`*`:`*`account`*`:cluster:`*`DbClusterInstanceName`*

  Ad esempio: `arn:aws:rds:us-west-2:111122223333:cluster:database-1`

  Per ulteriori informazioni, consulta Working with Amazon Resource Names (ARNs) in Amazon RDS.

AWS::Route53::HealthCheck

Un controllo dello stato di Amazon Route 53.

- Formato ARN: `arn:`*`partition`*`:route53:::healthcheck/`*`Id`*

  Ad esempio: `arn:aws:route53:::healthcheck/123456-1111-2222-3333`

AWS::SQS::Queue

Una coda Amazon SQS.

- Formato ARN: `arn:partition:sqs:region:account:QueueName`

  Ad esempio: `arn:aws:sqs:us-west-2:111122223333:StandardQueue`

  Per ulteriori informazioni, consulta le risorse e le operazioni di Amazon Simple Queue Service.

AWS::SNS::Topic

Argomento Amazon SNS

- Formato ARN: `arn:partition:sns:region:account:TopicName`

  Ad esempio: `arn:aws:sns:us-west-2:111122223333:TopicName`

  Per ulteriori informazioni, consulta il formato ARN delle risorse Amazon SNS.

AWS::SNS::Subscription

Un abbonamento Amazon SNS.

- Formato ARN: `arn:partition:sns:region:account:TopicName:SubscriptionId`

  Ad esempio: `arn:aws:sns:us-west-2:111122223333:TopicName:12345678901234567890`

AWS::EC2::VPC

Un virtual private cloud (VPC).

- Formato ARN: `arn:partition:ec2:region:account:vpc/VpcId`

  Ad esempio: `arn:aws:ec2:us-west-2:111122223333:vpc/vpc-123456789`

  Per ulteriori informazioni, consulta Risorse VPC.

AWS::EC2::VPNConnection

Una connessione di rete privata virtuale (VPN).

- Formato ARN: `arn:partition:ec2:region:account:vpn-connection/VpnConnectionId`

  Ad esempio: `arn:aws:ec2:us-west-2:111122223333:vpn-connection/vpn-123456789`

Per ulteriori informazioni, consulta Tipi di risorse definiti da Amazon EC2.

AWS::EC2::VPNGateway

Un gateway di rete privata virtuale (VPN).

- Formato ARN: `arn:partition:ec2:region:account:vpn-gateway/VpnGatewayId`

  Ad esempio: `arn:aws:ec2:us-west-2:111122223333:vpn-gateway/vgw-123456789acbdefgh`

  Per ulteriori informazioni, consulta Tipi di risorse definiti da Amazon EC2.

AWS::Route53RecoveryReadiness::DNSTargetResource

Una risorsa di destinazione DNS per i controlli di fattibilità include il tipo di record DNS, il nome di dominio, l'ARN della zona ospitata di Route 53 e l'ARN o l'ID del set di record Route 53 di Network Load Balancer.

- Formato ARN per la zona ospitata: `arn:partition:route53::account:hostedzone/Id`

  Esempio di una zona ospitata: `arn:aws:route53::111122223333:hostedzone/abcHostedZone`

  NOTA: è necessario includere l'ID dell'account nella zona ospitata ARNs, come specificato qui. L'ID dell'account è necessario affinché ARC possa interrogare la risorsa. Il formato è intenzionalmente diverso dal formato ARN richiesto da Amazon Route 53, descritto nei tipi di risorse del servizio Route 53 nel Service Authorization Reference.

- Formato ARN per Network Load Balancer: `arn:partition:elasticloadbalancing:region:account:loadbalancer/net/LoadBalancerName`

  Esempio di Network Load Balancer: `arn:aws:elasticloadbalancing:us-west-2:111122223333:loadbalancer/net/sandbox-net/123456789acbdefgh`

  Per ulteriori informazioni, consulta le risorse di Elastic Load Balancing.

Registrazione e monitoraggio per il controllo di fattibilità in Amazon Application Recovery Controller (ARC)

> **Note**
>
> La funzionalità di controllo della disponibilità in Amazon Application Recovery Controller (ARC) non sarà più aperta ai nuovi clienti a partire dal 30 aprile 2026. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta Amazon Application Recovery Controller (ARC) readiness check availability change.

Puoi utilizzare Amazon e Amazon CloudWatch EventBridge per monitorare il controllo di disponibilità in Amazon Application Recovery Controller (ARC), per analizzare i modelli e aiutare a risolvere i problemi. AWS CloudTrail

> **Note**
>
> È necessario visualizzare le CloudWatch metriche e i log per ARC nella regione Stati Uniti occidentali (Oregon), sia nella console che quando si utilizza. AWS CLI Quando utilizzi la AWS CLI, specifica la regione Stati Uniti occidentali (Oregon) per il comando includendo il seguente parametro:. `--region us-west-2`

Argomenti

- Utilizzo di Amazon CloudWatch con Readiness Check in ARC
- Registrazione delle chiamate API per il controllo della disponibilità utilizzando AWS CloudTrail
- Utilizzo del Readiness Check in ARC con Amazon EventBridge

Utilizzo di Amazon CloudWatch con Readiness Check in ARC

> **Note**
>
> La funzionalità di controllo della disponibilità in Amazon Application Recovery Controller (ARC) non sarà più aperta ai nuovi clienti a partire dal 30 aprile 2026. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta Amazon Application Recovery Controller (ARC) readiness check availability change.

Amazon Application Recovery Controller (ARC) pubblica punti dati su Amazon CloudWatch per i controlli di fattibilità. CloudWatch ti consente di recuperare le statistiche su tali punti dati sotto forma di un insieme ordinato di dati di serie temporali, noti come metriche. Pensa a un parametro come a una variabile da monitorare e ai dati di utilizzo come ai valori di questa variabile nel tempo. Ad esempio, è possibile monitorare il traffico attraverso una AWS regione in un periodo di tempo specificato. A ogni punto di dati sono associati un timestamp e un'unità di misura facoltativa.

Puoi utilizzare le metriche per verificare che le prestazioni del sistema siano quelle previste. Ad esempio, puoi creare un CloudWatch allarme per monitorare una metrica specifica e avviare un'azione (come l'invio di una notifica a un indirizzo e-mail) se la metrica supera quello che consideri un intervallo accettabile.

Per ulteriori informazioni, consulta la Amazon CloudWatch User Guide.

Argomenti

- Metriche ARC
- Statistiche per le metriche ARC
- Visualizza le CloudWatch metriche in ARC

Metriche ARC

Lo spazio dei nomi `AWS/Route53RecoveryReadiness` include le metriche descritte di seguito.

Metrica	Description
`ReadinessChecks`	Rappresenta il numero di controlli di conformità elaborati da ARC. La metrica può essere dimensionata in base ai suoi stati, elencati di seguito. Unità:. `Count` Criteri di segnalazione: vi è un valore diverso da zero. Statistiche: L'unica statistica utile è`Sum`. Dimensioni • `READY`

Metrica	Description
	• NOT_READY • NOT_AUTHORIZED • UNKNOWN
Resources	Rappresenta il numero di risorse elaborate da ARC, che possono essere dimensionate in base al relativo identificatore di risorsa, come definito dall'API. Unità:. Count Criteri di segnalazione: vi è un valore diverso da zero. Statistiche: L'unica statistica utile èSum. Dimensioni • ResourceSetType : Questi sono i tipi di risorse, filtrati in base al numero di risorse per tipo dato valutato da ARC Ad esempio: AWS::CloudWatch::Alarm

Statistiche per le metriche ARC

CloudWatch fornisce statistiche basate sui punti dati metrici pubblicati da ARC. Le statistiche sono aggregazioni di dati metrici su un periodo di tempo specificato. Quando richiedi le statistiche, il flusso di dati restituito viene identificato dal nome e dalla dimensione del parametro. Una dimensione è una name/value coppia che identifica in modo univoco una metrica.

Di seguito sono riportati alcuni esempi di metric/dimension combinazioni che potresti trovare utili:

- Visualizza il numero di controlli di preparazione valutati per quanto riguarda la disponibilità da ARC.
- Visualizza il numero totale di risorse per un determinato tipo di set di risorse valutato da ARC.

Visualizza le CloudWatch metriche in ARC

Puoi visualizzare le CloudWatch metriche per ARC utilizzando la CloudWatch console o il. AWS CLI Nella console, le metriche vengono visualizzate come grafici di monitoraggio.

È necessario visualizzare le CloudWatch metriche per ARC nella regione Stati Uniti occidentali (Oregon), sia nella console che quando si utilizza. AWS CLI Quando utilizzi la AWS CLI, specifica la regione Stati Uniti occidentali (Oregon) per il comando includendo il seguente parametro:. `--region us-west-2`

Per visualizzare le metriche utilizzando la console CloudWatch

1. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Nel riquadro di navigazione, seleziona Parametri.
3. Seleziona lo spazio dei nomi Route53 RecoveryReadiness.
4. (Opzionale) Per visualizzare tutte le dimensioni di un parametro, digitarne il nome nel campo di ricerca.

Per visualizzare le metriche utilizzando il AWS CLI

Utilizza il seguente comando list-metrics per elencare i parametri disponibili:

```
aws cloudwatch list-metrics --namespace AWS/Route53RecoveryReadiness --region us-west-2
```

Per ottenere le statistiche relative a una metrica, utilizzare il AWS CLI

Utilizzate il get-metric-statisticscomando seguente per ottenere le statistiche per una metrica e una dimensione specificate. Tieni presente che CloudWatch considera ogni combinazione unica di dimensioni come una metrica separata. Non puoi recuperare le statistiche utilizzando combinazioni di dimensioni che non sono state pubblicate specificamente. Occorre specificare le stesse dimensioni utilizzate al momento della creazione dei parametri.

L'esempio seguente elenca i controlli di fattibilità totali valutati, al minuto, per un account in ARC.

```
aws cloudwatch get-metric-statistics --namespace AWS/Route53RecoveryReadiness \
--metric-name ReadinessChecks \
--region us-west-2 \
--statistics Sum --period 60 \
--dimensions Name=State,Value=READY \
--start-time 2021-07-03T01:00:00Z --end-time 2021-07-03T01:20:00Z
```

Di seguito è riportato un esempio di output del comando:

```
{
```

```
    "Label": "ReadinessChecks",
    "Datapoints": [
        {
            "Timestamp": "2021-07-08T18:00:00Z",
            "Sum": 1.0,
            "Unit": "Count"
        },
        {
            "Timestamp": "2021-07-08T18:04:00Z",
            "Sum": 1.0,
            "Unit": "Count"
        },
        {
            "Timestamp": "2021-07-08T18:01:00Z",
            "Sum": 1.0,
            "Unit": "Count"
        },
        {
            "Timestamp": "2021-07-08T18:02:00Z",
            "Sum": 1.0,
            "Unit": "Count"
        },
        {
            "Timestamp": "2021-07-08T18:03:00Z",
            "Sum": 1.0,
            "Unit": "Count"
        }
    ]
}
```


Registrazione delle chiamate API per il controllo della disponibilità utilizzando AWS CloudTrail

> **Note**
>
> La funzionalità di controllo della disponibilità in Amazon Application Recovery Controller (ARC) non sarà più aperta ai nuovi clienti a partire dal 30 aprile 2026. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta Amazon Application Recovery Controller (ARC) readiness check availability change.

è integrato con AWS CloudTrail, un servizio che fornisce una registrazione delle azioni intraprese da un utente, ruolo o AWS servizio in ARC. CloudTrail acquisisce tutte le chiamate API per ARC come eventi. Le chiamate acquisite includono chiamate dalla console ARC e chiamate in codice alle operazioni dell'API ARC.

Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per ARC. 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, è possibile determinare la richiesta che è stata effettuata ad ARC, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e ulteriori dettagli.

Per ulteriori informazioni CloudTrail, consulta la Guida AWS CloudTrail per l'utente.

Informazioni ARC in CloudTrail

CloudTrail è abilitato sul tuo account al Account AWS momento della creazione dell'account. Quando si verifica un'attività in ARC, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi AWS di servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare eventi recenti in Account AWS. Per ulteriori informazioni, consulta Lavorare con la cronologia CloudTrail degli eventi.

Per una registrazione continua degli eventi del tuo Account AWS, compresi gli eventi per ARC, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando si crea un percorso nella console, questo sarà valido in tutte le Regioni AWS. Il trail registra gli eventi di tutte le regioni della AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica della creazione di un percorso
- CloudTrail servizi e integrazioni supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di CloudTrail registro da più regioni e ricezione di file di CloudTrail registro da più account

Tutte le azioni ARC vengono registrate CloudTrail e sono documentate nella Recovery Readiness API Reference Guide per Amazon Application Recovery Controller, nella Recovery Control

Configuration API Reference Guide per Amazon Application Recovery Controller e nella Routing Control API Recovery Guide per Amazon Application Recovery Controller. Ad esempio, le chiamate `UpdateRoutingControlState` e le `CreateRecoveryGroup` azioni generano voci nei file di registro. `CreateCluster` CloudTrail

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con credenziali utente root o AWS Identity and Access Management (IAM).
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro AWS servizio.

Per ulteriori informazioni, consulta Elemento CloudTrail userIdentity.

Visualizzazione degli eventi ARC nella cronologia degli eventi

CloudTrail consente di visualizzare gli eventi recenti nella cronologia degli eventi. Per visualizzare gli eventi per le richieste API ARC, devi scegliere US West (Oregon) nel selettore di regione nella parte superiore della console. Per ulteriori informazioni, consulta Lavorare con la cronologia CloudTrail degli eventi nella Guida per l'AWS CloudTrail utente.

Comprendere le voci dei file di registro ARC

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'`CreateRecoveryGroup`azione per il controllo di prontezza.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
```

```
        "arn": "arn:aws:iam::111122223333:role/admin",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROA33L3W36EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/admin",
                "accountId": "111122223333",
                "userName": "EXAMPLENAME"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2021-07-06T17:38:05Z"
            }
        }
    },
    "eventTime": "2021-07-06T18:08:03Z",
    "eventSource": "route53-recovery-readiness.amazonaws.com",
    "eventName": "CreateRecoveryGroup",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.50",
    "userAgent": "Boto3/1.17.101 Python/3.8.10 Linux/4.14.231-180.360.amzn2.x86_64
 exec-env/AWS_Lambda_python3.8 Botocore/1.20.102",
    "requestParameters": {
        "recoveryGroupName": "MyRecoveryGroup"
    },
    "responseElements": {
        "Access-Control-Expose-Headers": "x-amzn-errortype,x-amzn-requestid,x-amzn-
errormessage,x-amzn-trace-id,x-amzn-requestid,x-amz-apigw-id,date",
        "cells": [],
        "recoveryGroupName": "MyRecoveryGroup",
        "recoveryGroupArn": "arn:aws:route53-recovery-readiness::111122223333:recovery-
group/MyRecoveryGroup",
        "tags": "***"
    },
    "requestID": "fd42dcf7-6446-41e9-b408-d096example",
    "eventID": "4b5c42df-1174-46c8-be99-d67aexample",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333"
```

```
}
```

Utilizzo del Readiness Check in ARC con Amazon EventBridge

> **Note**
>
> La funzionalità di controllo della disponibilità in Amazon Application Recovery Controller (ARC) non sarà più aperta ai nuovi clienti a partire dal 30 aprile 2026. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta Amazon Application Recovery Controller (ARC) readiness check availability change.

Con Amazon EventBridge, puoi configurare regole basate sugli eventi che monitorano la tua disponibilità, controllano le risorse in Amazon Application Recovery Controller (ARC) e quindi avviare azioni mirate che utilizzano altri servizi. AWS Ad esempio, puoi impostare una regola per l'invio di notifiche e-mail segnalando un argomento di Amazon SNS quando lo stato di un controllo di disponibilità cambia da READY a NOT READY.

> **Note**
>
> ARC pubblica solo EventBridge eventi per il controllo della disponibilità nella regione Stati Uniti occidentali (Oregon) (us-west-2). AWS Per ricevere EventBridge gli eventi per il controllo di disponibilità, create EventBridge delle regole nella regione Stati Uniti occidentali (Oregon).

Puoi creare regole in Amazon EventBridge per agire sul seguente evento di verifica della disponibilità ARC:

- Prontezza del controllo di prontezza. L'evento specifica se lo stato del controllo di prontezza cambia, ad esempio, da READY a NOT READY.

Per acquisire eventi ARC specifici che ti interessano, definisci modelli specifici dell'evento da EventBridge utilizzare per rilevare gli eventi. I pattern di eventi hanno la stessa struttura degli eventi a cui corrispondono. Il modello cita i campi che desideri abbinare e fornisce i valori che stai cercando.

Gli eventi vengono emessi secondo il principio del massimo sforzo. Vengono trasmessi da ARC a quasi EventBridge in tempo reale in normali circostanze operative. Tuttavia, possono verificarsi situazioni che potrebbero ritardare o impedire la consegna di un evento.

Per informazioni su come EventBridge le regole funzionano con i modelli di eventi, consulta Eventi e modelli di eventi in EventBridge.

Monitora una risorsa per il controllo di fattibilità con EventBridge

Con EventBridge, puoi creare regole che definiscono le azioni da intraprendere quando ARC emette eventi per le risorse di controllo della prontezza.

Per digitare o copiare e incollare un pattern di eventi nella EventBridge console, nella console, seleziona l'opzione Inserisci la mia opzione. Per aiutarvi a determinare i modelli di eventi che potrebbero esservi utili, questo argomento include esempi di modelli di eventi di preparazione.

Per creare una regola per un evento risorsa

1. Apri la EventBridge console Amazon all'indirizzo https://console.aws.amazon.com/events/.
2. Per Regione AWS creare la regola, scegli US West (Oregon). Questa è la regione richiesta per gli eventi di preparazione.
3. Scegliere Create rule (Crea regola).
4. Immettere un Name (Nome) per la regola e, facoltativamente, una descrizione.
5. Per Event bus, lascia il valore predefinito, default.
6. Scegli Next (Successivo).
7. Per il passo Build event pattern, per Event source, lascia il valore predefinito, AWS events.
8. In Evento di esempio, scegli Inserisci il mio.
9. Per gli eventi di esempio, digita o copia e incolla un modello di evento. Per alcuni esempi, consultate la sezione successiva.

Esempi di modelli di eventi di prontezza

I modelli di eventi hanno la stessa struttura degli eventi a cui corrispondono. Il modello cita i campi che desideri abbinare e fornisce i valori che stai cercando.

È possibile copiare e incollare i modelli di eventi da questa sezione EventBridge per creare regole da utilizzare per monitorare le azioni e le risorse ARC.

I seguenti modelli di eventi forniscono esempi che è possibile utilizzare EventBridge per la funzionalità di controllo di fattibilità in ARC.

- Seleziona tutti gli eventi dal controllo di fattibilità ARC.

```
{
    "source": [
        "aws.route53-recovery-readiness"
    ]
}
```

- Seleziona solo gli eventi relativi alle celle.

```
{
    "source": [
        "aws.route53-recovery-readiness"
    ],
    "detail-type": [
        "Route 53 Application Recovery Controller cell readiness status change"
    ]
}
```

- Seleziona solo gli eventi relativi a una cella specifica chiamata *`MyExampleCell`*.

```
{
    "source": [
        "aws.route53-recovery-readiness"
    ],
    "detail-type": [
        "Route 53 Application Recovery Controller cell readiness status change"
    ],
    "resources": [
        "arn:aws:route53-recovery-readiness::111122223333:cell/MyExampleCell"
    ]
}
```

- Seleziona solo gli eventi in cui viene raggiunto lo stato di un gruppo di ripristino, di una cella o di un controllo di fattibilità. `NOT READY`

```
{
   "source":[
      "aws.route53-recovery-readiness"
   ],
   "detail-type":{
      "new-state":{
         "readiness-status":[
```

```
            "NOT_READY"
         ]
      }
   }
}
```

- Seleziona solo gli eventi in cui un gruppo di ripristino, una cella o un controllo di fattibilità diventa qualcosa tranne *READY*

```
{
   "source":[
      "aws.route53-recovery-readiness"
   ],
   "detail":{
      "new-state":{
         "readiness-status":[
            {
               "anything-but":"READY"
            }
         ]
      }
   }
}
```

Di seguito è riportato un esempio di evento ARC relativo alla modifica dello stato di preparazione di un gruppo di ripristino:

```
{
    "version": "0",
    "account":"111122223333",
    "detail-type":"Route 53 Application Recovery Controller recovery group readiness
 status change",
    "source":"route53-recovery-readiness.amazonaws.com",
    "time":"2020-11-03T00:31:54Z",
    "id": "1234a678-1b23-c123-12fd3f456e78",
    "region": "us-west-2",
    "resources":[
        "arn:aws:route53-recovery-readiness::111122223333:recovery-group/BillingApp"
    ],
    "detail": {
        "recovery-group-name": "BillingApp",
        "previous-state": {
```

```
            "readiness-status": "READY|NOT_READY|UNKNOWN|NOT_AUTHORIZED"
        },
        "new-state": {
            "readiness-status": "READY|NOT_READY|UNKNOWN|NOT_AUTHORIZED"
        }
    }
}
```

Di seguito è riportato un esempio di evento ARC relativo alla modifica dello stato di disponibilità di una cella:

```
{
    "version": "0",
    "account":"111122223333",
    "detail-type":"Route 53 Application Recovery Controller cell readiness status
 change",
    "source":"route53-recovery-readiness.amazonaws.com",
    "time":"2020-11-03T00:31:54Z",
    "id": "1234a678-1b23-c123-12fd3f456e78",
    "region": "us-west-2",
    "resources":[
        "arn:aws:route53-recovery-readiness::111122223333:cell/PDXCell"
    ],
    "detail": {
        "cell-name": "PDXCell",
        "previous-state": {
            "readiness-status": "READY|NOT_READY|UNKNOWN|NOT_AUTHORIZED"
        },
        "new-state": {
            "readiness-status": "READY|NOT_READY|UNKNOWN|NOT_AUTHORIZED"
        }
    }
}
```

Di seguito è riportato un esempio di evento ARC relativo alla modifica dello stato di un controllo di prontezza:

```
{
    "version": "0",
    "account":"111122223333",
    "detail-type":"Route 53 Application Recovery Controller readiness check status
 change",
```

```
    "source":"route53-recovery-readiness.amazonaws.com",
    "time":"2020-11-03T00:31:54Z",
    "id": "1234a678-1b23-c123-12fd3f456e78",
    "region": "us-west-2",
    "resources":[
        "arn:aws:route53-recovery-readiness::111122223333:readiness-check/
UserTableReadinessCheck"
    ],
    "detail": {
    "readiness-check-name": "UserTableReadinessCheck",
        "previous-state": {
            "readiness-status": "READY|NOT_READY|UNKNOWN|NOT_AUTHORIZED"
        },
        "new-state": {
            "readiness-status": "READY|NOT_READY|UNKNOWN|NOT_AUTHORIZED"
        }
    }
}
```

Specificate un gruppo di CloudWatch log da utilizzare come destinazione

Quando si crea una EventBridge regola, è necessario specificare la destinazione a cui vengono inviati gli eventi corrispondenti alla regola. Per un elenco degli obiettivi disponibili per EventBridge, vedi Target disponibili nella EventBridge console. Uno degli obiettivi che puoi aggiungere a una EventBridge regola è un gruppo di CloudWatch log Amazon. Questa sezione descrive i requisiti per aggiungere gruppi di CloudWatch log come destinazioni e fornisce una procedura per aggiungere un gruppo di log quando si crea una regola.

Per aggiungere un gruppo di CloudWatch log come destinazione, è possibile effettuare una delle seguenti operazioni:

- Creare un nuovo gruppo di log
- Scegli un gruppo di log esistente

Se specifichi un nuovo gruppo di log utilizzando la console quando crei una regola, crea EventBridge automaticamente il gruppo di log per te. Assicurati che il gruppo di log che usi come destinazione per la EventBridge regola inizi con`/aws/events`. Se desideri scegliere un gruppo di log esistente, tieni presente che solo i gruppi di log che iniziano con `/aws/events` appaiono come opzioni nel menu a discesa. Per ulteriori informazioni, consulta Creare un nuovo gruppo di log nella Amazon CloudWatch User Guide.

Se crei o utilizzi un gruppo di CloudWatch log da utilizzare come destinazione utilizzando CloudWatch operazioni esterne alla console, assicurati di impostare le autorizzazioni correttamente. Se utilizzi la console per aggiungere un gruppo di log a una EventBridge regola, la politica basata sulle risorse per il gruppo di log viene aggiornata automaticamente. Tuttavia, se si utilizza AWS Command Line Interface o un AWS SDK per specificare un gruppo di log, è necessario aggiornare la politica basata sulle risorse per il gruppo di log. La seguente politica di esempio illustra le autorizzazioni che è necessario definire in una politica basata sulle risorse per il gruppo di log:

JSON

```
{
    "Version":"2012-10-17",

    "Statement": [
        {
            "Action": [
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "events.amazonaws.com",
                    "delivery.logs.amazonaws.com"
                ]
            },
            "Resource": "arn:aws:logs:us-east-1:222222222222:log-group:/aws/
events/*:*",
            "Sid": "TrustEventsToStoreLogEvent"
        }
    ]
}
```

Non è possibile configurare una politica basata sulle risorse per un gruppo di log utilizzando la console. Per aggiungere le autorizzazioni richieste a una politica basata sulle risorse, utilizza l'operazione API. CloudWatch PutResourcePolicy Quindi, puoi utilizzare il comando describe-resource-policiesCLI per verificare che la tua politica sia stata applicata correttamente.

Per creare una regola per un evento di risorsa e specificare un target per un gruppo di CloudWatch log

1. Apri la EventBridge console Amazon all'indirizzo https://console.aws.amazon.com/events/.
2. Scegli Regione AWS quello in cui vuoi creare la regola.
3. Scegli Crea regola e inserisci tutte le informazioni su quella regola, come lo schema dell'evento o i dettagli della pianificazione.

   Per ulteriori informazioni sulla creazione di EventBridge regole di preparazione, consulta Monitorare una risorsa per il controllo di prontezza con. EventBridge
4. Nella pagina Seleziona destinazione, scegli CloudWatchcome obiettivo.
5. Scegli un gruppo di CloudWatch log dal menu a discesa.

Identity and Access Management per il controllo di idoneità in ARC

> **Note**
>
> La funzionalità di controllo della disponibilità in Amazon Application Recovery Controller (ARC) non sarà più aperta ai nuovi clienti a partire dal 30 aprile 2026. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta Amazon Application Recovery Controller (ARC) readiness check availability change.

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

Indice

- In che modo il controllo di disponibilità in Amazon Application Recovery Controller (ARC) funziona con IAM
- Esempi di policy basate sull'identità per il controllo di idoneità in ARC
- Utilizzo del ruolo collegato al servizio per il controllo di disponibilità in ARC
- AWS politiche gestite per il controllo della disponibilità in ARC

In che modo il controllo di disponibilità in Amazon Application Recovery Controller (ARC) funziona con IAM

Prima di utilizzare IAM per gestire l'accesso ad ARC, scopri quali funzionalità IAM sono disponibili per l'uso con ARC.

Prima di utilizzare IAM per gestire l'accesso al controllo di fattibilità in Amazon Application Recovery Controller (ARC), scopri quali funzionalità IAM sono disponibili per l'uso con Readiness Check.

Funzionalità IAM che puoi utilizzare con Readiness Check in Amazon Application Recovery Controller (ARC)

Funzionalità IAM	Supporto per il controllo di disponibilità
Policy basate sull'identità	Sì
Policy basate su risorse	No
Operazioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione delle policy	Sì
ACLs	No
ABAC (tag nelle policy)	Sì
Credenziali temporanee	Sì
Autorizzazioni del principale	Sì
Ruoli di servizio	No
Ruoli collegati al servizio	Sì

Per avere una panoramica generale di alto livello su come AWS i 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 il controllo di idoneità

Supporta le policy basate sull'identità: sì

Le policy basate sull'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 di IAM.

Con le policy basate sull'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. 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 IAM.

Per visualizzare esempi di politiche ARC basate sull'identità, vedere. Esempi di policy basate sull'identità in Amazon Application Recovery Controller (ARC)

Politiche basate sulle risorse nell'ambito del controllo di fattibilità

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 di 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.

Azioni politiche per il controllo della prontezza

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 entità 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 in una policy. Includere le operazioni in una policy per concedere le autorizzazioni di eseguire l'operazione associata.

Per visualizzare un elenco delle azioni ARC per il controllo della fattibilità, consulta Azioni definite da Amazon Route 53 Recovery Readiness nel Service Authorization Reference.

Le azioni politiche in ARC for Readiness Check utilizzano i seguenti prefissi prima dell'azione:

```
route53-recovery-readiness
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola. Ad esempio, quanto segue:

```
"Action": [
      "route53-recovery-readiness:action1",
      "route53-recovery-readiness:action2"
         ]
```

È possibile specificare più azioni tramite caratteri jolly (*). Ad esempio, per specificare tutte le azioni che iniziano con la parola `Describe`, includi la seguente azione:

```
"Action": "route53-recovery-readiness:Describe*"
```

Per visualizzare esempi di politiche ARC basate sull'identità per il controllo di idoneità, vedere. Esempi di policy basate sull'identità per il controllo di idoneità in ARC

Risorse politiche per il controllo di idoneità

Supporta le risorse relative alle policy: sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità 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. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). Per le azioni che non supportano le autorizzazioni a livello di risorsa, si utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

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

Per visualizzare un elenco di azioni ARC per lo spostamento di zona, consulta Azioni definite da Amazon Route 53 Recovery Readiness.

Per visualizzare esempi di politiche ARC basate sull'identità per il controllo della disponibilità, consulta. Esempi di policy basate sull'identità per il controllo di idoneità in ARC

Chiavi relative alle condizioni delle policy per il controllo di idoneità

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 entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento `Condition` specifica quando le istruzioni vengono eseguite in base a criteri definiti. 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. 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 di azioni ARC per il controllo della fattibilità, consulta Condition keys for Amazon Route 53 Recovery Readiness

Per visualizzare le azioni e le risorse che puoi utilizzare con una chiave di condizione con controllo di fattibilità, consulta Azioni definite da Amazon Route 53 Recovery Readiness

Per visualizzare esempi di politiche ARC basate sull'identità per il controllo di fattibilità, consulta. Esempi di policy basate sull'identità per il controllo di idoneità in ARC

Accedete agli elenchi di controllo () ACLs durante il controllo di fattibilità

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.

Controllo degli accessi basato sugli attributi (ABAC) con controllo di prontezza

Supporta ABAC (tag nelle policy): parzialmente

Il controllo degli accessi basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi, chiamati tag. Puoi allegare tag a entità e AWS risorse IAM, quindi progettare politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag sulla risorsa.

Per controllare l'accesso basato su tag, fornire 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 Sì. Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per maggiori informazioni su ABAC, consulta Definizione delle autorizzazioni con autorizzazione ABAC nella Guida per l'utente di 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.

Recovery Readiness (Readiness check) supporta ABAC.

Utilizzo di credenziali temporanee con controllo di prontezza

Supporta le credenziali temporanee: sì

Le credenziali temporanee forniscono l'accesso a breve termine alle AWS risorse e vengono create automaticamente quando si utilizza la federazione o si cambia ruolo. AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza temporanee in IAM e Servizi AWS compatibili con IAM nella Guida per l'utente IAM.

Autorizzazioni principali trasversali per il controllo di idoneità

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

Quando utilizzi un'entità IAM (utente o ruolo) per eseguire azioni AWS, sei considerato un principale. Le policy concedono autorizzazioni a un'entità. Quando si utilizzano alcuni servizi, è possibile eseguire un'azione che attiva un'altra azione in un servizio diverso. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni.

Per verificare se un'azione in fase di verifica della prontezza richiede ulteriori azioni dipendenti in una policy, consulta Amazon Route 53 Recovery Readiness

Ruoli di servizio per il controllo di fattibilità

Supporta i ruoli di servizio: no

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.

Ruoli collegati ai servizi per il controllo di fattibilità

Supporta i ruoli collegati ai servizi: sì

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'operazione 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 al servizio, ma non modificarle.

Per informazioni dettagliate sulla creazione o la gestione di ruoli collegati ai servizi ARC, consulta. Utilizzo del ruolo collegato al servizio per il controllo di disponibilità in ARC

Per ulteriori informazioni su come creare e gestire i ruoli collegati ai servizi, consulta Servizi AWS supportati da IAM. Trova un servizio nella tabella che include un `Yes` nella colonna Service-linked role (Ruolo collegato ai servizi). Scegli il collegamento Sì per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Esempi di policy basate sull'identità per il controllo di idoneità in ARC

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare risorse ARC. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM.

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 di IAM.

Per dettagli sulle azioni e sui tipi di risorse definiti da ARC, incluso il formato di ARNs per ogni tipo di risorsa, consulta Azioni, risorse e chiavi di condizione per Amazon Application Recovery Controller (ARC) nel Service Authorization Reference.

Argomenti

- Best practice per le policy
- Esempio: accesso alla console di Readiness Check
- Esempi: azioni dell'API Readiness Check per il controllo di prontezza

Best practice per le policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare le risorse ARC nel tuo account. Queste operazioni possono comportare costi aggiuntivi per l' Account AWS. Quando si creano o modificano policy basate sull'identità, seguire 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 maggiori informazioni, consulta Policy gestite da AWS o Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente di IAM.

- Applicazione delle autorizzazioni con privilegio minimo - Quando si impostano le autorizzazioni con le policy IAM, concedere 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 privilegio minimo. Per maggiori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso - Per limitare l'accesso ad azioni e risorse è possibile aggiungere una condizione alle 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 CloudFormation. Per maggiori informazioni, consultare la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente di IAM.
- Utilizzo dello strumento di analisi degli accessi IAM per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali - Lo strumento di analisi degli accessi IAM convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio (JSON) della policy IAM e alle best practice di IAM. Lo strumento di analisi degli accessi IAM offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per maggiori informazioni, consultare Convalida delle policy per il Sistema di analisi degli accessi IAM nella Guida per l'utente di 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, aggiungere le condizioni MFA alle policy. Per maggiori informazioni, consultare Protezione dell'accesso API con MFA nella Guida per l'utente di IAM.

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

Esempio: accesso alla console di Readiness Check

Per accedere alla console Amazon Application Recovery Controller (ARC), devi disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle risorse ARC 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 agli utenti che effettuano chiamate solo verso AWS CLI o l' AWS API. Al contrario, è opportuno concedere l'accesso solo alle azioni che corrispondono all'operazione API che stanno cercando di eseguire.

Per garantire che utenti e ruoli possano ancora utilizzare la console di controllo della fattibilità quando consenti l'accesso solo a operazioni API specifiche, allega anche una policy `ReadOnly` AWS gestita per il controllo di fattibilità alle entità. Per ulteriori informazioni, consulta la pagina Readiness check Readiness check managed policies o Adding permissions to a user nella IAM User Guide.

Per eseguire alcune attività, gli utenti devono disporre dell'autorizzazione per creare il ruolo collegato al servizio associato al controllo di preparazione in ARC. Per ulteriori informazioni, consulta Utilizzo del ruolo collegato al servizio per il controllo di disponibilità in ARC.

Per consentire agli utenti l'accesso completo all'utilizzo delle funzionalità di controllo della disponibilità tramite la console, allega all'utente una politica come la seguente:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                   "route53-recovery-readiness:CreateCell",
                   "route53-recovery-readiness:CreateCrossAccountAuthorization",
                   "route53-recovery-readiness:CreateReadinessCheck",
                   "route53-recovery-readiness:CreateRecoveryGroup",
                   "route53-recovery-readiness:CreateResourceSet",
                   "route53-recovery-readiness:DeleteCell",
                   "route53-recovery-readiness:DeleteCrossAccountAuthorization",
                   "route53-recovery-readiness:DeleteReadinessCheck",
                   "route53-recovery-readiness:DeleteRecoveryGroup",
                   "route53-recovery-readiness:DeleteResourceSet",
                   "route53-recovery-readiness:GetArchitectureRecommendations",
                   "route53-recovery-readiness:GetCell",
                   "route53-recovery-readiness:GetCellReadinessSummary",
                   "route53-recovery-readiness:GetReadinessCheck",
                   "route53-recovery-readiness:GetReadinessCheckResourceStatus",
```

```
                "route53-recovery-readiness:GetReadinessCheckStatus",
                "route53-recovery-readiness:GetRecoveryGroup",
                "route53-recovery-readiness:GetRecoveryGroupReadinessSummary",
                "route53-recovery-readiness:GetResourceSet",
                "route53-recovery-readiness:ListCells",
                "route53-recovery-readiness:ListCrossAccountAuthorizations",
                "route53-recovery-readiness:ListReadinessChecks",
                "route53-recovery-readiness:ListRecoveryGroups",
                "route53-recovery-readiness:ListResourceSets",
                "route53-recovery-readiness:ListRules",
                "route53-recovery-readiness:UpdateCell",
                "route53-recovery-readiness:UpdateReadinessCheck",
                "route53-recovery-readiness:UpdateRecoveryGroup",
                "route53-recovery-readiness:UpdateResourceSet"
            ],
            "Resource": "*"
        }
    ]
}
```

Esempi: azioni dell'API Readiness Check per il controllo di prontezza

Per garantire che un utente possa utilizzare le azioni dell'API ARC per lavorare con il piano di controllo ARC Readiness Check, ad esempio per creare gruppi di ripristino, set di risorse e controlli di fattibilità, allega una policy che corrisponda alle operazioni API con cui l'utente deve lavorare, come descritto di seguito.

Per eseguire alcune attività, gli utenti devono disporre dell'autorizzazione per creare il ruolo collegato al servizio associato al controllo della disponibilità in ARC. Per ulteriori informazioni, consulta Utilizzo del ruolo collegato al servizio per il controllo di disponibilità in ARC.

Per utilizzare le operazioni API per il controllo della fattibilità, allega all'utente una policy come la seguente:

JSON

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

```
            "Action": [
                  "route53-recovery-readiness:CreateCell",
                  "route53-recovery-readiness:CreateCrossAccountAuthorization",
                  "route53-recovery-readiness:CreateReadinessCheck",
                  "route53-recovery-readiness:CreateRecoveryGroup",
                  "route53-recovery-readiness:CreateResourceSet",
                  "route53-recovery-readiness:DeleteCell",
                  "route53-recovery-readiness:DeleteCrossAccountAuthorization",
                  "route53-recovery-readiness:DeleteReadinessCheck",
                  "route53-recovery-readiness:DeleteRecoveryGroup",
                  "route53-recovery-readiness:DeleteResourceSet",
                  "route53-recovery-readiness:GetArchitectureRecommendations",
                  "route53-recovery-readiness:GetCell",
                  "route53-recovery-readiness:GetCellReadinessSummary",
                  "route53-recovery-readiness:GetReadinessCheck",
                  "route53-recovery-readiness:GetReadinessCheckResourceStatus",
                  "route53-recovery-readiness:GetReadinessCheckStatus",
                  "route53-recovery-readiness:GetRecoveryGroup",
                  "route53-recovery-readiness:GetRecoveryGroupReadinessSummary",
                  "route53-recovery-readiness:GetResourceSet",
                  "route53-recovery-readiness:ListCells",
                  "route53-recovery-readiness:ListCrossAccountAuthorizations",
                  "route53-recovery-readiness:ListReadinessChecks",
                  "route53-recovery-readiness:ListRecoveryGroups",
                  "route53-recovery-readiness:ListResourceSets",
                  "route53-recovery-readiness:ListRules",
                  "route53-recovery-readiness:ListTagsForResources",
                  "route53-recovery-readiness:UpdateCell",
                  "route53-recovery-readiness:UpdateReadinessCheck",
                  "route53-recovery-readiness:UpdateRecoveryGroup",
                  "route53-recovery-readiness:UpdateResourceSet",
                  "route53-recovery-readiness:TagResource",
                  "route53-recovery-readiness:UntagResource"
             ],
            "Resource": "*"
        }
    ]
}
```

Utilizzo del ruolo collegato al servizio per il controllo di disponibilità in ARC

Amazon Application Recovery Controller utilizza AWS Identity and Access Management ruoli collegati ai servizi (IAM). Un ruolo collegato al servizio è un tipo unico di ruolo IAM collegato direttamente a un servizio, in questo caso ARC. I ruoli collegati ai servizi sono predefiniti da ARC e includono tutte le autorizzazioni richieste dal servizio per chiamare altri AWS servizi per conto dell'utente per scopi specifici.

I ruoli collegati ai servizi semplificano la configurazione di ARC perché non è necessario aggiungere manualmente le autorizzazioni necessarie. ARC definisce le autorizzazioni dei suoi ruoli collegati ai servizi e, se non diversamente definito, solo ARC può assumerne i ruoli. Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere collegata a nessun'altra entità IAM.

È possibile eliminare un ruolo collegato ai servizi solo dopo aver eliminato le risorse correlate. Questo protegge le tue risorse ARC perché non puoi rimuovere inavvertitamente l'autorizzazione ad accedere alle risorse.

Per informazioni su altri servizi che supportano i ruoli collegati ai servizi, consulta AWS Servizi che funzionano con IAM e cerca i servizi con Sì nella colonna Ruolo collegato ai servizi. Scegli Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

ARC ha i seguenti ruoli collegati ai servizi, descritti in questo capitolo:

- ARC utilizza il ruolo collegato al servizio denominato Route53 RecoveryReadinessServiceRolePolicy per accedere a risorse e configurazioni per verificare la disponibilità.
- ARC utilizza il ruolo collegato al servizio denominato autoshift practice run, per monitorare gli CloudWatch allarmi Amazon e gli eventi dei clienti forniti dai clienti Health Dashboard e per avviare le sessioni pratiche.

Autorizzazioni di ruolo collegate al servizio per Route53 RecoveryReadinessServiceRolePolicy

ARC utilizza un ruolo collegato al servizio denominato Route53 RecoveryReadinessServiceRolePolicy per accedere a risorse e configurazioni per verificare la disponibilità. Questa sezione descrive le autorizzazioni per il ruolo collegato al servizio e le informazioni sulla creazione, la modifica e l'eliminazione del ruolo.

Autorizzazioni di ruolo collegate al servizio per Route53 RecoveryReadinessServiceRolePolicy

Questo ruolo collegato al servizio utilizza la policy gestita. `Route53RecoveryReadinessServiceRolePolicy`

Il ruolo RecoveryReadinessServiceRolePolicy collegato al servizio Route53 si affida al seguente servizio per l'assunzione del ruolo:

- `route53-recovery-readiness.amazonaws.com`

Per visualizzare le autorizzazioni per questa politica, consulta RecoveryReadinessServiceRolePolicyRoute53 nel Managed Policy Reference.AWS

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Creazione del ruolo collegato al servizio Route53 per ARC RecoveryReadinessServiceRolePolicy

Non è necessario creare manualmente il ruolo collegato al servizio Route53. RecoveryReadinessServiceRolePolicy Quando create il primo controllo di conformità o l'autorizzazione tra account nella, nella o nell' AWS API Console di gestione AWS, ARC crea automaticamente il ruolo collegato al servizio. AWS CLI

Se elimini questo ruolo collegato ai servizi, è possibile ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Quando crei il primo controllo di conformità o l'autorizzazione tra account, ARC crea nuovamente il ruolo collegato al servizio per te.

Modifica del ruolo collegato al servizio Route53 per ARC RecoveryReadinessServiceRolePolicy

ARC non consente di modificare il ruolo collegato al servizio Route53. RecoveryReadinessServiceRolePolicy Dopo aver creato il ruolo collegato al servizio, non è possibile modificare il nome del ruolo perché altre entità potrebbero fare riferimento al ruolo. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Eliminazione del ruolo collegato al servizio Route53 RecoveryReadinessServiceRolePolicy per ARC

Se non è più necessario utilizzare una funzionalità o un servizio che richiede un ruolo collegato al servizio, ti consigliamo di eliminare il ruolo. In questo modo non sarà più presente un'entità non

utilizzata che non viene monitorata e gestita attivamente. Tuttavia, è necessario effettuare la pulizia delle risorse associate al ruolo collegato al servizio prima di poterlo eliminare manualmente.

Dopo aver rimosso i controlli di conformità e le autorizzazioni tra account, puoi eliminare il ruolo collegato al servizio di Route53. RecoveryReadinessServiceRolePolicy Per ulteriori informazioni sui controlli di idoneità, vedere. Controllo di prontezza in ARC Per ulteriori informazioni sulle autorizzazioni tra account, vedere. Creazione di autorizzazioni per più account in ARC

> **Note**
>
> Se il servizio ARC utilizza il ruolo quando si tenta di eliminare le risorse, l'eliminazione del ruolo di servizio potrebbe non riuscire. In tal caso, attendi qualche minuto e riprova a eliminare il ruolo.

Per eliminare manualmente il ruolo collegato ai servizi mediante IAM

Utilizza la console IAM AWS CLI, o l' AWS API per eliminare il ruolo collegato al RecoveryReadinessServiceRolePolicy servizio Route53. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato al servizio nella Guida per l'utente di IAM.

Aggiornamenti al ruolo collegato al servizio ARC per il controllo di idoneità

Per gli aggiornamenti alle politiche AWS gestite per i ruoli collegati ai servizi ARC, consulta la tabella degli aggiornamenti delle politiche AWS gestite per ARC. È inoltre possibile abbonarsi agli avvisi RSS automatici nella pagina della cronologia dei documenti ARC.

AWS politiche gestite per il controllo della disponibilità in ARC

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 Si consiglia pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente specifiche per i propri 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, consultare Policy gestite da AWS nella Guida per l'utente di IAM.

AWS politica gestita: Route53 RecoveryReadinessServiceRolePolicy

Non è possibile collegare `Route53RecoveryReadinessServiceRolePolicy`alle entità IAM. Questa policy è associata a un ruolo collegato al servizio che consente ad Amazon Application Recovery Controller (ARC) di accedere a AWS servizi e risorse utilizzati o gestiti da ARC. Per ulteriori informazioni, consulta Utilizzo del ruolo collegato al servizio per il controllo di disponibilità in ARC.

AWS politica gestita: 53 AmazonRoute RecoveryReadinessFullAccess

È possibile collegare `AmazonRoute53RecoveryReadinessFullAccess` alle entità IAM. Questa politica garantisce il pieno accesso alle azioni per lavorare con la preparazione al ripristino (controllo di preparazione) in ARC. Collegala agli utenti IAM e ad altri responsabili che necessitano dell'accesso completo alle azioni di preparazione al ripristino.

Per visualizzare le autorizzazioni per questa policy, vedi AmazonRoute53 RecoveryReadinessFullAccess nel AWS Managed Policy Reference.

AWS politica gestita: 53 AmazonRoute RecoveryReadinessReadOnlyAccess

È possibile collegare `AmazonRoute53RecoveryReadinessReadOnlyAccess` alle entità IAM. Questa politica garantisce l'accesso in sola lettura alle azioni volte a garantire la preparazione al ripristino in ARC. È utile per gli utenti che devono visualizzare gli stati di preparazione e le configurazioni dei gruppi di ripristino. Questi utenti non possono creare, aggiornare o eliminare le risorse di preparazione al ripristino.

Per visualizzare le autorizzazioni per questa politica, vedere AmazonRoute53 RecoveryReadinessReadOnlyAccess nel AWS Managed Policy Reference.

Aggiornamenti relativi alle policy AWS gestite per la preparazione

Per informazioni dettagliate sugli aggiornamenti delle policy AWS gestite per il controllo di fattibilità in ARC da quando questo servizio ha iniziato a tenere traccia di queste modifiche, vedere. Aggiornamenti alle politiche AWS gestite per Amazon Application Recovery Controller (ARC) Per avvisi automatici sulle modifiche a questa pagina, iscriviti al feed RSS nella pagina della cronologia dei documenti ARC.

Quote per il controllo di prontezza

> **Note**
>
> La funzionalità di controllo della disponibilità in Amazon Application Recovery Controller (ARC) non sarà più aperta ai nuovi clienti a partire dal 30 aprile 2026. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta Amazon Application Recovery Controller (ARC) readiness check availability change.

Il controllo di conformità in Amazon Application Recovery Controller (ARC) è soggetto alle seguenti quote (precedentemente denominate limiti).

Entità	Quota
Numero di gruppi di ripristino per account	5
Numero di celle per account	15
Numero di celle annidate per cella	3
Numero di celle per gruppo di recupero	3
Numero di risorse per cella	10
Numero di risorse per gruppo di ripristino	10
Numero di risorse per set di risorse	6
Numero di set di risorse per account	200
Numero di controlli di idoneità per account	200
Numero di autorizzazioni su più account	100

Cambio di regione in ARC

È possibile utilizzare Region switch in ARC per orchestrare attività di ripristino complesse e su larga scala per le risorse applicative su più AWS account, per garantire la continuità aziendale e ridurre

il sovraccarico operativo. Lo switch di regione offre una soluzione centralizzata e osservabile che puoi eseguire manualmente o automatizzare utilizzando i trigger di allarme di Amazon CloudWatch . In caso di Regione AWS problemi, puoi eseguire i piani che hai creato utilizzando Region Switch per eseguire il failover o trasferire le tue risorse in un'altra regione. Ciò garantisce che l'applicazione possa continuare a funzionare e funzionare in condizioni ottimali. Regione AWS

Region Switch si basa sul concetto di piano, che viene progettato e configurato per esigenze di ripristino specifiche. Ogni piano include flussi di lavoro costituiti da fasi. Ogni passaggio esegue uno o più blocchi di esecuzione, che lo switch di regione esegue in parallelo o in sequenza, per completare il ripristino di un'applicazione. Ogni blocco di esecuzione gestisce un'attività diversa, come il trasferimento delle risorse o la gestione del reindirizzamento del traffico per l'applicazione. Per una flessibilità ancora maggiore, puoi creare piani per i genitori, aggiungendo piani per bambini a un piano generale per genitori.

Il cambio di regione include quanto segue:

- Support active/passive e active/active configurazioni. È possibile eseguire il failover e il failback se si dispone di configurazioni active/passive multiregionali, oppure lo shift-away e return se l'applicazione è configurata come in più regioni. active/active
- Supporto su più account per le risorse applicative incluse nel ripristino dell'applicazione. Puoi anche condividere i piani Region Switch tra più account.
- Failover o switchover automatico, attivando l'esecuzione del piano in base agli allarmi di Amazon. CloudWatch In alternativa, puoi scegliere di eseguire manualmente un piano di cambio di regione.
- Dashboard complete che offrono visibilità in tempo reale sul processo di ripristino.
- Ciascuno include un piano dati Regione AWS, in modo da poter eseguire il piano di cambio di regione senza dipendere dalla regione che si sta disattivando.

Il cambio di regione è completamente gestito da. AWS L'utilizzo di Region Switch consente di beneficiare della resilienza di una piattaforma di ripristino incentrata sui requisiti specifici dell'applicazione, anziché creare e gestire script e raccogliere manualmente dati sui ripristini.

Informazioni su Region Switch

Con Region Switch, puoi orchestrare i passaggi specifici per cambiare l'applicazione in Regione AWS cui è in esecuzione la tua applicazione multiregionale.

Il cambio di regione si basa sul concetto di piano, che viene progettato e configurato per esigenze di ripristino specifiche. Ogni piano include flussi di lavoro costituiti da fasi. Ogni passaggio esegue

uno o più blocchi di esecuzione, che lo switch di regione esegue in parallelo o in sequenza, per completare il ripristino di un'applicazione. Ogni blocco di esecuzione gestisce un'attività diversa, come il trasferimento delle risorse o la gestione del reindirizzamento del traffico per l'applicazione. Per una flessibilità ancora maggiore, puoi creare piani per i genitori aggiungendo piani per bambini.

Ogni volta che crei o aggiorni un piano, Region switch esegue una valutazione del piano per garantire che non vi siano problemi con le autorizzazioni IAM, le configurazioni delle risorse o la capacità di esecuzione. Region switch esegue queste valutazioni regolarmente e genera un avviso per eventuali problemi rilevati.

Region switch calcola inoltre un valore effettivo del tempo di ripristino per ogni esecuzione del piano, per aiutarvi a valutare se il piano soddisfa gli obiettivi prefissati. È possibile visualizzare i tempi di ripristino e altri dettagli sull'esecuzione dei piani nei dashboard di Region Switch in. Console di gestione AWS Per ulteriori informazioni, consulta Dashboard di cambio di regione.

Per ulteriori informazioni su ciascuna di queste aree in Region Switch, consulta le seguenti sezioni.

Piani di cambio di regione

Un piano di cambio di regione è la risorsa di primo livello in Region Switch. È necessario adattare il piano a una specifica applicazione multiregionale. Un piano consente di creare flussi di lavoro per ripristinare le applicazioni eseguendo una serie di blocchi di esecuzione di switch di regione che attivano o disattivano l'applicazione e le relative risorse, comprese le risorse tra account diversi, nella Regione AWS modalità specificata.

Un piano è composto da uno o più flussi di lavoro, per consentirti di attivarne o disattivarne uno specifico. Regione AWSÈ possibile configurare i blocchi di esecuzione in un flusso di lavoro in modo che vengano eseguiti in sequenza oppure è possibile specificare che alcuni blocchi vengano eseguiti in parallelo.

Per un piano configurato per un approccio active/passive multiregionale, è necessario creare un flusso di lavoro che può essere utilizzato per attivare una delle regioni o due flussi di lavoro di attivazione separati, uno per ciascuna regione. Per un piano configurato per un approccio attivo/attivo, crei un flusso di lavoro per attivare le regioni e un flusso di lavoro per disattivare le regioni.

Regioni AWS sono località geografiche in tutto il mondo in cui si trovano i data center dei AWS cluster. Ogni regione è progettata per essere completamente isolata dalle altre regioni, garantendo stabilità e tolleranza ai guasti. Quando si utilizza Region Switch, è necessario considerare in quali regioni è distribuita l'applicazione e quali regioni si desidera utilizzare per il ripristino.

Il cambio di regione supporta il ripristino tra due aree qualsiasi Regioni AWS in cui il servizio è disponibile. Quando si configura un piano di cambio di regione, si specificano le regioni in cui viene distribuita l'applicazione e l'approccio di ripristino che si desidera utilizzare: active/passive o attivo/attivo.

Ad esempio, potresti avere un approccio active/passive multiregionale con us-east-1 come regione principale e us-west-2 come regione di standby. Per ripristinare l'applicazione da un problema operativo che ha un impatto sull'applicazione in us-east-1, è possibile eseguire il piano di cambio di regione per attivare us-west-2. Ciò comporterebbe il passaggio dell'applicazione dalle risorse in us-east-1 alle risorse in us-west-2.

I piani di cambio di regione vengono eseguiti utilizzando le autorizzazioni associate al ruolo IAM che specifichi al momento della creazione del piano.

Puoi creare più piani, uno per ciascuna delle tue applicazioni multiregionali, e quindi orchestrare il ripristino tra questi piani nell'ordine richiesto creando un piano principale. Un piano principale è un piano che utilizza i blocchi di esecuzione del piano Region Switch come fasi. La gerarchia dei piani è limitata a due livelli (genitore e figlio), ma è possibile includere più piani per bambini nello stesso piano principale.

Flussi di lavoro e blocchi di esecuzione

Dopo aver creato un piano di cambio di regione, è necessario aggiungere uno o più flussi di lavoro al piano per definire i passaggi che si desidera che il piano esegua per il ripristino dell'applicazione. Per ogni flusso di lavoro, si aggiungono passaggi che contengono blocchi di esecuzione. Ogni blocco di esecuzione esegue un'azione di ripristino specifica, ad esempio il ridimensionamento delle risorse o l'aggiornamento dei controlli di routing per reindirizzare il traffico. I passaggi organizzano questi blocchi di esecuzione e controllano se vengono eseguiti in parallelo o in sequenza. Creando piani principali, puoi anche orchestrare l'ordine in cui più applicazioni vengono ripristinate nella regione che stai attivando.

I blocchi di esecuzione vengono organizzati in fasi all'interno di un flusso di lavoro. Ogni passaggio può contenere uno o più blocchi di esecuzione eseguiti in parallelo e puoi organizzare i passaggi in modo che vengano eseguiti in sequenza nel tuo flusso di lavoro. Inoltre, a seconda della risorsa, puoi avere la possibilità di eseguire un blocco di esecuzione con esecuzione regolare (pianificata) o non corretta (non pianificata).

- Esecuzione elegante: un flusso di lavoro di esecuzione pianificato. Quando l'ambiente è integro, è possibile utilizzare il flusso di lavoro Graceful per eseguire tutte le fasi necessarie a un'esecuzione ordinata del piano.
- Esecuzione non corretta: un'esecuzione non pianificata. La modalità di flusso di lavoro non corretta utilizza solo i passaggi e le azioni necessari. Questa modalità modifica il comportamento dei blocchi di esecuzione in un flusso di lavoro o ignora blocchi di esecuzione specifici.
- Esecuzione post-ripristino: un flusso di lavoro che viene eseguito dopo un ripristino riuscito per prepararsi a futuri eventi regionali. Le esecuzioni successive al ripristino possono creare repliche di lettura, eseguire logica personalizzata tramite funzioni Lambda, aggiungere porte di approvazione manuali e incorporare piani secondari per un'orchestrazione complessa. Queste esecuzioni richiedono che entrambe le regioni siano integre e vengano eseguite nella regione precedentemente compromessa.

Infine, puoi anche configurare risorse tra account diversi per un blocco di esecuzione. Innanzitutto, è necessario configurare le autorizzazioni seguendo le istruzioni riportate in. Supporto per più account in Region Switch Dopo aver configurato i ruoli IAM richiesti, puoi aggiungere risorse cross-account nei blocchi di esecuzione dei flussi di lavoro del tuo piano. Per aggiungere risorse su più account, quando aggiungi un passaggio, specifichi un ruolo IAM di destinazione con autorizzazioni per la risorsa di altri. Account AWSÈ inoltre necessario specificare l'ID esterno fornito nella politica di fiducia per il ruolo tra account diversi. Per i dettagli sulla creazione dei ruoli IAM richiesti, consultaAutorizzazioni relative alle risorse per più account.

Per ulteriori informazioni sui flussi di lavoro, consultaCrea flussi di lavoro del piano Region Switch. Per informazioni dettagliate su ciascun tipo di blocco di esecuzione, inclusi i passaggi di configurazione, il suo funzionamento e gli elementi valutati nell'ambito della valutazione del piano, consulta. Aggiungere blocchi di esecuzione

Valutazione del piano

La valutazione del piano è un processo automatizzato che Region Switch esegue quando un piano viene creato o aggiornato e successivamente ogni 30 minuti, durante lo stato stazionario. Il processo di valutazione verifica diversi aspetti critici della configurazione del piano e delle configurazioni delle risorse. Le valutazioni includono la verifica delle autorizzazioni IAM, delle configurazioni delle risorse e della capacità di esecuzione.

Se Region switch rileva un problema che potrebbe impedire la corretta esecuzione del piano, genera un avviso di valutazione del piano, che viene evidenziato nella pagina dei dettagli del piano nella

console. Puoi anche utilizzare gli avvisi di valutazione del piano con Amazon EventBridge oppure puoi visualizzare gli avvisi utilizzando l'API Region Switch. Per ulteriori informazioni sull'API Plan Evaluation, consulta GetPlanEvaluationStatusla Region Switch API Reference Guide per Amazon Application Recovery Controller (ARC).

Puoi vedere i dettagli e le soluzioni suggerite per i problemi che emergono dalla valutazione del piano nella scheda Valutazione del piano nella pagina dei dettagli del piano. Ti consigliamo di testare il ripristino delle applicazioni anche eseguendo il tuo piano di cambio di regione e di non affidarti esclusivamente alla valutazione del piano di cambio di regione per verificare che il piano di ripristino funzioni come previsto.

Rapporti automatici sull'esecuzione del piano

Region Switch può generare automaticamente report PDF completi per l'esecuzione dei piani per aiutarvi a soddisfare i requisiti di conformità normativa. Questi report forniscono prove dei test di disaster recovery e degli eventi di ripristino effettivi, tra cui tempistiche di esecuzione dettagliate, configurazioni dei piani e stati delle risorse.

Quando configuri la generazione automatica di report per un piano, Region switch crea un report PDF al termine di ogni esecuzione del piano e lo invia a un bucket Amazon S3 specificato dall'utente. I report sono generalmente disponibili entro 30 minuti dal completamento dell'esecuzione. Si applicano i costi di storage S3.

Ogni rapporto include:

- Riepilogo esecutivo con panoramica del servizio e data di creazione del report
- Pianifica i dettagli della configurazione così come esistevano al momento dell'esecuzione
- Cronologia dettagliata dell'esecuzione con passaggi, risorse interessate e stati
- Pianifica gli avvisi presenti all'inizio dell'esecuzione
- Stati degli CloudWatch allarmi di Amazon e cronologia degli allarmi associati
- Per i piani per i genitori, i dettagli di configurazione ed esecuzione dei piani secondari
- Glossario di termini e concetti

Per abilitare la generazione automatica dei report, si configura una destinazione di output dei report quando si crea o si aggiorna un piano. È inoltre necessario assicurarsi che il ruolo IAM di esecuzione del piano disponga delle autorizzazioni necessarie per scrivere report nel bucket Amazon S3 e accedere alle risorse necessarie per generare il contenuto del report. Per ulteriori informazioni

sulle autorizzazioni richieste, consultare Autorizzazioni per l'esecuzione automatica dei report di esecuzione del piano.

Puoi visualizzare lo stato della generazione dei report e scaricare i report completati dalla pagina dei dettagli di esecuzione del piano nella console. Se nella generazione dei report si verificano errori, ad esempio autorizzazioni insufficienti o bucket Amazon S3 non configurati correttamente, Region Switch fornisce i dettagli dell'errore per aiutarti a risolvere il problema.

La valutazione del piano convalida continuamente la configurazione del report, inclusa la verifica che il ruolo di esecuzione disponga delle autorizzazioni IAM richieste. Se Region switch rileva problemi di configurazione che impedirebbero la corretta generazione dei report, genera avvisi che è possibile visualizzare nella pagina dei dettagli del piano.

Allarmi regionali e tempo di ripristino effettivo

Il cambio di regione calcola un valore effettivo del tempo di ripristino per ogni esecuzione del piano, che è possibile visualizzare dopo l'esecuzione di un piano. Il tempo di ripristino effettivo viene visualizzato nella pagina dei dettagli di esecuzione del piano, in modo da poter confrontare il tempo effettivo con l'obiettivo del tempo di ripristino specificato al momento della creazione del piano.

Il tempo di ripristino effettivo viene calcolato come il tempo totale impiegato per il completamento dell'esecuzione di un piano e il tempo aggiuntivo trascorso prima che specifici CloudWatch allarmi Amazon configurati tornino allo stato verde.

Per supportare il calcolo accurato del tempo di ripristino effettivo per l'esecuzione del piano, devi configurare gli CloudWatch allarmi Amazon regionali per un piano di switch di regione che fornisca un segnale sullo stato dell'applicazione in ciascuna regione. Quando viene eseguito un piano, Region switch utilizza questi allarmi sullo stato dell'applicazione per determinare quando l'applicazione è nuovamente integra. Quindi, Region switch calcola il tempo di ripristino effettivo in base al tempo impiegato per l'esecuzione del piano e al tempo necessario per ripristinare l'integrità dell'applicazione, in base agli allarmi sullo stato dell'applicazione configurati.

Prima di aggiungere CloudWatch allarmi a un piano di cambio di regione, assicurati di disporre della politica IAM corretta. Per ulteriori informazioni, consulta CloudWatch allarmi per le autorizzazioni di integrità dell'applicazione.

Regioni AWS

Il cambio di regione è disponibile in tutte le regioni commerciali Regioni AWS e in quelle AWS GovCloud (degli Stati Uniti).

Per informazioni dettagliate sul supporto regionale e sugli endpoint di servizio per Amazon Application Recovery Controller (ARC), consulta gli endpoint e le quote di Amazon Application Recovery Controller (ARC) nel riferimento generale di Amazon Web Services.

Nome della regione	Regione	Endpoint	Protocollo
US East (Ohio)	us-east-2	arc-region-switch.us-east-2.api.aws arc-region-switch-fips.us-east-2.api.aws	HTTPS HTTPS
US East (N. Virginia)	us-east-1	arc-region-switch.us-east-1.api.aws arc-region-switch-control-plane-fips.us-east-1.api.aws arc-region-switch-fips.us-east-1.api.aws arc-region-switch-control-plane.us-east-1.api.aws	HTTPS HTTPS HTTPS HTTPS
Stati Uniti occidentali (California settentrionale)	us-west-1	arc-region-switch.us-west-1.api.aws arc-region-switch-fips.us-west-1.api.aws	HTTPS HTTPS
Stati Uniti occidentali (Oregon)	us-west-2	arc-region-switch.us-west-2.api.aws arc-region-switch-fips.us-west-2.api.aws	HTTPS HTTPS
Africa (Città del Capo)	af-south-1	arc-region-switch.af-south-1.api.aws	HTTPS

Nome della regione	Regione	Endpoint	Protocollo	
Asia Pacifico (Hong Kong)	ap-east-1	arc-region-switch.ap-east-1.api.aws	HTTPS	
Asia Pacific (Hyderabad)	ap-south-2	arc-region-switch.ap-south-2.api.aws	HTTPS	
Asia Pacifico (Giacarta)	ap-southeast-3	arc-region-switch.ap-southeast-3.api.aws	HTTPS	
Asia Pacifico (Malesia)	ap-southeast-5	arc-region-switch.ap-southeast-5.api.aws	HTTPS	
Asia Pacifico (Melbourne)	ap-southeast-4	arc-region-switch.ap-southeast-4.api.aws	HTTPS	
Asia Pacifico (Mumbai)	ap-south-1	arc-region-switch.ap-south-1.api.aws	HTTPS	
Asia Pacifico (Nuova Zelanda)	ap-southeast-6	arc-region-switch.ap-southeast-6.api.aws	HTTPS	

Nome della regione	Regione	Endpoint	Protocollo	
Asia Pacifico (Osaka-Locale)	ap-northeast-3	arc-region-switch.ap-northeast-3.api.aws	HTTPS	
Asia Pacifico (Seoul)	ap-northeast-2	arc-region-switch.ap-northeast-2.api.aws	HTTPS	
Asia Pacifico (Singapore)	ap-southeast-1	arc-region-switch.ap-southeast-1.api.aws	HTTPS	
Asia Pacifico (Sydney)	ap-southeast-2	arc-region-switch.ap-southeast-2.api.aws	HTTPS	
Asia Pacifico (Taipei)	ap-east-2	arc-region-switch.ap-east-2.api.aws	HTTPS	
Asia Pacifico (Thailandia)	ap-southeast-7	arc-region-switch.ap-southeast-7.api.aws	HTTPS	
Asia Pacifico (Tokyo)	ap-northeast-1	arc-region-switch.ap-northeast-1.api.aws	HTTPS	
Canada (Centrale)	ca-central-1	arc-region-switch.ca-central-1.api.aws	HTTPS	

Nome della regione	Regione	Endpoint	Protocollo	
Canada occidentale (Calgary)	ca-west-1	arc-region-switch.ca-west-1.api.aws	HTTPS	
Europa (Francoforte)	eu-central-1	arc-region-switch.eu-central-1.api.aws	HTTPS	
Europa (Irlanda)	eu-west-1	arc-region-switch.eu-west-1.api.aws	HTTPS	
Europa (Londra)	eu-west-2	arc-region-switch.eu-west-2.api.aws	HTTPS	
Europa (Milano)	eu-south-1	arc-region-switch.eu-south-1.api.aws	HTTPS	
Europa (Parigi)	eu-west-3	arc-region-switch.eu-west-3.api.aws	HTTPS	
Europa (Spagna)	eu-south-2	arc-region-switch.eu-south-2.api.aws	HTTPS	
Europa (Stoccolma)	eu-north-1	arc-region-switch.eu-north-1.api.aws	HTTPS	
Europa (Zurigo)	eu-central-2	arc-region-switch.eu-central-2.api.aws	HTTPS	
Israele (Tel Aviv)	il-central-1	arc-region-switch.il-central-1.api.aws	HTTPS	

Nome della regione	Regione	Endpoint	Protocollo
Messico (Centrale)	mx-central-1	arc-region-switch.mx-central-1.api.aws	HTTPS
Medio Oriente (Bahrein)	me-south-1	arc-region-switch.me-south-1.api.aws	HTTPS
Medio Oriente (Emirati Arabi Uniti)	me-central-1	arc-region-switch.me-central-1.api.aws	HTTPS
Sud America (São Paulo)	sa-east-1	arc-region-switch.sa-east-1.api.aws	HTTPS
AWS GovCloud (Stati Uniti orientali)	us-gov-east-1	arc-region-switch.us-gov-east-1.api.aws arc-region-switch-fips.us-gov-east-1.api.aws	HTTPS HTTPS
AWS GovCloud (Stati Uniti occidentali)	us-gov-west-1	arc-region-switch.us-gov-west-1.api.aws arc-region-switch-control-plane-fips.us-gov-west-1.api.aws arc-region-switch-fips.us-gov-west-1.api.aws arc-region-switch-control-plane.us-gov-west-1.api.aws	HTTPS HTTPS HTTPS HTTPS

Componenti del cambio di regione

Di seguito sono riportati i componenti e i concetti relativi alla funzionalità di cambio di regione in Amazon Application Recovery Controller (ARC).

Pianificazione

Un piano è il processo di ripristino fondamentale per la tua applicazione. Puoi creare un piano creando uno o più flussi di lavoro con blocchi di esecuzione da eseguire in sequenza o in parallelo. Quindi, in caso di problemi a livello regionale, si esegue il piano per completare il ripristino dell'applicazione spostando l'applicazione in una regione integra.

Piano per bambini

Un piano secondario è un piano autonomo che può essere eseguito all'interno di un piano principale, per coordinare scenari di ripristino delle applicazioni più complessi. È possibile annidare i piani Region Switch a un livello.

Flusso di lavoro

Un piano di cambio di regione include uno o più flussi di lavoro. Un flusso di lavoro è costituito da passaggi che contengono blocchi di esecuzione, specificati per l'esecuzione in parallelo o in sequenza, per completare l'attivazione o la disattivazione di una regione come parte di un piano di ripristino. Per un piano configurato in base a un active/passive approccio, è necessario creare un unico flusso di lavoro che può essere utilizzato per attivare una delle regioni o flussi di lavoro di attivazione separati, uno per ogni regione. Per un piano configurato per un active/active approccio, crei un flusso di lavoro per attivare le regioni e un flusso di lavoro per disattivare le regioni.

Blocco di esecuzione

Si aggiungono passaggi ai flussi di lavoro del piano di cambio di regione contenenti un blocco di esecuzione. I blocchi di esecuzione consentono di specificare il ripristino per più applicazioni o risorse in una regione di attivazione. Quando aggiungi un passaggio a un flusso di lavoro, puoi aggiungerlo in sequenza con altri passaggi o in parallelo con uno o più altri passaggi.

Configurazioni graziose e sgradevoli

È possibile scegliere di eseguire blocchi di esecuzione specifici con esecuzione regolare (pianificata) o non corretta (non pianificata). Quando l'ambiente è integro, è possibile utilizzare l'elegante flusso di lavoro per eseguire tutte le fasi necessarie all'esecuzione ordinata del piano. La modalità di flusso di lavoro poco funzionale utilizza solo i passaggi e le azioni necessari.

Quando si esegue un piano in modalità ungraceful, modifica il comportamento dei blocchi di esecuzione in un flusso di lavoro o ignora blocchi di esecuzione specifici, a seconda del tipo di blocco di esecuzione.

Tipi specifici di blocchi di esecuzione hanno un comportamento diverso quando vengono eseguiti in modo non corretto. I dettagli su queste differenze sono descritti nella sezione che include dettagli su ciascun tipo di blocco di esecuzione. Per ulteriori informazioni, consulta Aggiungere blocchi di esecuzione.

Configurazioni Active/active and active/passive

Esistono due approcci principali per creare una configurazione resiliente per un'applicazione in più regioni: active/passive uno attivo/attivo. Il cambio di regione supporta il ripristino delle applicazioni per entrambi questi approcci.

Con una active/passive configurazione, puoi distribuire due repliche dell'applicazione in due regioni diverse, con il traffico dei clienti diretto a una sola regione.

Con una active/active configurazione, si distribuiscono due repliche in due regioni diverse, ma entrambe le repliche elaborano il lavoro o ricevono traffico.

Esecuzione del piano

Quando viene eseguito un piano di cambio di regione, implementa il ripristino di un'applicazione quando una regione viene compromessa attivando una regione integra per l'applicazione e il traffico che riceve. Con una active/active configurazione, esegui anche l'esecuzione di un piano per disattivare la regione danneggiata.

Allarmi relativi allo stato delle applicazioni

Gli allarmi sullo stato delle applicazioni sono CloudWatch allarmi specificati per un piano per indicare lo stato dell'applicazione in ciascuna regione. Il cambio di regione utilizza gli allarmi sullo stato dell'applicazione per determinare il tempo di ripristino effettivo dopo aver cambiato regione per implementare il ripristino.

Triggers

È possibile utilizzare i trigger in Region Switch per automatizzare il ripristino delle applicazioni. Quando crei un trigger, specifichi uno o più CloudWatch allarmi Amazon e definisci quali condizioni di allarme (ad esempio «rosso» o «verde») devono avviare l'esecuzione del piano. Quando vengono soddisfatte le condizioni specificate, Region switch esegue automaticamente il piano. I trigger sono diversi dagli allarmi sullo stato delle applicazioni: i trigger avviano

l'esecuzione del piano, mentre gli allarmi sullo stato dell'applicazione aiutano Region Switch a calcolare il tempo di ripristino effettivo dopo il completamento di un piano.

Flusso di lavoro post-ripristino

Un flusso di lavoro post-ripristino è un flusso di lavoro opzionale che viene eseguito dopo un ripristino riuscito per prepararsi a futuri eventi regionali. Questi flussi di lavoro richiedono che entrambe le regioni siano integre e funzionino nella regione precedentemente compromessa. Le esecuzioni successive al ripristino fanno riferimento all'ID di esecuzione del ripristino più recente.

I flussi di lavoro post-ripristino supportano i seguenti blocchi di esecuzione:

- RDS Create Cross-Region Replica
- Azione personalizzata Lambda
- Approvazione manuale
- Piano di cambio di regione

Pannelli di controllo

Region Switch include dashboard in cui è possibile tenere traccia dei dettagli sull'esecuzione dei piani in tempo reale.

Piani di dati e controllo per Region Switch

Quando pianifichi il failover e il disaster recovery, considera la resilienza dei tuoi meccanismi di failover. Ti consigliamo di assicurarti che i meccanismi da cui dipendi durante il failover siano altamente disponibili, in modo da poterli utilizzare quando ne hai bisogno in uno scenario di emergenza. In genere, è consigliabile utilizzare le funzioni del piano dati per i meccanismi ogni volta che è possibile, per la massima affidabilità e tolleranza ai guasti. In quest'ottica, è importante capire in che modo la funzionalità di un servizio è suddivisa tra piani di controllo e piani dati e quando è possibile contare su un'aspettativa di estrema affidabilità con il piano dati di un servizio.

Come per molti AWS servizi, la funzionalità relativa alla funzionalità Region Switch è supportata da un piano di controllo e da piani dati. Sebbene entrambi i tipi siano progettati per essere affidabili, un piano di controllo è ottimizzato per la coerenza dei dati, mentre un piano dati è ottimizzato per la disponibilità. Un piano dati è progettato per la resilienza in modo da poter mantenere la disponibilità anche durante eventi dirompenti, quando un piano di controllo potrebbe non essere disponibile.

In generale, un piano di controllo consente di eseguire funzioni di gestione di base, come creare, aggiornare ed eliminare risorse nel servizio. Un piano dati fornisce le funzionalità principali di

un servizio. Per questo motivo, si consiglia di utilizzare le operazioni del piano dati quando la disponibilità è importante, ad esempio quando è necessario ottenere informazioni su un piano di cambio di regione durante un'interruzione.

Per il cambio di regione, i piani di controllo e i piani dati sono suddivisi come segue:

- Il piano di controllo per Region Switch si trova nella regione (us-east-1) degli Stati Uniti orientali (Virginia settentrionale) AWS GovCloud , nella regione (-1) degli Stati Uniti orientali us-gov-west (Virginia settentrionale) e deve essere utilizzato solo per la gestione dei servizi, ovvero la creazione e l'aggiornamento di piani, non per il ripristino, ovvero l'esecuzione di piani. Le operazioni dell'API del piano di controllo della configurazione dello switch Region non sono altamente disponibili.
- Lo switch di regione dispone di piani dati indipendenti in ciascuno di essi Regione AWS. È necessario utilizzare il piano dati per le azioni di ripristino, ovvero per l'esecuzione di piani di cambio di regione. Per un elenco delle operazioni del piano dati, vedereOperazioni API di cambio di regione. Queste operazioni sul piano dati con commutazione di regione sono altamente disponibili.

Region Switch fornisce una console indipendente in ciascuna di esse Regione AWS, che richiama le operazioni dell'API del piano dati per le attività di ripristino, in modo da poter utilizzare la console nella regione che stai attivando per eseguire piani per il ripristino delle applicazioni. Per ulteriori informazioni sulle considerazioni chiave relative alla preparazione e al completamento di un'operazione di ripristino con Region Switch, consulta. Le migliori pratiche per il cambio di regione in ARC

Per ulteriori informazioni sui piani dati, sui piani di controllo e su come AWS crea servizi per soddisfare gli obiettivi di alta disponibilità, consulta il paper Static stability using Availability Zones in Amazon Builders' Library.

Etichettatura per lo switch ARC Region;

I tag sono parole o frasi (metadati) che usi per identificare e organizzare le tue AWS risorse. È possibile aggiungere più tag a ogni risorsa e ogni tag include una chiave e un valore che definisci. Ad esempio, la chiave potrebbe essere l'ambiente e il valore potrebbe essere la produzione. Puoi cercare e filtrare le tue risorse in base ai tag che aggiungi.

Puoi taggare la seguente risorsa in Region switch in ARC:

- Piani

L'aggiunta di tag in ARC è disponibile solo tramite l'API, ad esempio utilizzando il AWS CLI.

Di seguito sono riportati alcuni esempi di etichettatura nel cambio di regione utilizzando. AWS CLI

```
aws arc-region-switch --region us-east-1 create-plan --plan-name example-plan --tags Region=IAD,Stage=Prod
```

Per ulteriori informazioni, consulta TagResourcela Guida di riferimento dell'API Region Switch per Amazon Application Recovery Controller (ARC).

Prezzi di Region Switch in ARC

Paghi un costo mensile fisso per il piano di cambio di regione che configuri.

Per informazioni dettagliate sui prezzi di ARC ed esempi di prezzi, consulta ARC Pricing.

Le migliori pratiche per il cambio di regione in ARC

Consigliamo le seguenti best practice per la preparazione al ripristino e al failover con Region Switch in Amazon Application Recovery Controller (ARC).

Argomenti

- Mantieni le credenziali create appositamente e di lunga durata sicure e sempre accessibili AWS
- Scegli valori TTL inferiori per i record DNS coinvolti nel failover
- Riserva la capacità richiesta per le applicazioni critiche
- Utilizza le operazioni estremamente affidabili dell'API Data Plane per elencare e ottenere informazioni sui piani di cambio di regione
- Test di failover con ARC

Mantieni le credenziali create appositamente e di lunga durata sicure e sempre accessibili AWS

> In uno scenario di disaster recovery (DR), riduci al minimo le dipendenze dal sistema utilizzando un approccio semplice per accedere ed eseguire le attività di ripristino. AWS Crea credenziali IAM a lunga durata specifiche per le attività di DR e conservale in modo sicuro in una cassaforte fisica locale o in un deposito virtuale, a cui accedervi quando necessario. Con IAM, puoi gestire centralmente le credenziali di sicurezza, come le chiavi di accesso e le autorizzazioni per l'accesso alle risorse. AWS Per le attività diverse dal DR, ti consigliamo di continuare a utilizzare l'accesso federato, utilizzando AWS servizi come Single Sign-On.AWS

Scegliete valori TTL inferiori per i record DNS coinvolti nel failover

Per i record DNS che potrebbe essere necessario modificare nell'ambito del meccanismo di failover, in particolare per i record il cui stato di integrità è stato verificato, è opportuno utilizzare valori TTL inferiori. Per questo scenario, è comune impostare un TTL di 60 o 120 secondi.

L'impostazione DNS TTL (time to live) indica ai resolver DNS per quanto tempo devono memorizzare nella cache un record prima di richiederne uno nuovo. Quando scegli un TTL, fai un compromesso tra latenza e affidabilità e reattività al cambiamento. Con un TTL più breve su un record, i resolver DNS notano gli aggiornamenti del record più rapidamente perché il TTL specifica che devono eseguire query più frequentemente.

Per ulteriori informazioni, consulta Scelta dei valori TTL per i record DNS nelle migliori pratiche per Amazon Route 53 DNS.

Riserva la capacità richiesta per le applicazioni critiche

Region Switch include tipi di blocchi di esecuzione che aiutano a scalare le risorse di calcolo come parte del ripristino. Se si utilizzano questi blocchi di esecuzione in un piano, Region switch non garantisce il raggiungimento della capacità di elaborazione desiderata. Se disponi di un'applicazione critica e devi garantire l'accesso alla capacità, ti consigliamo di riservare la capacità.

Esistono strategie che puoi seguire per riservare la capacità di elaborazione in una regione secondaria limitando al contempo i costi. Per ulteriori informazioni, consulta Pilot light with reserved capacity: come ottimizzare i costi di disaster recovery utilizzando On-Demand Capacity Reservations.

Utilizza le operazioni estremamente affidabili dell'API Data Plane per elencare e ottenere informazioni sui piani di cambio di regione

Utilizza le operazioni dell'API del piano dati per elaborare ed eseguire il tuo piano di cambio di regione durante un evento. Per un elenco delle operazioni del piano dati di cambio di regione, vedereOperazioni API di cambio di regione.

La console di commutazione di regione in ciascuna regione utilizza le operazioni del piano dati per eseguire i piani di commutazione di regione. È inoltre possibile richiamare le operazioni dell'API del piano dati utilizzando AWS CLI o eseguendo il codice scritto utilizzando uno dei AWS SDKs. ARC offre un'affidabilità estrema con l'API nel piano dati.

Prova il ripristino delle applicazioni con ARC

Prova regolarmente il ripristino delle applicazioni con ARC Region Switch, per attivare uno stack di applicazioni secondario in un altro Regione AWS o per passare a una configurazione attiva-attiva eseguendo un piano di cambio di regione per disattivare una delle regioni.

È importante assicurarsi che i piani di cambio di regione che hai creato siano allineati con le risorse corrette del tuo stack e che tutto funzioni come previsto. È necessario verificarlo dopo aver configurato il Region Switch per l'ambiente e continuare a eseguire il test periodicamente, in modo da verificare che i processi di ripristino funzionino correttamente. Esegui questi test regolarmente, prima che si verifichi una situazione di errore, per evitare tempi di inattività per gli utenti.

Failover DNS dello switch ARC Region e ripristino accelerato Route 53

Il ripristino accelerato fornisce un RTO target di 60 minuti da APIs utilizzare per aggiornare i record delle zone ospitate pubbliche abilitate per questa funzionalità. Se è necessario mantenere il controllo sull'RTO e non attendere il ripristino completo di AWS quello APIs necessario, è consigliabile utilizzare ARC Routing control o ARC Region switch Route 53 Health Check Execution Block.

Tutorial: Creare un piano di cambio di active/passive regione

Questo tutorial ti guida nella creazione di un piano di cambio di active/passive regione per un'applicazione in esecuzione in us-east-1 e nel ripristino in us-west-2. L'esempio include istanze Amazon EC2 per l'elaborazione, Amazon Aurora Global Database per lo storage e Amazon Route 53 per DNS.

In questo tutorial, completerai i seguenti passaggi:

- Crea un piano di cambio di regione
- Crea i flussi di lavoro e i blocchi di esecuzione del piano
- Crea un blocco di esecuzione di gruppo EC2 Auto Scaling
- Crea due blocchi di esecuzione manuale dell'approvazione
- Crea due blocchi di esecuzione Lambda con azioni personalizzate
- Crea un blocco di esecuzione di Amazon Aurora Global Database
- Crea un blocco di controllo del routing ARC
- Esegui il piano di cambio di regione

Prerequisiti

Prima di iniziare questo tutorial, verifica di avere i seguenti prerequisiti in entrambe le regioni:

- Ruoli IAM con autorizzazioni appropriate
- Gruppi di Auto Scaling EC2
- Funzioni Lambda per pagine di manutenzione e recinzioni
- Aurora Global Database
- Controlli di routing ARC

Fase 1: Creare il piano di cambio di regione

1. Dalla console Region Switch, scegli Crea piano di switch Region.
2. Fornisci i seguenti dettagli:
   - Regione principale: scegli us-east-1
   - Regione di standby: scegli us-west-2
   - Obiettivo del tempo di ripristino (RTO) desiderato (opzionale)
   - Ruolo IAM: inserire il ruolo IAM per l'esecuzione del piano. Questo ruolo IAM consente alla regione di passare ai AWS servizi di chiamata durante l'esecuzione.
3. Scegli Create (Crea).

(Facoltativo) Aggiungi risorse da diversi AWS account al tuo piano di cambio di regione:

1. Crea il ruolo tra account:
   - Nell'account che ospita la risorsa, crea un ruolo IAM.
   - Aggiungi le autorizzazioni per le risorse specifiche a cui accederà il piano.
   - Aggiungi una politica di fiducia che consenta al ruolo di esecuzione di assumere il nuovo ruolo.
   - Inserisci e prendi nota di un ID esterno che utilizzerai come segreto condiviso.
2. Configura la risorsa nel tuo piano:
   - Quando aggiungi la risorsa al tuo piano, specifica due campi aggiuntivi:
     - crossAccountRole: L'ARN del ruolo creato nel passaggio 1
     - ExternalID: l'ID esterno che hai inserito nel passaggio 1

Esempio di configurazione per un blocco di esecuzione EC2 Auto Scaling che accede alle risorse nell'account 987654321:

```
{
  "executionBlock": "EC2AutoScaling",
  "name": "ASG",
  "crossAccountRole": "arn:aws:iam::987654321:role/RegionSwitchCrossAccountRole",
  "externalId": "unique-external-id-123",
  "autoScalingGroupArn": "arn:aws:autoscaling:us-
west-2:987654321:autoScalingGroup:*:autoScalingGroupName/CrossAccountASG"
}
```

Autorizzazioni richieste:

- Il ruolo di esecuzione deve avere l'AssumeRole autorizzazione sts: per il ruolo interaccount.
- Il ruolo tra account diversi deve disporre delle autorizzazioni solo per le risorse specifiche a cui si accede.
- La politica di fiducia del ruolo interaccount deve includere:
  - L'account del ruolo di esecuzione come entità attendibile.
  - La condizione dell'ID esterno.
- Per ulteriori informazioni sulla configurazione di un ruolo tra account, vedere. Autorizzazioni relative alle risorse per più account

Prima di eseguire il piano, Region switch verificherà quanto segue:

- Il ruolo di esecuzione può assumere il ruolo tra account diversi.
- Il ruolo tra account diversi dispone delle autorizzazioni richieste.
- L'ID esterno corrisponde alla politica di attendibilità.

Fase 2: Costruisci i flussi di lavoro e i blocchi di esecuzione del piano

1. Dalla pagina dei dettagli del piano Region Switch, scegli Crea flussi di lavoro.
2. Seleziona Crea lo stesso flusso di lavoro di attivazione per tutte le regioni.
3. Inserisci una descrizione del flusso di lavoro di attivazione della regione (opzionale). Questo verrà utilizzato per identificare facilmente il flusso di lavoro durante l'esecuzione del piano.

4. Seleziona Salva e continua.

Aggiungi il blocco di esecuzione EC2 Auto Scaling

Per ulteriori informazioni su questo blocco di esecuzione, consulta. Blocco di esecuzione di gruppo Amazon EC2 Auto Scaling

1. Scegli Aggiungi un passaggio, quindi seleziona Esegui in sequenza.
2. Seleziona il blocco di esecuzione EC2 Auto Scaling, quindi scegli Aggiungi e modifica. Questo blocco ti consentirà di iniziare ad aumentare la capacità nella regione passiva.
3. Nel pannello di destra, configura il blocco:

   - Nome del passaggio: inserisci «Scale»
   - Descrizione della fase (opzionale)
   - ARN del gruppo Auto Scaling per us-east-1: l'ARN del tuo ASG in us-east-1
   - ARN del gruppo Auto Scaling per us-west-2: l'ARN del tuo ASG in us-west-2
   - Percentuale corrispondente alla capacità della regione di origine: immettere 100
   - Approccio al monitoraggio della capacità: lascia come «Più recente»
   - Timeout (opzionale)

   Per informazioni sulle autorizzazioni IAM richieste per questo blocco di esecuzione, consulta. Politica di esempio per i blocchi di esecuzione di EC2 Auto Scaling
4. Scegli Salva passaggio.

Aggiungi un blocco di esecuzione dell'approvazione manuale

Per ulteriori informazioni su questo blocco di esecuzione, vedereBlocco di esecuzione dell'approvazione manuale.

1. Scegli Aggiungi un passaggio.
2. Seleziona il blocco Esecuzione manuale dell'approvazione e aggiungilo alla finestra di progettazione. Questo blocco consente la verifica umana prima di procedere.
3. Nel pannello di destra, configura il blocco:

   - Nome del passaggio: inserisci «Approvazione manuale prima della configurazione»

- Descrizione della fase (opzionale)
- Ruolo di approvazione IAM: il ruolo che un utente deve assumere per approvare l'esecuzione
- Timeout (opzionale). Dopo il timeout, l'esecuzione viene messa in pausa e puoi scegliere di riprovare, saltare o annullare.

Per informazioni sulle autorizzazioni IAM richieste per questo blocco di esecuzione, consulta. Esempio di politica di approvazione manuale, blocco di esecuzione

4. Scegli Salva passaggio.

Aggiungi un blocco di esecuzione Lambda ad azione personalizzata per la pagina di manutenzione

Per ulteriori informazioni su questo blocco di esecuzione, vedereBlocco di esecuzione Lambda ad azione personalizzata.

1. Scegli Aggiungi un passaggio.
2. Seleziona il blocco di esecuzione Lambda dell'azione personalizzata, quindi scegli Aggiungi e modifica. Questo blocco pubblica una pagina di manutenzione nella Regione che si sta attivando.
3. Nel pannello di destra, configura il blocco:

   - Nome del passaggio: inserisci «Visualizza la pagina di manutenzione»
   - Descrizione della fase (opzionale)
   - Lambda ARN per l'attivazione di us-east-1: l'ARN della funzione Lambda della pagina di manutenzione implementata in us-east-1
   - Lambda ARN per l'attivazione di us-west-2: l'ARN della funzione Lambda della pagina di manutenzione implementata in us-west-2
   - Regione per eseguire la funzione Lambda: scegli Esegui nella regione di attivazione
   - Timeout (opzionale)
   - Intervallo tra tentativi (opzionale)

   Per informazioni sulle autorizzazioni IAM richieste per questo blocco di esecuzione, consulta. Politica di esempio del blocco di esecuzione Lambda ad azione personalizzata

4. Scegli Salva passaggio.

Aggiungi il blocco di esecuzione Aurora Global Database

Per ulteriori informazioni su questo blocco di esecuzione, consultaBlocco di esecuzione di Amazon Aurora Global Database.

1. Scegli Aggiungi un passaggio.
2. Seleziona il blocco di esecuzione Aurora Global Database, quindi scegli Aggiungi e modifica. Questo blocco attiva uno switchover globale del database Aurora (nessuna perdita di dati). Per ulteriori informazioni, vedere Uso dello switchover o del failover per Aurora Global Database nella Guida per l'utente di Aurora.
3. Nel pannello di destra, configura il blocco:

   - Nome del passaggio: Enter Aurora switchover
   - Descrizione della fase (opzionale)
   - Identificatore globale del database Aurora: il nome del cluster Aurora
   - ARN del cluster utilizzato per l'attivazione di us-east-1: l'ARN del cluster Aurora in us-east-1
   - ARN del cluster utilizzato per l'attivazione di us-west-2: l'ARN del cluster Aurora in us-west-2
   - Seleziona l'opzione per il database Aurora: scegli Switchover
   - Timeout (opzionale)

   Per informazioni sulle autorizzazioni IAM richieste per questo blocco di esecuzione, consulta. Politica di esempio dei blocchi di esecuzione di Aurora Global Database
4. Scegli Salva passaggio.

Aggiungi il blocco di esecuzione del controllo di routing ARC

Per ulteriori informazioni su questo blocco di esecuzione, vedereBlocco di esecuzione del controllo del routing ARC.

1. Scegli Aggiungi un passaggio.
2. Seleziona il blocco di esecuzione del controllo del routing ARC, quindi scegli Aggiungi e modifica. Questo blocco esegue un failover DNS per spostare il traffico verso la regione passiva.
3. Nel pannello di destra, configura il blocco:

   - Nome del passaggio: Enter Toggle DNS
   - Descrizione della fase (opzionale)

- Controlli di routing utilizzati nell'attivazione di us-east-1: scegli Aggiungi controlli di routing
- Timeout: inserisci un valore di timeout.

4. Scegli Aggiungi controllo di routing:
   - ARN di controllo del routing: L'ARN del controllo di routing che controlla us-east-1
   - Stato di controllo del routing: scegli Attivato
5. Scegli nuovamente Aggiungi controllo del routing:
   - ARN di controllo del routing: L'ARN del controllo di routing che controlla us-west-2
   - Stato di controllo del routing: scegli Off
6. Scegli Save (Salva).
7. Controlli di routing utilizzati nell'attivazione di us-west-2: scegli Aggiungi controlli di routing
8. Scegli Aggiungi controllo di routing:
   - ARN di controllo del routing: L'ARN del controllo di routing che controlla us-west-2
   - Stato di controllo del routing: scegli Attivato
9. Scegli nuovamente Aggiungi controllo del routing:
   - ARN di controllo del routing: L'ARN del controllo di routing che controlla us-east-1
   - Stato di controllo del routing: scegli Off
10. Scegli Save (Salva).
11. Scegli Salva passaggio.

    Per informazioni sulle autorizzazioni IAM richieste per questo blocco di esecuzione, consultaIl routing ARC controlla la politica di esempio dei blocchi di esecuzione.
12. Scegli Save (Salva).

Fase 3: Esegui il piano

1. Nella pagina dei dettagli del piano Region Switch, in alto a destra, scegli Esegui.
2. Inserisci i dettagli dell'esecuzione:
   - Seleziona la regione da attivare.
   - Seleziona la modalità di esecuzione del piano.
   - (Facoltativo) Visualizza le fasi di esecuzione.

- Conferma l'esecuzione del piano.

3. Scegli Avvia.
4. È possibile visualizzare i passaggi dettagliati durante l'esecuzione del piano nella pagina dei dettagli di esecuzione. È possibile visualizzare ogni fase dell'esecuzione del piano, inclusi l'ora di inizio, l'ora di fine, l'ARN della risorsa e i messaggi di registro.

Una volta ripristinata la regione danneggiata, è possibile eseguire nuovamente il piano (modificando i parametri forniti) per attivare la regione originale e riportare le operazioni dell'applicazione alla regione principale originale.

Tutorial: configura la generazione automatica del rapporto di esecuzione del piano

Questo tutorial ti guida nella configurazione della generazione automatica dei report di esecuzione del piano per un piano di cambio di regione. I report forniscono una documentazione PDF completa sull'esecuzione dei piani ai fini della conformità.

In questo tutorial, completerai i seguenti passaggi:

- Crea un bucket Amazon S3 per l'archiviazione dei report
- Abilita la generazione automatica dei report su un piano di cambio di regione
- Esegui il piano e scarica il rapporto

Prerequisiti

Prima di iniziare questo tutorial, verifica di disporre di quanto segue:

- Un piano di cambio di regione esistente con flussi di lavoro configurati
- Autorizzazioni per creare bucket Amazon S3
- Il ruolo IAM di esecuzione del piano è stato configurato con le autorizzazioni richieste. Per ulteriori informazioni, consulta Autorizzazioni per l'esecuzione automatica dei report di esecuzione del piano.

Fase 1: creare un bucket Amazon S3 per i report

1. Apri la console Amazon S3 all'indirizzo. https://console.aws.amazon.com/s3/

2. Seleziona Crea bucket.
3. Fornisci i seguenti dettagli:
   - Nome del bucket: inserisci un nome univoco, ad esempio `my-region-switch-reports`
   - Blocca impostazioni di accesso pubblico: mantieni bloccato tutto l'accesso pubblico (consigliato)
   - Bucket Versioning: abilita il controllo delle versioni (opzionale ma consigliato)
   - Crittografia predefinita: seleziona la crittografia. Se si utilizza SSM-KMS, sono planExecutionRole necessari kms: Encrypt e kms: GenerateDataKey autorizzazioni sulla CMK predefinita del bucket s3
4. Seleziona Crea bucket.
5. Nota il nome del bucket da utilizzare nel passaggio successivo.

Passaggio 2: abilita la generazione automatica dei report nel tuo piano

1. Apri la console Region Switch all'indirizzo. https://console.aws.amazon.com/route53recovery/regionswitch/home
2. Seleziona il piano per cui desideri configurare i report.
3. Scegli Nella barra di navigazione, vai su Azioni e seleziona Modifica dettagli del piano.
4. Nella sezione Impostazioni del rapporto, fornisci quanto segue:
   - Seleziona Abilita la generazione automatica dei report
   - URI Amazon S3: seleziona o inserisci l'URI S3 del bucket che hai creato nella fase 1
   - ID dell'account proprietario del bucket: inserisci l'ID dell'account del proprietario del bucket
5. Scegli Save (Salva).
6. Attendi il completamento della valutazione del piano. In caso di problemi di configurazione, nella pagina dei dettagli del piano verranno visualizzati degli avvisi.

Fase 3: Esegui il piano e scarica il rapporto

1. Nella pagina dei dettagli del piano, scegli Esegui.
2. Completa l'esecuzione del piano normalmente, selezionando la regione da attivare e la modalità di esecuzione.
3. Una volta completata l'esecuzione del piano, vai alla pagina dei dettagli dell'esecuzione.

4. Nella sezione Report sull'esecuzione del piano, monitora lo stato di generazione del report. La generazione del report viene in genere completata entro 30 minuti dal completamento dell'esecuzione.
5. Quando lo stato del rapporto è Completato, scegli Scarica il rapporto sull'esecuzione del piano per scaricare il PDF.
6. In alternativa, accedi al tuo bucket Amazon S3 per accedere direttamente al report. I report vengono archiviati con il seguente schema di denominazione: `ExecutionReport-${planVersion.ownerAccountId}-${planName}-${execution.regionTo}-${event.executionId}-${dateStr}.pdf`

Il rapporto generato include:

- Riepilogo esecutivo con panoramica del servizio e data di creazione del report
- Pianifica i dettagli della configurazione così come esistevano al momento dell'esecuzione
- Cronologia dettagliata dell'esecuzione con passaggi, risorse interessate e stati
- Pianifica gli avvisi presenti all'inizio dell'esecuzione
- Stati degli CloudWatch allarmi di Amazon e cronologia degli allarmi associati
- Per i piani per i genitori, i dettagli di configurazione ed esecuzione dei piani secondari
- Glossario di termini e concetti

Risoluzione dei problemi

Se la generazione del report fallisce, verifica quanto segue:

- Errori di autorizzazione: verifica che il ruolo di esecuzione disponga delle autorizzazioni IAM corrette. Per ulteriori informazioni, consulta Autorizzazioni per l'esecuzione automatica dei report di esecuzione del piano. Controlla gli avvisi di valutazione del piano per problemi di autorizzazione specifici.
- Accesso al bucket Amazon S3: assicurati che il bucket Amazon S3 esista e sia accessibile dalla regione in cui è configurato il piano. Verifica che le policy bucket non blocchino l'accesso dal ruolo di esecuzione.
- Crittografia dei bucket: se utilizzi chiavi KMS gestite dal cliente per la crittografia dei bucket, assicurati che il ruolo di esecuzione disponga delle autorizzazioni per utilizzare la chiave KMS.

Per ulteriore assistenza, visualizza i messaggi di errore dettagliati nella pagina dei dettagli di esecuzione o contatta l' AWS assistenza.

Tutorial: Esegui un flusso di lavoro post-ripristino RDS

Questo tutorial ti guida nell'esecuzione di un flusso di lavoro post-ripristino dopo un failover RDS riuscito. Questa esecuzione post-ripristino ripristina la ridondanza ristabilendo la replica tra regioni per il database RDS, assicurando che il database RDS sia pronto per i futuri eventi regionali.

In questo tutorial, completerai i seguenti passaggi:

- Verifica i prerequisiti per l'esecuzione dopo il ripristino
- Crea un flusso di lavoro post-ripristino con il blocco di esecuzione RDS Create Cross-Region Replica
- Esegui il flusso di lavoro post-ripristino

Prerequisiti

Prima di iniziare questo tutorial, verifica di disporre di quanto segue:

- Un active/passive piano di cambio di regione con un flusso di lavoro di attivazione che include un blocco di esecuzione RDS Promote Read Replica
- Un'esecuzione di attivazione riuscita che ha promosso una replica di lettura nell'altra regione
- Entrambe le regioni sono sane e accessibili
- L'ID di esecuzione dell'esecuzione di ripristino più recente

Passaggio 1: creare un flusso di lavoro post-ripristino

1. Dalla console Region Switch scegli il piano, scegli Modifica flussi di lavoro, seleziona Config, seleziona Includi il flusso di lavoro successivo al ripristino nel piano e salva.
2. Nella pagina Modifica flussi di lavoro, seleziona il menu a discesa Seleziona un flusso di lavoro per aggiungere passaggi e scegli Post-ripristino.
3. Scegli Aggiungi un passaggio.
4. Seleziona il blocco di esecuzione Amazon RDS create cross Region Replica.
5. Nel pannello di destra, configura il blocco:

- Nome del passaggio: inserisci «Crea una replica di lettura interregionale»
- Descrizione della fase (opzionale)
- ARN dell'istanza DB RDS per la regione primaria: l'ARN del database nella regione primaria deve essere lo stesso della fase di promozione della lettura della replica
- ARN dell'istanza DB RDS per la regione secondaria: l'ARN del database promosso nella fase secondaria deve essere lo stesso della fase di promozione della lettura della replica
- Timeout (opzionale): inserisci un valore di timeout, ad esempio 90 minuti

Per informazioni sulle autorizzazioni IAM richieste per questo blocco di esecuzione, consulta. Policy di esempio per i blocchi di esecuzione di Amazon RDS

6. Scegli Salva passaggio.
7. Scegli Salva flusso di lavoro.

Passaggio 2: Esegui il flusso di lavoro post-ripristino

1. Nella pagina dei dettagli del piano di cambio di regione, in alto a destra, scegli Esegui dopo il ripristino.
2. Inserisci i dettagli dell'esecuzione:
   - ID di esecuzione del ripristino: inserire l'ID di esecuzione dell'esecuzione di ripristino più recente. Questo campo viene utilizzato per identificare la regione attualmente attiva.
   - Regione in cui eseguire: seleziona la regione inattiva che non riceve alcun traffico applicativo. Questa è la regione in cui verrà creata una replica di lettura.
3. Esamina i passaggi di esecuzione e conferma l'esecuzione.
4. Selezionare Start Execution (Avvia esecuzione).
5. Monitora l'avanzamento dell'esecuzione nella pagina dei dettagli dell'esecuzione. Il blocco di esecuzione RDS Create Cross-Region Replica rinominerà la vecchia istanza primaria e creerà una nuova replica di lettura nella regione precedentemente compromessa.

Una volta completata correttamente l'esecuzione post-ripristino, la replica tra regioni dell'applicazione verrà ripristinata e sarete pronti per i futuri eventi regionali. È possibile verificare se la nuova replica di lettura è stata creata controllando la console RDS nella regione di destinazione. La vecchia versione principale verrà rinominata e contrassegnata con Switch. renamedByRegion

> **Important**
>
> Il cambio di regione verifica che l'ID di esecuzione del ripristino corrisponda all'ultima esecuzione nota per il piano. Se l'ID di esecuzione non è valido o non è l'ID dell'ultima esecuzione di ripristino nota, l'esecuzione successiva al ripristino non verrà eseguita.

Operazioni API di cambio di regione

La tabella seguente elenca le operazioni ARC che è possibile utilizzare per il cambio di regione, con collegamenti alla documentazione pertinente.

Azione	Utilizzo della console ARC	Utilizzando l'API ARC	API del piano dati
Approva o nega una fase di esecuzione del piano	Consulta Blocco di esecuzione dell'approvazione manuale.	Consulta la sezione ApprovePlanExecutionStep	Sì
Annullare l'esecuzione di un piano	Consulta Crea un piano di cambio di regione.	Consulta la sezione CancelPlanExecution	Sì
Creare un piano	Consulta Crea un piano di cambio di regione.	Consulta la sezione CreatePlan	No
Eliminare un piano	Consulta Lavorare con Region Switch.	Consulta la sezione DeletePlan	No
Procurati un piano	Consulta Lavorare con Region Switch.	Consulta la sezione GetPlan	No
Ottieni lo stato di valutazione del piano	Consulta Valutazione del piano.	Consulta la sezione GetPlanEvaluationStatus	Sì

Azione	Utilizzo della console ARC	Utilizzando l'API ARC	API del piano dati
Ottieni l'esecuzione di un piano	Consulta Dashboard di cambio di regione.	Consulta la sezione GetPlanExecution	Sì
Prepara un piano in Region	Consulta Lavorare con Region Switch.	Consulta la sezione GetPlanInRegion	Sì
Elenca gli eventi di esecuzione del piano	Consulta Esegui un piano di cambio di regione per ripristinare un'applicazione.	Consulta la sezione ListPlanExecutionEvents	Sì
Elenca le esecuzioni dei piani	Consulta Esegui un piano di cambio di regione per ripristinare un'applicazione.	Consulta la sezione ListPlanExecutions	Sì
Elenca i piani	Consulta Lavorare con Region Switch.	Consulta la sezione ListPlans	No
Elenca i piani nella regione	Consulta Lavorare con Region Switch.	Consulta la sezione ListPlansInRegion	Sì
Elenca i controlli sanitari della Route 53 per un piano	Per informazioni, consultare Blocco di esecuzione del controllo dello stato di Amazon Route 53.	Vedi ListRoute53HealthChecksForPlan	No
Elenca i controlli sanitari della Route 53 per un piano nella regione	Per informazioni, consultare Blocco di esecuzione del controllo dello stato di Amazon Route 53.	Vedi ListRoute53HealthChecksForPlanInRegion	Sì

Azione	Utilizzo della console ARC	Utilizzando l'API ARC	API del piano dati
Elencare i tag associati a una risorsa	Consulta Etichettatura per lo switch ARC Region;.	Consulta la sezione ListTagsForResource	No
Avvia l'esecuzione di un piano	Consulta Esegui un piano di cambio di regione per ripristinare un'applicazione.	Consulta la sezione StartPlanExecution	Sì
Applicazione di tag a una risorsa	Consulta Crea un piano di cambio di regione.	Consulta la sezione TagResource	No
Rimuovere i tag da una risorsa	Consulta Etichettatura per lo switch ARC Region;.	Consulta la sezione UntagResource	No
Aggiornare un piano	Consulta Crea un piano di cambio di regione.	Consulta la sezione UpdatePlan	No
Aggiornare l'esecuzione di un piano	Consulta Crea un piano di cambio di regione.	Consulta la sezione UpdatePlanExecution	Sì
Aggiornare una fase di esecuzione del piano	Consulta Crea un piano di cambio di regione.	Consulta la sezione UpdatePlanExecutionStep	Sì

Lavorare con Region Switch

Questa sezione fornisce step-by-step istruzioni per utilizzare i piani di cambio di regione, che è possibile utilizzare per ripristinare applicazioni multiregionali. Il cambio di regione consente di creare piani per entrambi gli approcci active/passive di active/active ripristino.

Per creare un piano di ripristino per l'applicazione, procedi come segue:

1. Crea un piano di cambio di regione. Un piano è una struttura con determinati attributi, ad esempio lo specifico in Regioni AWS cui viene eseguita l'applicazione. Ogni piano include uno o più flussi di lavoro.

   Facoltativamente, puoi creare diversi piani e inserirli in un piano di recupero generale.
2. Crea un flusso di lavoro per il piano. Non puoi eseguire un piano senza prima creare un flusso di lavoro.
3. Nel flusso di lavoro, aggiungi uno o più passaggi, ciascuno dei quali è un blocco di esecuzione.

   Ad esempio, puoi aggiungere un passaggio per scalare i gruppi di Auto Scaling EC2 in una regione di destinazione.
4. Dopo aver aggiunto passaggi al flusso di lavoro, potrebbero essere necessari passaggi aggiuntivi, come la configurazione dei controlli di integrità in Amazon Route 53. Ogni sezione del blocco di esecuzione include le informazioni di configurazione necessarie. Per ulteriori informazioni, consulta Aggiungere blocchi di esecuzione.
5. Per ripristinare l'applicazione quando è in esecuzione in un ambiente con problemi Regione AWS, esegui il piano.

   È possibile tenere traccia dello stato di avanzamento dell'esecuzione di un piano visualizzando le informazioni nella dashboard globale o nella dashboard regionale.

Le sezioni seguenti forniscono informazioni dettagliate e passaggi per creare un piano e flussi di lavoro e aggiungere fasi di blocco di esecuzione nei flussi di lavoro.

Indice

- Crea un piano di cambio di regione
- Crea flussi di lavoro del piano Region Switch
- Aggiungere blocchi di esecuzione
- Crea piani per bambini
- Crea un trigger per un piano di cambio di regione
- Esegui un piano di cambio di regione per ripristinare un'applicazione

Le procedure in questa sezione illustrano come utilizzare piani, flussi di lavoro, blocchi di esecuzione e trigger utilizzando. Console di gestione AWS Per utilizzare invece le operazioni dell'API Region Switch, consulta. Operazioni API di cambio di regione

Crea un piano di cambio di regione

Puoi creare due diversi tipi di piani in Region switch: un active/active piano o un active/passive piano. Quando crei un piano, specifica il tipo che si applica al modo in cui desideri gestire il failover.

- Un approccio attivo/passivo implementa due repliche di applicazioni in due regioni, con il traffico indirizzato solo verso la regione attiva. È possibile attivare la replica nella regione passiva eseguendo il piano di commutazione di regione.
- Un approccio attivo/attivo implementa due repliche di applicazioni in due regioni ed entrambe le repliche elaborano il lavoro o ricevono traffico.

Per creare un piano di cambio di regione

1. Dalla console Region Switch, scegli Crea un piano di cambio di regione con active/passive approccio.
2. Fornisci i seguenti dettagli:
   - Nome del piano: inserisci un nome descrittivo per il piano.
   - Approccio multiregionale: seleziona Attivo/passivo o Attivo/attivo. Questo approccio significa che due repliche delle applicazioni vengono distribuite in due regioni, con il traffico instradato solo nella regione attiva. È possibile attivare la replica nella regione passiva eseguendo il piano di commutazione di regione.
     - Scegli attivo/passivo se hai distribuito due repliche di applicazioni in due regioni, con il traffico indirizzato solo verso la regione attiva. È quindi possibile attivare la replica nella regione passiva eseguendo il piano di cambio di regione che specifica Attivo/passivo.
     - Scegliete Attiva/attiva se avete distribuito due repliche di applicazioni in due regioni ed entrambe le repliche stanno elaborando il lavoro o ricevendo traffico.
   - Regioni o regioni primarie e di standby: seleziona le regioni principali e di standby per l'applicazione. Per una active/active distribuzione, seleziona le regioni in cui vengono distribuite le repliche.
   - Obiettivo del tempo di ripristino (RTO): immettere l'RTO desiderato. Region Switch lo utilizza per fornire informazioni sul tempo impiegato per completare l'esecuzione del piano di cambio di regione rispetto all'RTO desiderato.

- Ruolo IAM: fornisci un ruolo IAM per Region Switch da utilizzare per eseguire il piano. Per ulteriori informazioni sulle autorizzazioni, consultare Identity and Access Management per lo switch di regione in ARC.
- CloudWatch Allarme Amazon: fornisci un allarme sullo stato dell'applicazione che hai creato con Amazon CloudWatch, per indicare lo stato della tua applicazione in ogni regione. Il cambio di regione utilizza questi allarmi sullo stato delle applicazioni per determinare il tempo di ripristino effettivo dopo aver cambiato regione per implementare il ripristino.

  Prima di aggiungere CloudWatch allarmi a un piano di cambio di regione, assicurati di disporre della politica IAM corretta. Per ulteriori informazioni, consulta CloudWatch allarmi per le autorizzazioni di integrità dell'applicazione.
- Generazione automatica di report: facoltativamente, abilita la generazione automatica di report per l'esecuzione dei piani. Se abilitato, Region Switch genera un report PDF completo al termine di ogni esecuzione del piano e lo consegna a un bucket Amazon S3 specificato dall'utente. Fornisci l'URI di Amazon S3 e l'ID dell'account proprietario del bucket.

  Prima di abilitare la generazione automatica di report per i piani, assicurati di disporre della politica IAM corretta. Per ulteriori informazioni sulla generazione di report e sulle autorizzazioni richieste, consultaRapporti automatici sull'esecuzione del piano.
- Tag: facoltativamente, aggiungi uno o più tag al tuo piano.

Crea flussi di lavoro del piano Region Switch

Dopo aver creato un piano di cambio di regione, è necessario definire e creare flussi di lavoro che specifichino il processo di ripristino dell'applicazione. Per ogni piano, definisci uno o più flussi di lavoro che completano il ripristino dell'applicazione. In ogni flusso di lavoro, aggiungi passaggi che includono blocchi di esecuzione che definiscono ogni azione che Region Switch deve eseguire per il ripristino dell'applicazione.

Il numero di flussi di lavoro creati dipende dallo scenario di distribuzione dell'applicazione e dalle preferenze di gestione del ripristino. Esempio:

- Se il tuo piano di cambio di regione prevede active/active application deployment, you also need to create a deactivation workflow. This means that for or active/active distribuzioni, avrai un minimo di due flussi di lavoro: un flusso di lavoro di attivazione e uno di disattivazione.

- Se il tuo piano di cambio di regione prevede la distribuzione di un' active/passive applicazione, hai una regione principale e una secondaria. Se scegli di avere flussi di lavoro di attivazione separati per ogni regione, creerai due flussi di lavoro: uno per ogni regione.

Per creare flussi di lavoro tra piani di cambio di regione

1. Nel piano di cambio di regione che hai creato, scegli Crea flussi di lavoro.
2. Seleziona una delle seguenti opzioni di flusso di lavoro:
   - Crea lo stesso flusso di lavoro di attivazione per tutte le regioni: consente di utilizzare lo stesso flusso di lavoro di attivazione in tutte le regioni.
   - Crea flussi di lavoro separatamente per ogni regione: crea un flusso di lavoro di attivazione individuale per ogni regione.
3. Facoltativamente, fornisci una descrizione per ogni flusso di lavoro.
4. Definite il flusso di lavoro necessario per ripristinare l'applicazione. Nel flusso di lavoro, aggiungete blocchi di esecuzione per definire i passaggi che desiderate che Region Switch esegua per il ripristino. Ogni blocco di esecuzione definisce azioni, come il reindirizzamento del traffico delle applicazioni o il ripristino del database in una regione di attivazione, e supporta le risorse in un'altra. Account AWS Puoi scegliere di far eseguire i blocchi di esecuzione in parallelo o in sequenza. Per informazioni dettagliate sui blocchi di esecuzione specifici che puoi aggiungere ai flussi di lavoro, consulta. Aggiungere blocchi di esecuzione
5. A seconda dell'opzione di workflow selezionata, procedi come segue:
   - Se hai selezionato Crea lo stesso flusso di lavoro di attivazione per tutte le regioni, è necessario un unico flusso di lavoro di attivazione.
   - Se hai selezionato Crea flussi di lavoro separatamente per ogni regione, sono necessari due flussi di lavoro di attivazione.

   Per active/active i piani, è necessario definire sia un flusso di lavoro di attivazione che uno di disattivazione.

Aggiungere blocchi di esecuzione

È necessario aggiungere passaggi ai flussi di lavoro del piano Region Switch, per eseguire i singoli passaggi per completare il failover o lo switchover dell'applicazione. Per informazioni dettagliate sulla funzionalità e sul comportamento di ogni tipo di blocco di esecuzione, vedere le seguenti descrizioni.

Region switch esegue una valutazione del piano immediatamente dopo la creazione o l'aggiornamento di un piano e successivamente ogni 30 minuti durante lo stato stazionario. Region switch memorizza le informazioni sulla valutazione del piano in tutte le regioni in cui è configurato il piano. Ogni sezione relativa ai blocchi di esecuzione include informazioni su ciò che viene valutato quando Region Switch esegue la valutazione del piano.

Region switch include tipi di blocchi di esecuzione che aiutano a scalare le risorse di calcolo come parte del ripristino. Se utilizzi questi blocchi di esecuzione in un piano, tieni presente che Region Switch non garantisce il raggiungimento della capacità di elaborazione desiderata. Se disponi di un'applicazione critica e devi garantire l'accesso alla capacità, ti consigliamo di riservare la capacità. Esistono strategie che puoi seguire per riservare la capacità di elaborazione in una regione secondaria limitando al contempo i costi. Per ulteriori informazioni, consulta Pilot light with reserved capacity: come ottimizzare i costi di disaster recovery utilizzando On-Demand Capacity Reservations.

Lo switch di regione supporta i seguenti blocchi di esecuzione.

Blocco di esecuzione	Funzione	Configurazione sgradevole
Blocco di esecuzione del piano di switch ARC Region	Orchestra il ripristino per più applicazioni in un'unica esecuzione specificando i piani secondari da eseguire.	Avvia i piani per bambini con le loro configurazioni sgradevoli.
Blocco di esecuzione di gruppo Amazon EC2 Auto Scaling	Ridimensiona le risorse di calcolo EC2 che si trovano in un gruppo Auto Scaling come parte dell'esecuzione del piano.	Specificate la percentuale minima di capacità di elaborazione che deve corrispondere nella regione che state attivando.
Blocco di esecuzione per la scalabilità delle risorse di Amazon EKS	Ridimensiona i cluster pod Amazon EKS come parte dell'esecuzione del piano.	N/D

Blocco di esecuzione	Funzione	Configurazione sgradevole
Blocco di esecuzione per la scalabilità del servizio Amazon ECS	Ridimensiona le attività del servizio Amazon ECS come parte dell'esecuzione del piano.	N/D
Blocco di esecuzione del controllo del routing ARC	Aggiungi un passaggio per modificare lo stato di uno o più controlli di routing ARC, per reindirizzare il traffico dell'applicazione verso una destinazione. Regione AWS	N/D
Blocco di esecuzione di Amazon Aurora Global Database	Esegui un flusso di lavoro di ripristino per un database globale Aurora.	Esegui un failover dei database globali Aurora (può potenzialmente causare la perdita di dati).
Blocco di esecuzione di Amazon DocumentDB Global Cluster	Esegui un flusso di lavoro di ripristino per un cluster globale Amazon DocumentDB.	Esegui un failover globale del cluster Amazon DocumentDB (può potenzialmente causare la perdita di dati).
Blocco di esecuzione Amazon RDS Promote Read Replica	Promuovi una replica di lettura di Amazon RDS in un'istanza di database autonoma.	N/D
Blocco di esecuzione Amazon RDS Create Cross-Region Replica	Crea una replica di lettura interregionale per un'istanza di database Amazon RDS come parte del processo di post-ripristino.	N/D

Blocco di esecuzione	Funzione	Configurazione sgradevole
Blocco di esecuzione dell'approvazione manuale	Inserisci una fase di approvazione per richiedere l'approvazione o l'annullamento di un'esecuzione prima di procedere.	N/D
Blocco di esecuzione Lambda ad azione personalizzata	Aggiungi un passaggio personalizzato per l'esecuzione di una funzione Lambda, per abilitare azioni personalizzate.	Salta il passaggio.
Blocco di esecuzione del controllo dello stato di Amazon Route 53	Speciifica le regioni verso le quali verrà reindirizzato il traffico dell'applicazione durante il failover.	N/D

Blocco di esecuzione del piano di switch ARC Region

Il blocco di esecuzione del piano di cambio di regione consente di orchestrare l'ordine in cui più applicazioni passano alla regione che si desidera attivare, facendo riferimento ad altri piani secondari di cambio di regione. Utilizzando questa relazione padre/figlio, è possibile creare processi di ripristino complessi e coordinati che gestiscono più risorse e dipendenze nell'infrastruttura.

Configurazione

Quando si utilizza il blocco di esecuzione del piano di cambio di regione, si seleziona uno specifico piano di cambio di regione che si desidera eseguire nel flusso di lavoro del piano che si sta creando.

> **Important**
>
> Prima di configurare il blocco di esecuzione, assicurati di disporre della politica IAM corretta. Per ulteriori informazioni, consulta Esempio di politica di esempio per l'esecuzione del piano di cambio di regione.

Per configurare un blocco di esecuzione del piano Region Switch, inserisci i seguenti valori:

1. Nome della fase: inserisci un nome.
2. Descrizione della fase (opzionale): inserisci una descrizione della fase.
3. Piano di cambio di regione: seleziona un piano da eseguire nel flusso di lavoro per il piano corrente.

Quindi, scegli Salva passaggio.

Come funziona

Utilizza il blocco di esecuzione del piano Region Switch per creare flussi di lavoro principali con parent/child relazioni. Tieni presente che questo blocco di esecuzione non supporta livelli aggiuntivi di piani figlio e limita il numero di piani genitore-figlio. I piani per bambini devono supportare le stesse regioni supportate dal piano principale e devono avere lo stesso approccio di recupero del piano principale (active/active ovvero attivo/passivo).

Questo blocco supporta modalità di esecuzione sia graceful che ungraceful. Le impostazioni sgradevoli avvieranno i piani per bambini con la loro configurazione sgradevole. Se il blocco Region Switch è stato eseguito correttamente e poi è passato alla modalità di esecuzione non corretta, anche qualsiasi piano secondario passerà alla modalità di esecuzione non corretta.

Cosa viene valutato nell'ambito della valutazione del piano

Se condividi un piano tra più account e il piano non è più condiviso con l'account del piano principale, Region switch evaluation restituisce un avviso che indica che il piano non è valido.

Blocco di esecuzione di gruppo Amazon EC2 Auto Scaling

Il blocco di esecuzione di gruppo EC2 Auto Scaling consente di scalare le istanze EC2 come parte del processo di ripristino multiregionale. Puoi definire una percentuale di capacità rispetto alla regione che stai lasciando (origine e destinazione).

Configurazione

Quando configuri il blocco di esecuzione di gruppo EC2 Auto Scaling, inserisci gli ARN EC2 Auto Scaling per le regioni specifiche associate al tuo piano. È necessario inserire EC2 ARNs Auto Scaling in ogni regione che si desidera aumentare durante l'esecuzione del piano.

> **Important**
>
> Prima di configurare il blocco di esecuzione, assicurati di disporre della politica IAM corretta. Per ulteriori informazioni, consulta Politica di esempio per i blocchi di esecuzione di EC2 Auto Scaling.

Per configurare un blocco di esecuzione di gruppo EC2 Auto Scaling, inserisci i seguenti valori:

1. Nome della fase: inserisci un nome.
2. Descrizione della fase (opzionale): inserisci una descrizione della fase.
3. ARN per regione del gruppo EC2 Auto Scaling: inserisci l'ARN per il gruppo Auto Scaling EC2 in ogni regione del tuo piano.
4. Percentuale corrispondente alla capacità della Regione attivata: Inserisci la percentuale desiderata del numero di istanze in esecuzione nel gruppo Auto Scaling da corrispondere per la Regione attivata.
5. Approccio al monitoraggio della capacità: seleziona uno dei seguenti approcci per il monitoraggio della capacità per i tuoi gruppi di Auto Scaling EC2:
   - Capacità operativa massima campionata nell'arco di 24 ore: scegli questa opzione per utilizzare il valore di capacità desiderata specificato nella configurazione del gruppo EC2 Auto Scaling. Questa opzione non crea costi aggiuntivi, ma è potenzialmente meno accurata rispetto all'utilizzo dell'altra opzione, le metriche. CloudWatch

     Nell'API Region Switch, questa opzione corrisponde alla specificazione`sampledMaxInLast24Hours`.

     Per ulteriori informazioni, consulta la sezione Impostazione dei limiti di scalabilità per il gruppo Auto Scaling nella Guida per l'utente di Amazon EC2 Auto Scaling.
   - Capacità operativa massima campionata in 24 ore con CloudWatch: scegli questa opzione per utilizzare i parametri specificati in Amazon CloudWatch for EC2 Auto Scaling. L'utilizzo dell'opzione può essere più accurato, ma comporta costi aggiuntivi legati all'utilizzo delle metriche. CloudWatch

     Nell'API Region Switch, questa opzione corrisponde alla specificazione. `autoscalingMaxInLast24Hours`

Per utilizzare questa opzione, devi prima abilitare le metriche di gruppo per i tuoi gruppi di Auto Scaling. Per ulteriori informazioni, consulta Enable Auto Scaling group metrics nella Amazon EC2 Auto Scaling User Guide.

6. Timeout: inserisci un valore di timeout.

Quindi, scegli Salva passaggio.

Come funziona

Dopo aver configurato un blocco di esecuzione di EC2 Auto Scaling, Region switch conferma che esiste un solo gruppo Auto Scaling di origine e un gruppo Auto Scaling di destinazione. Se sono presenti più gruppi di Auto Scaling, il blocco di esecuzione fallisce durante la valutazione del piano. La capacità target è definita come il numero di istanze con uno stato impostato su. `InService` Per ulteriori informazioni, consulta Ciclo di vita delle istanze EC2 Auto Scaling.

In base al valore specificato (quando si configura il blocco di esecuzione Auto Scaling) per una percentuale corrispondente, Region switch calcola la nuova capacità desiderata per il gruppo Auto Scaling di destinazione. La nuova capacità desiderata viene confrontata con la capacità desiderata del gruppo Auto Scaling di destinazione. La formula utilizzata da Region switch per calcolare la capacità desiderata è la seguente:`ceil(percentToMatch * Source Auto Scaling group capacity)`, dove ceil () è una funzione che arrotonda qualsiasi risultato frazionario. Se la capacità attuale desiderata del gruppo Auto Scaling di destinazione è maggiore o uguale alla capacità desiderata del nuovo gruppo Auto Scaling calcolato dallo switch di regione, il blocco di esecuzione procede. Si noti che il cambio di regione non riduce la capacità del gruppo Auto Scaling.

Quando Region switch esegue un blocco Auto Scaling, Region switch tenta di aumentare la capacità del gruppo Region Auto Scaling di destinazione in modo che corrisponda alla capacità desiderata. Quindi, il cambio di regione attende che la capacità del gruppo Auto Scaling richiesta sia soddisfatta nel gruppo Auto Scaling della regione di destinazione prima che il cambio di regione proceda alla fase successiva del piano.

> **Note**
>
> L'esecuzione di questo blocco modifica le impostazioni di capacità minima e desiderata dei gruppi di Auto Scaling, il che può causare variazioni di configurazione se gestisci questi valori infrastructure-as-code tramite strumenti o altre automazioni. Assicuratevi che i processi

di gestione della configurazione tengano conto di queste modifiche per evitare rollback involontari.

Se utilizzi un active/active approccio, Region switch utilizza l'altra regione configurata come origine. In altre parole, se una regione viene disattivata, il cambio di regione utilizza l'altra regione attiva come fonte per determinare la percentuale da scalare.

Questo blocco supporta sia le modalità di esecuzione graziose che le modalità di esecuzione ungraceful. È possibile configurare un'esecuzione non autorizzata specificando la percentuale minima di capacità di elaborazione da abbinare nella regione di destinazione prima che il passaggio alla fase successiva del piano passi al passaggio successivo.

Cosa viene valutato nell'ambito della valutazione del piano

Quando Region switch valuta il piano, Region switch esegue diversi controlli critici sulla configurazione e sulle autorizzazioni del blocco di esecuzione del gruppo EC2 Auto Scaling. La valutazione dei cambi di regione verifica che i gruppi Auto Scaling siano presenti in entrambe le regioni, assicura che siano configurati e accessibili correttamente e rileva il numero di istanze in esecuzione in ciascuna regione. Conferma inoltre che la capacità massima nel gruppo Auto Scaling della regione di destinazione è sufficiente per gestire la corrispondenza percentuale specificata della scala per la capacità richiesta.

Il cambio di regione verifica inoltre che il ruolo IAM del piano disponga delle autorizzazioni corrette per Auto Scaling. Per ulteriori informazioni sulle autorizzazioni richieste per i blocchi di esecuzione degli switch di regione, vedere. Esempi di politiche basate sull'identità per Region Switch in ARC
Se uno qualsiasi dei controlli fallisce, Region Switch restituisce messaggi di avviso, che è possibile visualizzare nella console. In alternativa, puoi ricevere gli avvisi di convalida tramite EventBridge o utilizzando le operazioni API.

Blocco di esecuzione per la scalabilità delle risorse di Amazon EKS

Il blocco di esecuzione per la scalabilità delle risorse EKS consente di scalare le risorse EKS come parte del processo di ripristino multiregionale. Quando si configura il blocco di esecuzione, si definisce una percentuale di capacità da scalare, rispetto alla capacità nella regione che viene disattivata.

Configura le autorizzazioni di accesso EKS

Prima di poter aggiungere una fase per la scalabilità delle risorse EKS, devi fornire a Region Switch le autorizzazioni necessarie per intraprendere azioni con le risorse Kubernetes nei tuoi cluster EKS. Per fornire l'accesso a Region switch, è necessario creare una voce di accesso EKS per il ruolo IAM utilizzato da Region switch per l'esecuzione del piano, utilizzando la seguente politica di accesso Region switch: `arn:aws:eks::aws:cluster-access-policy/AmazonARCRegionSwitchScalingPolicy`

Region Switch: politica di accesso EKS

Le seguenti informazioni forniscono dettagli sulla politica di accesso EKS.

Nome: `AmazonARCRegionSwitchScalingPolicy`

ARN della politica: `arn:aws:eks::aws:cluster-access-policy/AmazonARCRegionSwitchScalingPolicy`

Gruppi di API Kubernetes	Risorse di Kubernetes	Verbi di Kubernetes (autorizz azioni)
*	*/scala	ottieni, aggiorna
*	*/stato	get
scalabilità automatica	scalatori automatici a podi orizzontali	prendi, patch

Crea una voce di accesso EKS per Region Switch

L'esempio seguente descrive come creare le associazioni di accesso e politiche di accesso richieste in modo che Region Switch possa eseguire azioni specifiche per le tue risorse Kubernetes. In questo esempio, le autorizzazioni si applicano allo spazio dei nomi *`my-namespace1`* nel cluster EKS per il ruolo IAM. *`my-cluster`* `arn:aws:iam::555555555555:role/`*`my-role`*

Quando configuri queste autorizzazioni, assicurati di eseguire questi passaggi per entrambi i cluster EKS nel blocco di esecuzione.

Prerequisito

Prima di iniziare, modifica la modalità di autenticazione del cluster in una delle due `API_AND_CONFIG_MAP` opzioni. `API` La modifica della modalità di autorizzazione aggiunge l'API per le voci di accesso. Per ulteriori informazioni, consulta Modifica della modalità di autenticazione per utilizzare le voci di accesso nella Amazon EKS User Guide.

Crea la voce di accesso

Il primo passaggio consiste nel creare la voce di accesso utilizzando un AWS CLI comando simile al seguente:

```
aws eks create-access-entry --cluster-name my-cluster --principal-arn
        arn:aws:iam::555555555555:user/my-user --type STANDARD
```

Per ulteriori informazioni, consulta Creare voci di accesso nella Amazon EKS User Guide.

Crea l'associazione di immissione degli accessi

Quindi, create l'associazione alla politica di accesso Region Switch utilizzando un AWS CLI comando simile al seguente:

```
aws eks associate-access-policy --cluster-name my-cluster --principal-arn
 arn:aws:iam::555555555555:role/my-role \
         --access-scope type=namespace,namespaces=my-namespace1 --policy-arn
         arn:aws:eks::aws:cluster-access-policy/AmazonARCRegionSwitchScalingPolicy
```

Per ulteriori informazioni, consulta Associare le politiche di accesso alle voci di accesso nella Amazon EKS User Guide.

Assicurati di ripetere questi passaggi con il secondo cluster EKS nel blocco di esecuzione, nell'altra regione, per assicurarti che sia possibile accedere a entrambi i cluster tramite lo switch di regione.

Configurazione

> **Important**
>
> Prima di aggiungere una fase di scalabilità delle risorse EKS, assicurati innanzitutto di aver configurato le autorizzazioni corrette. Per ulteriori informazioni, consulta Configura le autorizzazioni di accesso EKS. Assicurati inoltre di disporre della politica IAM corretta. Per

ulteriori informazioni, consulta Esempio di policy di esempio per la scalabilità delle risorse di Amazon EKS.

Nota che Region switch attualmente supporta le seguenti ReplicaSet risorse: apps/v1, Deployment, and apps/v 1.

Per la configurazione del blocco di esecuzione, immettere i seguenti valori.

1. Nome della fase: inserisci un nome.
2. Descrizione della fase (opzionale): inserisci una descrizione della fase.
3. Nome dell'applicazione: inserisci il nome della tua applicazione EKS, ad esempio myApplication.
4. Tipo di risorsa Kubernetes: inserisci il tipo di risorsa per l'applicazione, ad esempio Deployment.
5. Risorsa per regione: per ogni regione, inserisci le informazioni per il cluster EKS, incluso l'ARN del cluster EKS, lo spazio dei nomi delle risorse e così via.
6. Percentuale corrispondente alla capacità della regione attivata: inserisci la percentuale desiderata di pod funzionanti nella regione di origine in modo che corrisponda alla regione attivata.
7. Approccio al monitoraggio della capacità: l'unica opzione per il monitoraggio della capacità è già stata selezionata, la capacità operativa massima è stata campionata nell'arco di 24 ore.

   Questo approccio di monitoraggio della capacità utilizza il `ReplicaCount` valore per le richieste di assistenza EKS. Per ulteriori informazioni, consulta Informazioni sullo spostamento zonale ARC in Amazon EKS nella Amazon Elastic Kubernetes Service User Guide.
8. Timeout: inserisci un valore di timeout.

Quindi, scegli Salva passaggio.

Come funziona

Durante l'esecuzione di un piano, Region switch recupera il numero massimo di repliche campionate nelle 24 ore precedenti per la risorsa di destinazione nella regione che stai attivando. Quindi, calcola il numero di repliche desiderato per la risorsa di destinazione utilizzando la seguente formula: `ceil(percentToMatch * Source replica count)`

Se il numero di repliche pronte per la destinazione è inferiore al valore desiderato, Region Switch ridimensiona il valore di replica della risorsa di destinazione in base alla capacità desiderata. Attende

che le repliche siano pronte, sfruttando lo scaler automatico del nodo per aumentare la capacità dei nodi, se necessario.

Se il `hpaName` campo opzionale non è vuoto, Region switch lo patcherà HorizontalPodAutoscaler per impedire qualsiasi ridimensionamento automatico durante o dopo l'esecuzione utilizzando la seguente patch: `{"spec":{"behavior":{"scaleDown": {"selectPolicy":"Disabled"}}}}`

Assicurati di configurare qualsiasi strumento di correzione delle deviazioni, come gli GitOps strumenti, in modo che ignori il campo di replica per le risorse della patch, oltre al campo. HorizontalPodAutoscaler

Cosa viene valutato nell'ambito della valutazione del piano

Quando Region switch valuta il piano, Region switch esegue diversi controlli sul blocco di esecuzione EKS configurato e sulle autorizzazioni. Region switch verifica che il ruolo IAM del piano disponga delle autorizzazioni corrette per descrivere i cluster EKS ed elencare le politiche di accesso associate. Region switch verifica inoltre che il ruolo IAM sia associato alla corretta policy di Access Entry, in modo che Region switch disponga delle autorizzazioni necessarie per agire sulle risorse Kubernetes. Infine, Region Switch conferma l'esistenza dei cluster EKS e delle risorse Kubernetes configurati.

Inoltre, Region switch verifica di aver raccolto e archiviato correttamente i dati di monitoraggio necessari (numero di repliche Kubernetes) e acquisisce il numero di pod in esecuzione necessari per eseguire il piano di switch di regione.

Blocco di esecuzione per la scalabilità del servizio Amazon ECS

Il blocco di esecuzione della scalabilità del servizio ECS consente di scalare il servizio ECS in una regione di destinazione come parte del processo di ripristino multiregionale. È possibile definire una percentuale di capacità rispetto alla regione da cui lo switch di regione viene disattivato o disattivato.

Configurazione

Per configurare il blocco di esecuzione del servizio ECS Service Scaling, inserisci i seguenti valori.

> **Important**
>
> Prima di configurare il blocco di esecuzione, assicurati di disporre della politica IAM corretta. Per ulteriori informazioni, consulta Policy di esempio del blocco di esecuzione della scalabilità del servizio Amazon ECS.

1. Nome della fase: inserisci un nome.
2. Descrizione della fase (opzionale): inserisci una descrizione della fase.
3. Risorsa per regione: per ogni regione, inserisci l'ARN del cluster ECS e l'ARN del servizio ECS.
4. Percentuale corrispondente al numero di attività della regione di origine: inserisci la percentuale desiderata di attività in esecuzione nella regione di origine in modo che corrisponda alla regione attivata.
5. Approccio al monitoraggio della capacità: seleziona uno dei seguenti approcci per il monitoraggio della capacità per Amazon ECS:
   - Capacità di esecuzione massima campionata in 24 ore: scegli questa opzione per utilizzare il valore del conteggio delle attività in esecuzione nel tuo servizio Amazon ECS. Questa opzione non crea costi aggiuntivi, ma è potenzialmente meno accurata rispetto all'utilizzo dell'altra opzione, CloudWatch le metriche.

     Nell'API Region Switch, questa opzione corrisponde alla specificazione`sampledMaxInLast24Hours`.

     Per ulteriori informazioni, consulta la sezione Ridimensionamento automatico del servizio Amazon ECS nella Amazon Elastic Container Service Developer Guide.
   - Capacità operativa massima campionata nell'arco di 24 ore tramite Container Insights: scegli questa opzione per utilizzare i parametri di Amazon ECS Container Insights. L'utilizzo dell'opzione può essere più preciso, ma comporta i costi aggiuntivi dell'utilizzo di Container Insights.

     Nell'API Region switch, questa opzione corrisponde alla specificazione`autoscalingMaxInLast24Hours`.

     Per utilizzare questa opzione, devi prima abilitare Container Insights. Per ulteriori informazioni, consulta Configurare Container Insights nella Amazon CloudWatch User Guide.
6. Timeout: inserisci un valore di timeout.

Quindi, scegli Salva passaggio.

Come funziona

Dopo aver configurato il blocco di esecuzione nel piano, Region Switch conferma che esiste un solo servizio ECS di origine e un servizio di destinazione. Se sono presenti più servizi, Region switch restituisce un avviso per il blocco di esecuzione. Region switch memorizza questi dati in tutte le regioni per cui è configurato il piano. La capacità target è definita come il numero desiderato impostato sul servizio ECS.

A titolo di active/passive approccio, Region switch calcola la nuova capacità desiderata per il servizio ECS nella regione di destinazione (in fase di attivazione). La nuova capacità desiderata viene confrontata con la capacità desiderata del servizio ECS di destinazione. La formula utilizzata da Region switch per calcolare la capacità desiderata è la seguente:`ceil(percentToMatch * Source Auto Scaling group capacity)`, dove ceil () è una funzione che arrotonda qualsiasi risultato frazionario. Se il conteggio corrente desiderato per il servizio ECS di destinazione è superiore alla nuova capacità desiderata calcolata per il servizio ECS, l'esecuzione del piano procede. Tieni presente che Region Switch non riduce la capacità del servizio ECS.

Se il servizio ECS ha l'Application Autoscaling abilitato, Region switch aggiorna la capacità minima in Application Autoscaling e aggiorna anche il conteggio desiderato nel servizio ECS.

Quando Region switch esegue un blocco di servizio ECS, Region switch tenta di aumentare la capacità Region ECS di destinazione in modo che corrisponda alla capacità desiderata. Quindi, Region switch attende che la capacità del servizio ECS richiesta sia soddisfatta nel servizio ECS della regione di destinazione prima che Region switch proceda alla fase successiva del piano. Se lo desideri, puoi configurare il passaggio da completare prima del completamento dell'evasione impostando un limite di timeout per il tempo di attesa del cambio di regione per il raggiungimento della capacità.

Se utilizzi un active/active approccio, lo switch Region utilizza l'altra regione configurata come origine. In altre parole, se una regione viene disattivata, il cambio di regione utilizza l'altra regione attiva come fonte per determinare la percentuale da scalare.

Cosa viene valutato nell'ambito della valutazione del piano

Quando Region switch valuta il piano, Region switch esegue diversi controlli sulla configurazione e sulle autorizzazioni del blocco di esecuzione del servizio ECS. Region switch verifica che i servizi ECS siano presenti sia nella regione di origine che in quella di destinazione e verifica che la capacità massima impostata per il servizio ECS della regione di destinazione sia sufficiente a gestire la

corrispondenza percentuale specificata della capacità della regione di destinazione. Il cambio di regione verifica inoltre che il ruolo IAM del piano disponga delle autorizzazioni corrette per il servizio ECS. Per ulteriori informazioni sulle autorizzazioni richieste per i blocchi di esecuzione degli switch di regione, consulta. Esempi di politiche basate sull'identità per Region Switch in ARC

Inoltre, Region switch verifica di aver raccolto e `ResourceMonitor` archiviato correttamente i dati di monitoraggio necessari per i servizi ECS e acquisisce un conteggio del numero di attività in esecuzione.

Se uno qualsiasi dei controlli fallisce, Region Switch restituisce messaggi di avviso, che è possibile visualizzare nella console. In alternativa, puoi ricevere gli avvisi di convalida tramite EventBridge o utilizzando le operazioni API.

Blocco di esecuzione del controllo del routing ARC

Se hai configurato il controllo del routing di Amazon Application Recovery Controller (ARC) per la tua applicazione, puoi aggiungere una fase di controllo del routing ARC per reindirizzare il traffico dell'applicazione. Questo passaggio consente di modificare lo stato di uno o più controlli di routing ARC per reindirizzare il traffico dell'applicazione verso una destinazione. Regione AWS Il controllo del routing ARC reindirizza il traffico utilizzando i controlli di integrità in Amazon Route 53 configurati con i record DNS associati ai controlli di routing.

> **Important**
>
> Il controllo del routing di Amazon Application Recovery Controller (ARC) è disponibile solo nella partizione AWS commerciale.

Configurazione

Per configurare un blocco di esecuzione del controllo del routing, inserisci i seguenti valori.

> **Important**
>
> Prima di configurare il blocco di esecuzione, assicurati di disporre della politica IAM corretta. Per ulteriori informazioni, consulta Il routing ARC controlla la politica di esempio dei blocchi di esecuzione.

1. Nome della fase: inserisci un nome.

2. Descrizione della fase (opzionale): inserisci una descrizione della fase.
3. Controlli di routing desiderati: per ogni regione che desideri attivare o disattivare, inserisci l'ARN del controllo di routing e lo stato iniziale per il controllo del routing, Attivato o Disattivato.
4. Timeout: inserire un valore di timeout.

Quindi, scegli Salva passaggio.

Lo schema previsto per questo blocco di esecuzione consiste nello specificare i controlli di routing e gli stati iniziali in linea con la specifica configurazione dell'applicazione. Regioni AWS Ad esempio, se disponete di un piano che consente di attivare la Regione A e la Regione B per la vostra applicazione, potreste avere un controllo di routing per la Regione A in cui impostate lo stato su On e un controllo di routing per la Regione B in cui impostate lo stato su On.

Quindi, quando si esegue il piano e si specifica che si desidera attivare la Regione A, il flusso di lavoro che include questo blocco di esecuzione aggiorna il controllo di routing specificato su On, che indirizza il traffico verso la Regione A.

Come funziona

Configurando un blocco di esecuzione del controllo del routing ARC, puoi reindirizzare il traffico delle applicazioni verso una destinazione o Regione AWS, per un active/active approccio, impedire che il traffico venga instradato verso una regione che stai disattivando. Se il tuo piano include più flussi di lavoro, assicurati di fornire gli stessi input per i record DNS per tutti i blocchi di esecuzione del controllo del routing che utilizzi.

Questo blocco non supporta la modalità di esecuzione non corretta.

Cosa viene valutato nell'ambito della valutazione del piano

Quando Region switch valuta il piano, Region switch esegue diversi controlli sui controlli di routing, sulla configurazione dei blocchi di esecuzione e sulle autorizzazioni. Region switch verifica che i controlli di routing specificati siano configurati e accessibili correttamente.

Il cambio di regione verifica inoltre che il ruolo IAM del piano disponga delle autorizzazioni necessarie per accedere e aggiornare gli stati di controllo del routing. Per ulteriori informazioni sulle autorizzazioni richieste per i blocchi di esecuzione degli switch di regione, vedere. Esempi di politiche basate sull'identità per Region Switch in ARC

Le autorizzazioni IAM corrette sono essenziali per il corretto funzionamento del blocco di esecuzione del controllo del routing. Se una di queste convalide fallisce, Region switch segnala la presenza

di problemi e fornisce messaggi di errore specifici per aiutarti a risolvere i problemi relativi alle autorizzazioni o alla configurazione. Ciò garantisce che il piano disponga dell'accesso necessario per gestire e interagire con i controlli di routing ARC durante l'esecuzione di questa fase durante l'esecuzione di un piano.

Confronto tra i controlli di routing ARC e i blocchi di esecuzione dei controlli di integrità di Route 53

Il blocco di esecuzione dei controlli sanitari di Amazon Route 53 nello switch Region offre un'alternativa a basso costo per la gestione del traffico basata su DNS. Tuttavia, questo blocco di esecuzione dipende dalla regione Regione AWS che stai attivando, quindi quella regione deve essere disponibile. Ciò soddisfa le esigenze della maggior parte dei clienti, poiché stanno attivando una regione sana.

I controlli di routing ARC forniscono una gestione del traffico basata su DNS altamente affidabile con uno SLA di disponibilità del 100%. Con i controlli di routing, i team operativi possono spostare il traffico tra le regioni con barriere di sicurezza. I controlli di routing forniscono una soluzione single-tenant con uno SLA del 100%. Un cluster di controllo del routing è distribuito su cinque regioni e può tollerare che due regioni siano offline. Se disponi di applicazioni estremamente critiche, valuta la possibilità di utilizzare i controlli di routing.

I controlli di routing non sono necessari per utilizzare Region Switch. È possibile utilizzare Region switch per gestire il reindirizzamento del traffico utilizzando i blocchi di esecuzione del controllo dello stato di Route 53 senza controlli di routing.

I controlli di routing aggiungono valore con Region Switch nelle seguenti situazioni:

- È necessario lo SLA di disponibilità al 100% per il meccanismo di controllo del traffico stesso.
- La tua organizzazione richiede controlli operativi manuali con regole di sicurezza per le applicazioni critiche.
- defense-in-depthVolete che i team operativi possano ignorare manualmente il routing automatico del traffico, se necessario.

I blocchi di esecuzione del controllo dello stato di Route 53 non dipendono dal piano di controllo. Le modifiche ai record di Health Check utilizzano il piano dati, quindi non richiedono la Regione di attivazione per elaborare gli aggiornamenti della configurazione. I blocchi di esecuzione del controllo dello stato di Route 53 sono sufficienti nelle seguenti situazioni:

- L'applicazione può dipendere da quella Regione AWS che si sta attivando.

- Il reindirizzamento automatico del traffico come parte del flusso di lavoro di ripristino soddisfa i tuoi requisiti.
- L'ottimizzazione dei costi è una priorità. I blocchi di esecuzione dei controlli di integrità Route 53 hanno un costo inferiore rispetto ai controlli di routing.

La maggior parte dei clienti inizia con i blocchi di esecuzione del controllo dello stato di Route 53 come meccanismo di routing del traffico predefinito e aggiunge controlli di routing solo per le applicazioni più critiche che richiedono la massima affidabilità per il meccanismo di gestione del traffico.

Blocco di esecuzione di Amazon Aurora Global Database

Il blocco di esecuzione di Amazon Aurora Global Database consente di eseguire un flusso di lavoro di failover o ripristino dello switchover per un database globale.

- Failover: utilizza questo approccio per il ripristino dopo un'interruzione non pianificata. Con questo approccio, esegui un failover interregionale su uno dei cluster DB secondari nei database globali Aurora. Il Recovery Point Objective (RPO) per questo approccio è in genere un valore diverso da zero misurato in secondi. La quantità di perdita di dati dipende dal ritardo di replica dei database globali di Aurora Regioni AWS al momento dell'errore. Per ulteriori informazioni, consulta Ripristino di un database globale di Amazon Aurora da un'interruzione non pianificata nella Guida per l'utente di Amazon Aurora.
- Switchover: questa operazione era precedentemente chiamata failover pianificato gestito. Usa questo approccio per scenari controllati, ad esempio la manutenzione operativa e altre procedure operative pianificate, in cui tutti i cluster Aurora e gli altri servizi con cui interagiscono sono in stato integro. Poiché questa funzionalità sincronizza i cluster di database secondari con il primario prima di apportare altre modifiche, l’RPO è 0 (nessuna perdita di dati). Per ulteriori informazioni, consulta Esecuzione degli switchovers per i database globali di Amazon Aurora nella Guida per l'utente di Amazon Aurora.

Configurazione

Per configurare un blocco di esecuzione di Aurora Global Database, immettere i seguenti valori.

> **Important**
>
> Prima di configurare il blocco di esecuzione, assicurati di disporre della politica IAM corretta. Per ulteriori informazioni, consulta Politica di esempio dei blocchi di esecuzione di Aurora Global Database.

1. Nome della fase: inserisci un nome.
2. Descrizione della fase (opzionale): inserisci una descrizione della fase.
3. Nome del cluster Aurora Global Database: immettere l'identificatore per il database globale.
4. ARN del cluster per regione: inserire l'ARN del cluster da utilizzare in ogni regione del piano.
5. Specificare l'opzione per il database Aurora: scegli Switchover o Failover (perdita di dati), a seconda di come desideri
6. Nome del cluster Aurora Global Database:
7. Timeout: inserire un valore di timeout.

Quindi, scegli Salva passaggio.

Come funziona

Configurando un blocco di esecuzione di Aurora Global Databases, è possibile eseguire il failover o lo switchover dei database globali come parte del ripristino dell'applicazione. Se utilizzi un active/active approccio, Region switch utilizza l'altra regione configurata come origine. In altre parole, se una regione viene disattivata, il cambio di regione utilizza l'altra regione attiva come fonte per determinare la percentuale da scalare.

Questo blocco supporta sia le modalità di esecuzione graziose che le modalità di esecuzione ungraceful. Le impostazioni non corrette eseguono un failover di Aurora Global Database, che potrebbe causare la perdita di dati.

Per ulteriori informazioni sul disaster recovery di Aurora Global Database, inclusi failover e switchover, consulta Using switchover o failover nei database globali di Amazon Aurora nella Guida per l'utente di Amazon Aurora.

Cosa viene valutato come parte della valutazione del piano

Quando Region switch valuta il piano, Region switch esegue diversi controlli sulla configurazione e sulle autorizzazioni del blocco di esecuzione Aurora. Region switch verifica che quanto segue sia corretto:

- Il cluster globale Aurora specificato nella configurazione esiste.
- Esistono cluster Aurora DB sia nella regione di origine che in quella di destinazione.
- I cluster DB di origine e di destinazione si trovano in uno stato che consente il passaggio a Global Database.
- Esistono istanze DB sia nel cluster di origine che in quello di destinazione
- Le versioni del motore di cluster globale per l'azione di switchover sono compatibili. Ciò include la verifica che i cluster utilizzino le stesse versioni principali, secondarie e patch, con alcune eccezioni elencate nella documentazione di Aurora.

Il cambio di regione verifica inoltre che il ruolo IAM del piano disponga delle autorizzazioni necessarie per il failover e lo switchover di Aurora. Per ulteriori informazioni sulle autorizzazioni richieste per i blocchi di esecuzione degli switch regionali, consulta. Esempi di politiche basate sull'identità per Region Switch in ARC

Le autorizzazioni IAM corrette sono essenziali per il corretto funzionamento del blocco di esecuzione Aurora. Se una di queste convalide fallisce, Region switch restituisce avvisi relativi alla presenza di problemi e fornisce messaggi di errore specifici per aiutarti a risolvere i problemi relativi alle autorizzazioni o alla configurazione. Ciò garantisce che il piano disponga dell'accesso necessario per gestire e interagire con Aurora durante l'esecuzione di questo passaggio durante l'esecuzione di un piano.

Blocco di esecuzione di Amazon DocumentDB Global Cluster

Il blocco di esecuzione di Amazon DocumentDB Global Cluster consente di eseguire un flusso di lavoro di failover o ripristino dello switchover per un cluster globale.

- Failover: utilizza questo approccio per il ripristino dopo un'interruzione non pianificata. Con questo approccio, esegui un failover tra regioni su uno dei cluster secondari del tuo cluster globale Amazon DocumentDB. Il Recovery Point Objective (RPO) per questo approccio è in genere un valore diverso da zero misurato in secondi. La quantità di perdita di dati dipende dal ritardo della replica globale del cluster di Amazon DocumentDB Regioni AWS al momento dell'errore.

- Switchover: utilizza questo approccio per scenari controllati, come la manutenzione operativa e altre procedure operative pianificate in cui tutti i cluster Amazon DocumentDB sono integri. Poiché questa funzionalità sincronizza i cluster secondari con quelli primari prima di apportare altre modifiche, l'RPO è 0 (nessuna perdita di dati).

Configurazione

Per configurare un blocco di esecuzione di Amazon DocumentDB Global Cluster, inserisci i seguenti valori.

> **Important**
>
> Prima di configurare il blocco di esecuzione, assicurati di disporre della politica IAM corretta. Per ulteriori informazioni, consulta Politica di esempio per i blocchi di esecuzione di Amazon DocumentDB Global Cluster.

1. Nome della fase: inserisci un nome.
2. Descrizione della fase (opzionale): inserisci una descrizione della fase.
3. Identificatore del cluster globale di Amazon DocumentDB: inserisci l'identificatore per il cluster globale.
4. ARN del cluster per regione: inserire l'ARN del cluster da utilizzare in ogni regione del piano.
5. Specificare l'opzione per il cluster Amazon DocumentDB: scegli Switchover o Failover (perdita di dati).
6. Timeout: inserisci un valore di timeout.

Quindi, scegli Salva passaggio.

Come funziona

Configurando un blocco di esecuzione di Amazon DocumentDB Global Cluster, puoi eseguire il failover o lo switchover dei cluster globali come parte del ripristino dell'applicazione. Se utilizzi un active/active approccio, Region switch utilizza l'altra regione configurata come origine. In altre parole, se una regione viene disattivata, il cambio di regione utilizza l'altra regione attiva come fonte per determinare la percentuale da scalare.

Questo blocco supporta sia le modalità di esecuzione graziose che le modalità di esecuzione ungraceful. Le impostazioni non corrette eseguono un failover di Amazon DocumentDB Global Cluster, che potrebbe causare la perdita di dati.

Durante le operazioni di switchover o failover, l'endpoint DNS utilizzato dai clienti per la scrittura verrà modificato. I clienti hanno la responsabilità di assicurarsi di utilizzare l'endpoint corretto una volta completata l'operazione.

Cosa viene valutato nell'ambito della valutazione del piano

Quando Region switch valuta il tuo piano, Region switch esegue diversi controlli sulla configurazione e sulle autorizzazioni del blocco di esecuzione di Amazon DocumentDB. Il cambio di regione verifica che quanto segue sia corretto:

- Il cluster globale Amazon DocumentDB specificato nella configurazione esiste.
- Esistono cluster Amazon DocumentDB sia nella regione di origine che in quella di destinazione.
- I cluster di origine e di destinazione sono disponibili.
- Esistono istanze sia nel cluster di origine che in quello di destinazione.
- Le versioni del motore di cluster globale sono compatibili.

Il cambio di regione verifica inoltre che il ruolo IAM del piano disponga delle autorizzazioni necessarie per il failover e lo switchover di Amazon DocumentDB. Per ulteriori informazioni sulle autorizzazioni richieste per i blocchi di esecuzione degli switch regionali, consulta. Esempi di politiche basate sull'identità per Region Switch in ARC

Le autorizzazioni IAM corrette sono essenziali per il corretto funzionamento del blocco di esecuzione di Amazon DocumentDB. Se una di queste convalide fallisce, Region switch segnala la presenza di problemi e fornisce messaggi di errore specifici per aiutarti a risolvere i problemi relativi alle autorizzazioni o alla configurazione. Ciò garantisce che il piano disponga dell'accesso necessario per gestire e interagire con Amazon DocumentDB durante l'esecuzione di questo passaggio durante l'esecuzione di un piano.

Blocco di esecuzione Amazon RDS Promote Read Replica

Il blocco di esecuzione di Amazon RDS Promote Read Replica consente di promuovere una replica di lettura di Amazon RDS su un'istanza di database autonoma come parte del processo di ripristino multiregionale. Ciò consente di eseguire il failover in una regione integra promuovendo la replica di lettura in quella regione in modo che diventi il nuovo database primario.

Configurazione

Per configurare un blocco di esecuzione Amazon RDS Promote Read Replica, inserisci i seguenti valori.

> **Important**
>
> Prima di configurare il blocco di esecuzione, assicurati di disporre della politica IAM corretta. Per ulteriori informazioni, consulta Policy di esempio per i blocchi di esecuzione di Amazon RDS.

1. Nome della fase: inserisci un nome.
2. Descrizione della fase (opzionale): inserisci una descrizione della fase.
3. ARN dell'istanza DB RDS per regione: immettere l'ARN dell'istanza di database per la replica di lettura in ogni regione del piano.
4. Timeout: immettere un valore di timeout.

Quindi, scegli Salva passaggio.

Come funziona

Configurando un blocco di esecuzione Amazon RDS Promote Read Replica, puoi promuovere una replica di lettura a un'istanza di database autonoma come parte del ripristino dell'applicazione. Quando esegui il piano, Region switch promuove la replica di lettura nella regione che stai attivando in modo che diventi un'istanza di database indipendente.

> **Note**
>
> Questo blocco supporta solo i piani active/passive

Durante la promozione, l'endpoint DNS utilizzato per connettersi al database rimarrà lo stesso. Tuttavia, l'istanza promossa non verrà più replicata dal database primario originale. È tua responsabilità garantire che la loro applicazione sia configurata per utilizzare l'endpoint corretto al termine dell'operazione.

Dopo la promozione, l'istanza promossa eredita le seguenti impostazioni di backup dall'istanza principale originale:

- Periodo di conservazione dei backup
- Finestra di backup preferita

Cosa viene valutato nell'ambito della valutazione del piano

Quando Region switch valuta il tuo piano, Region switch esegue diversi controlli sulla configurazione e sulle autorizzazioni del blocco di esecuzione di Amazon RDS. Il cambio di regione verifica che quanto segue sia corretto:

- Le istanze di database Amazon RDS specificate nella configurazione esistono.
- Le istanze di database nelle regioni non primarie sono repliche di lettura.
- Le repliche di lettura sono disponibili.
- Le istanze del database sono configurate correttamente per la replica tra regioni.

Il cambio di regione verifica inoltre che il ruolo IAM del piano disponga delle autorizzazioni necessarie per la promozione delle repliche di lettura di Amazon RDS. Per ulteriori informazioni sulle autorizzazioni richieste per i blocchi di esecuzione degli switch regionali, consulta. Esempi di politiche basate sull'identità per Region Switch in ARC

Le autorizzazioni IAM corrette sono essenziali per il corretto funzionamento del blocco di esecuzione di Amazon RDS. Se una di queste convalide fallisce, Region switch segnala la presenza di problemi e fornisce messaggi di errore specifici per aiutarti a risolvere i problemi relativi alle autorizzazioni o alla configurazione. Ciò garantisce che il piano disponga dell'accesso necessario per gestire e interagire con Amazon RDS durante questa fase durante l'esecuzione di un piano.

Blocco di esecuzione Amazon RDS Create Cross-Region Replica

Il blocco di esecuzione Amazon RDS Create Cross-Region Replica consente di creare una replica di lettura interregionale per un'istanza di database Amazon RDS come parte del processo di post-ripristino. Questo blocco di esecuzione viene in genere utilizzato dopo aver promosso una replica di lettura per ristabilire la replica tra regioni, assicurando che l'applicazione sia pronta per i futuri eventi regionali.

Configurazione

Per configurare un blocco di esecuzione Amazon RDS Create Cross-Region Replica, inserisci i seguenti valori.

> **Important**
>
> Prima di configurare il blocco di esecuzione, assicurati di disporre della politica IAM corretta. Per ulteriori informazioni, consulta Policy di esempio per i blocchi di esecuzione di Amazon RDS.

1. Nome della fase: inserisci un nome.
2. Descrizione della fase (opzionale): inserisci una descrizione della fase.
3. ARN dell'istanza DB di origine per regione: immettere l'ARN dell'istanza di database per il database di origine in ogni regione del piano. Il blocco di esecuzione utilizza l'identificatore della regione attivata come database di origine per creare la replica di lettura interregionale.
4. ARN dell'istanza DB di replica: immettere l'ARN dell'istanza da utilizzare per la nuova replica di lettura.
5. Timeout: inserire un valore di timeout.

Quindi, scegli Salva passaggio.

Come funziona

Configurando un blocco di esecuzione Amazon RDS Create Cross-Region Replica, puoi creare una replica di lettura nell'altra regione come parte del processo di post-ripristino. Questo blocco di esecuzione è progettato per essere eseguito dopo un failover riuscito per ristabilire la replica tra regioni.

Questo blocco può essere aggiunto solo ai piani. active/passive

Durante l'esecuzione, la vecchia istanza primaria verrà rinominata e contrassegnata con renamedByRegionSwitch. Quindi verrà creata una nuova istanza di replica di lettura con le seguenti impostazioni copiate dalla vecchia istanza primaria:

- Identificatore di istanza
- Gruppi di parametri database
- Gruppi di sottoreti database
- Chiave KMS
- Gruppi di sicurezza VPC
- Gruppi di opzioni

- Configurazione Multi-AZ
- ARN segreto di autenticazione del dominio

> **Important**
>
> L'istanza principale rinominata rimane in esecuzione e continua a comportare addebiti. Region Switch la contrassegna con renamedByRegionSwitch per identificarla, ma non la modifica o la elimina in altro modo. L'utente è responsabile della gestione dell'istanza rinominata, inclusa la decisione se mantenerla in esecuzione, interromperla o eliminarla in base ai requisiti operativi e di costo.

> **Note**
>
> Questo blocco di esecuzione è progettato per i flussi di lavoro successivi al ripristino e richiede che la regione di origine sia integra e accessibile. Deve essere utilizzato dopo un failover riuscito per ristabilire la replica tra regioni.

Cosa viene valutato nell'ambito della valutazione del piano

Quando Region switch valuta il tuo piano, Region switch esegue diversi controlli sulla configurazione e sulle autorizzazioni del blocco di esecuzione di Amazon RDS. Il cambio di regione verifica che quanto segue sia corretto:

- Le istanze del database ARNs nella configurazione sono valide e formattate correttamente.
- Le istanze del database di origine esistono nelle rispettive regioni.
- Le istanze del database di origine sono disponibili.

Il cambio di regione verifica inoltre che il ruolo IAM del piano disponga delle autorizzazioni necessarie per creare repliche di lettura Amazon RDS. Per ulteriori informazioni sulle autorizzazioni richieste per i blocchi di esecuzione degli switch regionali, consulta. Esempi di politiche basate sull'identità per Region Switch in ARC

Le autorizzazioni IAM corrette sono essenziali per il corretto funzionamento del blocco di esecuzione di Amazon RDS. Se una di queste convalide fallisce, Region switch segnala la presenza di problemi e fornisce messaggi di errore specifici per aiutarti a risolvere i problemi relativi alle autorizzazioni o alla

configurazione. Ciò garantisce che il piano disponga dell'accesso necessario per gestire e interagire con Amazon RDS durante questa fase durante l'esecuzione di un piano.

Blocco di esecuzione dell'approvazione manuale

Il blocco di esecuzione manuale dell'approvazione consente di inserire una fase di approvazione da associare a un ruolo IAM. Gli utenti con accesso al ruolo possono approvare o rifiutare l'esecuzione di un passaggio, sospenderlo fino alla concessione dell'approvazione o, potenzialmente, impedire l'avanzamento del piano.

Per garantire che sia richiesta l'approvazione manuale durante l'esecuzione del piano, si inserisce una fase di approvazione manuale in una posizione specifica del flusso di lavoro, quindi si configura il ruolo IAM per specificare chi può approvare la fase.

Configurazione

Per configurare un blocco di esecuzione manuale dell'approvazione, inserisci i seguenti valori.

> **Important**
>
> Prima di configurare il blocco di esecuzione, assicurati di disporre della politica IAM corretta. Per ulteriori informazioni, consulta Esempio di politica di approvazione manuale, blocco di esecuzione.

1. Nome della fase: inserisci un nome.
2. Descrizione della fase (opzionale): inserisci una descrizione della fase.
3. Ruolo di approvazione IAM: inserisci l'ARN per un ruolo IAM autorizzato ad approvare manualmente il proseguimento dell'esecuzione per il piano di cambio di regione. Il ruolo IAM deve rientrare nell'account proprietario del piano.
4. Timeout: inserisci un valore di timeout.

Quindi, scegli Salva passaggio.

Come funziona

Configurando un blocco di esecuzione dell'approvazione manuale, puoi richiedere un'approvazione come parte del ripristino dell'applicazione. Per un blocco di esecuzione manuale, Region switch esegue le seguenti operazioni:

- Quando Region switch esegue un blocco di esecuzione manuale, sospende l'esecuzione e imposta lo stato di esecuzione del piano su In attesa di approvazione.
- Chiunque abbia accesso al ruolo definito nel blocco di esecuzione può approvare o rifiutare l'esecuzione della fase.
- Se approva l'esecuzione della fase, Region switch procede con l'esecuzione del piano. Se rifiutano, Region switch annulla l'esecuzione del piano.

Questo blocco non supporta la modalità di esecuzione non corretta.

Cosa viene valutato nell'ambito della valutazione del piano

Region Switch non completa alcuna valutazione per i blocchi di esecuzione dell'approvazione manuale.

Blocco di esecuzione Lambda ad azione personalizzata

Il blocco di esecuzione Lambda dell'azione personalizzata consente di aggiungere un passaggio personalizzato a un piano utilizzando una funzione Lambda.

Configurazione

Per configurare un blocco di esecuzione Lambda, inserisci i seguenti valori.

> **Important**
>
> Prima di configurare il blocco di esecuzione, assicurati di disporre della politica IAM corretta. Per ulteriori informazioni, consulta Politica di esempio del blocco di esecuzione Lambda ad azione personalizzata.

1. Nome della fase: inserisci un nome.
2. Descrizione della fase (opzionale): inserisci una descrizione della fase.
3. ARN della funzione Lambda da richiamare durante l'attivazione o la disattivazione di Region: specifica l'ARN della funzione Lambda da eseguire per questo passaggio.
4. Regione in cui eseguire la funzione Lambda: nel menu a discesa, scegli la regione in cui desideri eseguire le funzioni Lambda.
5. Timeout: inserisci un valore di timeout.

6. Intervallo tra tentativi: inserisci un intervallo di tentativi per eseguire nuovamente la funzione Lambda se non riesce entro questo intervallo.

Quindi, scegli Salva passaggio.

Come funziona

- Quando crei un blocco di esecuzione Lambda di azione personalizzato, devi specificare due funzioni Lambda per la fase da eseguire, una in ciascuna delle regioni del piano.
- È possibile configurare in quale regione si desidera che la Lambda venga eseguita, ad esempio, nella regione di attivazione o nella regione di disattivazione. Tuttavia, se esegui nella regione di disattivazione, assumi una dipendenza da quella regione. Non è consigliabile dipendere dalla regione di disattivazione.

Questo blocco supporta sia le modalità di esecuzione graceful che ungraceful. In modalità di esecuzione non funzionale, Region switch salta la fase del blocco di esecuzione Lambda.

Cosa viene valutato nell'ambito della valutazione del piano

Quando Region switch valuta il piano, Region switch esegue diversi controlli sulla configurazione e sulle autorizzazioni del blocco di esecuzione Lambda. Region switch verifica che quanto segue sia corretto:

- Le funzioni Lambda specificate nella configurazione esistono.
- Le impostazioni di concorrenza delle funzioni Lambda non sono limitate, inclusa la verifica di quanto segue:
  - La concorrenza non è impostata su 0.
  - È disponibile almeno un'esecuzione simultanea oppure esiste una concorrenza non riservata.

Region switch esegue un'esecuzione a secco della funzione Lambda per convalidare i parametri e le autorizzazioni specificati, senza eseguire la logica della funzione effettiva. I costi standard Lambda vengono sostenuti quando si esegue una corsa a secco.

Il cambio di regione verifica inoltre che il ruolo IAM del piano disponga delle autorizzazioni necessarie per l'esecuzione di Lambda. Per ulteriori informazioni sulle autorizzazioni richieste per i blocchi di esecuzione degli switch di regione, consulta. Esempi di politiche basate sull'identità per Region Switch in ARC

Le autorizzazioni IAM corrette sono essenziali per il corretto funzionamento del blocco di esecuzione Lambda. Se una di queste convalide fallisce, Region switch restituisce avvisi relativi alla presenza di problemi e fornisce messaggi di errore specifici per aiutarti a risolvere i problemi relativi alle autorizzazioni o alla configurazione. Ciò garantisce che il piano disponga dell'accesso necessario per gestire e interagire con la Lambda durante l'esecuzione di questo passaggio durante l'esecuzione di un piano.

Blocco di esecuzione del controllo dello stato di Amazon Route 53

Il blocco di esecuzione del controllo dello stato di Amazon Route 53 consente di specificare le regioni a cui verrà reindirizzato il traffico dell'applicazione durante il failover. Il blocco di esecuzione crea controlli di integrità di Amazon Route 53, che puoi quindi allegare ai record DNS di Route 53 nel tuo account. Quando esegui il tuo piano di switch di regione, lo stato del controllo di integrità di Route 53 viene aggiornato e il traffico viene reindirizzato in base alla configurazione DNS.

> **Important**
>
> La zona ospitata da Route 53 deve trovarsi nella stessa partizione del piano di commutazione regionale.

Configurazione

Per configurare un blocco di esecuzione del controllo dello stato di salute di Route 53, inserisci i seguenti valori.

> **Important**
>
> Prima di configurare il blocco di esecuzione, assicurati di disporre della politica IAM corretta. Per ulteriori informazioni, consulta Politica di esempio del blocco di esecuzione del controllo dello stato di Route 53.

1. Nome della fase: inserisci un nome.
2. Descrizione della fase (opzionale): inserisci una descrizione della fase.
3. ID della zona ospitata: l'ID della zona ospitata per il dominio e i record DNS in Route 53.
4. Nome del record: inserisci il nome del record (nome di dominio) per i record che utilizzi, con i relativi controlli di integrità, per reindirizzare il traffico verso la tua applicazione. Region Switch

troverà i set di record Route 53 per il nome del record e tenterà di mappare ogni set di record su una regione, in base al nome della regione all'interno del Value o Set Identifier del set di record.

5. Identificatori del set di record (facoltativi): è possibile fornire manualmente gli identificatori del set di record se Region Switch non è in grado di mappare automaticamente i set di record alle regioni in base al nome del record fornito nel passaggio 4 dopo la creazione del piano. Se la valutazione del piano restituisce un avviso che indica che sono necessarie ulteriori informazioni, aggiorna il piano con gli identificatori dei set di record includendo quanto segue per ogni regione:
   - Identificatore del set di record: inserire l'identificatore del set o il valore o il percorso verso cui il traffico viene indirizzato per il set di record.
   - Regione: inserire la regione associata al set di record che contiene le informazioni sull'identificatore del set di record.
6. Scegli Salva passaggio.
7. Configura i controlli sanitari in Route 53.

   Region switch fornisce un ID di controllo dello stato, per ogni regione, per ogni nome di record all'interno di una zona ospitata definita nel blocco di esecuzione. Assicurati di configurare i controlli di integrità per i set di record corrispondenti nel tuo account in Route 53 in modo che Region Switch possa reindirizzare correttamente il traffico verso l'applicazione durante l'esecuzione del piano. Nella scheda Health checks della pagina dei dettagli del piano, puoi visualizzare i controlli di integrità per tutti i blocchi di esecuzione e le regioni.

Come funziona

Aggiungi una fase di controllo dello stato al flusso di lavoro di cambio di regione in modo da poter reindirizzare il traffico verso una regione secondaria, per active/passive le configurazioni, o lontano da una regione disattivata, per le configurazioni. active/active Se aggiungi più flussi di lavoro al tuo piano, fornisci gli stessi valori di configurazione per tutti i blocchi di esecuzione dei controlli di integrità che utilizzano gli stessi record DNS.

In base alle informazioni fornite durante la configurazione del blocco di esecuzione, Region Switch tenta di determinare il set di record corretto per ogni regione del piano. In genere, l'ID della zona ospitata e il nome del record sono informazioni sufficienti per determinare i set di record e le regioni associate. In caso contrario, quando Region Switch esegue la valutazione automatica del piano dopo la creazione del piano, viene restituito un avviso per indicare che sono necessarie ulteriori informazioni.

Region switch esegue i controlli di integrità per ogni blocco di esecuzione dei controlli di integrità della Route 53. Per i piani che utilizzano un approccio di active/passive ripristino, il controllo dello stato di salute per la regione primaria inizia con lo stato corretto, mentre il controllo sanitario per la regione di standby è inizialmente impostato su Non integro. Per i piani che utilizzano l'approccio di active/active recupero, i controlli sanitari per tutte le regioni iniziano dallo stato di salute.

Per consentire a Region Switch di eseguire correttamente questo blocco di esecuzione per il piano, è necessario aggiungere i controlli di integrità ai record DNS.

Per un active/active piano, la fase di esecuzione funziona nel modo seguente:

- Quando viene eseguito un flusso di lavoro di disattivazione per una regione, il controllo dello stato è impostato su non integro e il traffico non viene più indirizzato verso la regione.
- Quando viene eseguito un flusso di lavoro di attivazione per una regione, il controllo dello stato è impostato su integro e il traffico viene indirizzato verso la regione.

Per un active/passive piano, la fase di esecuzione funziona nel modo seguente:

- Quando viene eseguito un flusso di lavoro di attivazione per una regione, il controllo dello stato di tale regione viene impostato su integro e il traffico viene indirizzato verso la regione. Allo stesso tempo, il controllo sanitario per l'altra regione del piano non è corretto e il traffico non viene più indirizzato verso quella regione.

Cosa viene valutato nell'ambito della valutazione del piano

Quando Region switch valuta il piano, Region switch esegue diversi controlli sulla configurazione e sulle autorizzazioni del blocco di esecuzione del controllo dello stato di Route 53. Region switch verifica che i controlli di integrità siano allegati ai record DNS specificati nella configurazione del blocco di esecuzione. Cioè, Region Switch verifica che i record DNS di una regione specifica Regione AWS siano configurati per utilizzare i controlli di integrità per quella regione.

Confronto tra i controlli di routing ARC e i blocchi di esecuzione dei controlli di integrità di Route 53

Il blocco di esecuzione dei controlli sanitari di Amazon Route 53 nello switch Region offre un'alternativa a basso costo per la gestione del traffico basata su DNS. Tuttavia, questo blocco di esecuzione dipende dalla regione Regione AWS che stai attivando, quindi quella regione deve essere disponibile. Ciò soddisfa le esigenze della maggior parte dei clienti, poiché stanno attivando una regione sana.

I controlli di routing ARC forniscono una gestione del traffico basata su DNS altamente affidabile con uno SLA di disponibilità del 100%. Con i controlli di routing, i team operativi possono spostare il traffico tra le regioni con barriere di sicurezza. I controlli di routing forniscono una soluzione single-tenant con uno SLA del 100%. Un cluster di controllo del routing è distribuito su cinque regioni e può tollerare che due regioni siano offline. Se disponi di applicazioni estremamente critiche, valuta la possibilità di utilizzare i controlli di routing.

I controlli di routing non sono necessari per utilizzare Region Switch. È possibile utilizzare Region switch per gestire il reindirizzamento del traffico utilizzando i blocchi di esecuzione del controllo dello stato di Route 53 senza controlli di routing.

I controlli di routing aggiungono valore con Region Switch nelle seguenti situazioni:

- È necessario lo SLA di disponibilità al 100% per il meccanismo di controllo del traffico stesso.
- La tua organizzazione richiede controlli operativi manuali con regole di sicurezza per le applicazioni critiche.
- defense-in-depthVolete che i team operativi possano ignorare manualmente il routing automatico del traffico, se necessario.

I blocchi di esecuzione del controllo dello stato di Route 53 non dipendono dal piano di controllo. Le modifiche ai record di Health Check utilizzano il piano dati, quindi non richiedono la Regione di attivazione per elaborare gli aggiornamenti della configurazione. I blocchi di esecuzione del controllo dello stato di Route 53 sono sufficienti nelle seguenti situazioni:

- L'applicazione può dipendere da quella Regione AWS che si sta attivando.
- Il reindirizzamento automatico del traffico come parte del flusso di lavoro di ripristino soddisfa i tuoi requisiti.
- L'ottimizzazione dei costi è una priorità. I blocchi di esecuzione dei controlli di integrità Route 53 hanno un costo inferiore rispetto ai controlli di routing.

La maggior parte dei clienti inizia con i blocchi di esecuzione del controllo dello stato di Route 53 come meccanismo di routing del traffico predefinito e aggiunge controlli di routing solo per le applicazioni più critiche che richiedono la massima affidabilità per il meccanismo di gestione del traffico.

Crea piani per bambini

Per supportare scenari di ripristino più complessi, puoi creare piani secondari aggiungendoli con blocchi di esecuzione del piano Region Switch. La gerarchia è limitata a due livelli, ma un piano per genitori può includere più piani per bambini.

> **Important**
>
> Prima di creare un piano secondario, assicurati di disporre della politica IAM corretta. Per ulteriori informazioni, consulta Esempio di politica di esempio per l'esecuzione del piano di cambio di regione.

Per motivi di compatibilità, i piani per bambini devono supportare tutte le regioni supportate dal piano principale. Inoltre, l'approccio di recupero, active/active o attivo/passivo, deve essere lo stesso per i piani genitore e figlio.

Tieni presente i seguenti modi in cui un piano figlio risponde alle modifiche apportate a un piano genitore e agli scenari del piano genitore.

- Un blocco di esecuzione principale viene contrassegnato come completato quando tutti i piani figlio e gli altri blocchi di esecuzione al suo interno sono stati completati.
- Se un passaggio non riesce in un piano secondario, il blocco di esecuzione del piano Region Switch fallisce nel piano principale.
- Le azioni di controllo avviate nel piano genitore durante la fase di cambio di regione, come una pausa, un passaggio graduale o non corretto o una cancellazione, vengono eseguite automaticamente nel piano per bambini, indipendentemente dalla fase corrente del piano per bambini.
- Le operazioni Skips hanno un comportamento speciale: il piano principale viene saltato, ma il piano secondario verrà comunque eseguito.
- Se un piano secondario è già in esecuzione in un blocco di cambio di regione, per determinare se continua a funzionare, Region switch valuta la compatibilità del piano secondario con il piano principale. Se la configurazione del piano figlio soddisfa i requisiti del piano principale, Region switch considera il piano figlio come se fosse stato avviato dal piano principale.
- La fase del piano principale avrà esito negativo se il piano secondario viene eseguito con parametri di configurazione incompatibili, come i seguenti:

  - Il piano per bambini è attivo in una regione diversa
  - Il piano secondario sta eseguendo un'operazione di disattivazione quando Region Switch prevede che esegua un'operazione di attivazione
- Se il piano per i genitori viene completato con successo durante un periodo in cui un piano principale è sospeso, il piano principale avrà esito positivo quando riprenderà il piano principale.

Crea un trigger per un piano di cambio di regione

Se desideri automatizzare il ripristino della tua applicazione in Region Switch, puoi creare uno o più trigger per il tuo piano di cambio di regione. I trigger iniziano automaticamente a eseguire un piano di cambio di regione, in base alle condizioni di CloudWatch allarme scelte.

Per creare un trigger per un piano di cambio di regione

1. Dopo aver creato un piano, nella pagina dei dettagli del piano, seleziona la scheda Trigger.
2. Scegli Gestisci i trigger.
3. Seleziona i flussi di lavoro di cui desideri automatizzare l'esecuzione, quindi scegli Aggiungi trigger.
4. Fornisci una descrizione del trigger.
5. Seleziona un CloudWatch allarme, quindi seleziona fino a 10 CloudWatch allarmi per creare le condizioni per l'attivazione.

   Quando selezioni più di una condizione, tutte le condizioni devono essere soddisfatte prima che inizi l'esecuzione automatica del piano.

Il trigger avvia l'esecuzione del piano quando un CloudWatch allarme passa a soddisfare le condizioni per l'attivazione. Quando il trigger viene aggiunto al piano, se le condizioni sono già soddisfatte, il piano non viene eseguito, il che impedisce eventi di failover non intenzionali.

Esegui un piano di cambio di regione per ripristinare un'applicazione

Per ripristinare un'applicazione quando un'applicazione Regione AWS è danneggiata, esegui un piano di cambio di regione in Amazon Application Recovery Controller (ARC).

- Se l'applicazione viene distribuita con un active/active approccio, i flussi di lavoro del piano disattivano la regione danneggiata in modo che l'altra regione attiva venga ridimensionata in modo appropriato e inizi a ricevere tutto il traffico dell'applicazione.

- Se l'applicazione viene distribuita con un active/passive approccio, i flussi di lavoro del piano disattivano la regione danneggiata e attivano la regione di standby, aumentando le risorse in tale area, se necessario, e reindirizzando il traffico dell'applicazione verso la regione di standby.

Per eseguire il ripristino dell'applicazione manualmente, esegui il piano di cambio di regione effettuando le seguenti operazioni.

Un'altra opzione è quella di attivare automaticamente un'esecuzione con CloudWatch allarmi Amazon specifici specificati per avviare l'esecuzione di un piano. Puoi specificare i trigger per l'esecuzione del piano quando crei o aggiorni un piano. Per ulteriori informazioni, consulta Crea un trigger per un piano di cambio di regione.

Per eseguire un piano di cambio di regione

1. Nella Console di gestione AWS, accedi a Regione AWS quello che desideri attivare per la tua applicazione.
2. Sulla console Amazon Application Recovery Controller (ARC), scegli Region switch, quindi seleziona il piano che desideri eseguire.
3. Scegli Execute plan.
4. Se il tuo piano include passaggi di approvazione manuali, approva ogni passaggio quando richiesto.

Durante l'esecuzione di un piano, è possibile monitorarne l'avanzamento nella pagina dei dettagli di esecuzione, che si apre quando si sceglie di eseguire un piano.

È inoltre possibile visualizzare le informazioni sul ripristino delle applicazioni in corso nei dashboard di Region Switch. Nella console Region Switch, nella barra di navigazione a sinistra, in Cambio di regione, scegli una delle seguenti opzioni:

- Dashboard globale
- Esecuzioni nel nome della regione

Tieni presente che, in caso di problemi in una regione, la dashboard globale potrebbe non mostrare tutti i dati del tuo piano. Per questo motivo, ti consigliamo di fare affidamento solo sulla dashboard delle esecuzioni regionali durante gli eventi operativi. Il dashboard Regional Executions è più resiliente perché utilizza il piano dati locale dello switch Region.

Una volta completata l'esecuzione del piano, è possibile visualizzare le informazioni sull'esecuzione del piano e su altri piani eseguiti da Region Switch nella pagina dei dettagli del piano nella scheda Cronologia di esecuzione del piano.

Dashboard di cambio di regione

Il cambio di regione include una dashboard globale che puoi utilizzare per osservare lo stato dei piani di cambio di regione nell'organizzazione e nelle regioni. Region Switch dispone anche di un pannello di controllo delle esecuzioni regionali che mostra solo le esecuzioni dei piani nella regione in cui sei attualmente connesso a. Console di gestione AWS

Tieni presente che, in caso di problemi in una regione, la dashboard globale potrebbe non mostrare tutti i dati del tuo piano. Per questo motivo, ti consigliamo di fare affidamento solo sulla dashboard delle esecuzioni regionali durante gli eventi operativi. Il dashboard Regional Executions è più resiliente perché utilizza il piano dati locale dello switch Region.

Per aprire il pannello di controllo globale Region Switch

1. Apri la console ARC all'indirizzohttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. In Cambio di regione, scegli Dashboard globale.

Per aprire la dashboard Regional Switch Regional

1. Apri la console ARC all'indirizzohttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. In Cambio di regione, scegli Dashboard regionale.

Supporto per più account in Region Switch

In Region Switch, puoi aggiungere risorse da altri account ai tuoi piani. Puoi anche condividere un piano di cambio di regione con altri account. Per ulteriori informazioni, consultare le sezioni indicate di seguito.

Risorse per più account

Il cambio di regione consente di ospitare le risorse in un account separato dall'account che contiene il piano di cambio di regione. Quando Region switch esegue un piano, assume l'ExecutionRole. Se il

piano utilizza le risorse di un account diverso dall'account che ospita il piano, Region Switch utilizza ExecutionRole per assumere l'accesso a tali risorse. crossAccountRole

Ogni risorsa del piano Region Switch ha due campi opzionali: crossAccountRole e ExternalID.

- crossAccountRole: Questo ruolo consente l'accesso alle risorse in un account diverso dall'account che ospita il piano di cambio di regione. Il ruolo necessita solo delle autorizzazioni per agire sulle risorse del suo account e non ha bisogno di autorizzazioni per agire sulle risorse dell'account che ospita il piano di cambio di regione.
- ExternalId: Questo è l'ID esterno STS indicato nella politica di fiducia dell'account che contiene la risorsa che richiede un'azione. È una stringa alfanumerica che rappresenta il segreto condiviso tra i due account.

Condivisione dei piani di cambio di regione

Region switch si integra con AWS Resource Access Manager (AWS RAM) per consentirti di condividere i piani tra Account AWS di loro. Quando condividi un piano, gli account da te specificati possono visualizzare i dettagli del piano, eseguire il piano e visualizzare le esecuzioni del piano, il che offre maggiore controllo e flessibilità per le funzionalità di ripristino tra diversi team.

Per iniziare con la condivisione tra account in Region Switch, devi creare una condivisione di risorse in. AWS RAM La condivisione delle risorse specifica i partecipanti autorizzati a condividere il piano di proprietà del tuo account. I partecipanti possono visualizzare ed eseguire il piano condiviso tramite la console, la CLI o. AWS SDKs

Importante: Account AWS devi essere il proprietario dei piani che desideri condividere. Non puoi condividere un piano che è stato condiviso con te. Per condividere un piano con la propria organizzazione o con un'unità organizzativa in AWS Organizations, è necessario abilitare la condivisione con Organizations.

Per ulteriori informazioni su AWS RAM, vedereSupporta i piani di condivisione tra account per ARC Region Switch.

Supporta i piani di condivisione tra account per ARC Region Switch

Amazon Application Recovery Controller (ARC) si integra con AWS Resource Access Manager per abilitare la condivisione delle risorse. AWS RAM è un servizio che consente di condividere risorse con altri Account AWS o tramite AWS Organizations. Per ARC Region Switch, puoi condividere

il piano Region Switch. (Per utilizzare le risorse di un altro account del piano, si utilizza un ruolo CrossAccount. Per ulteriori informazioni, consultaRisorse per più account.)

Con AWS RAM, condividi le risorse di tua proprietà creando una condivisione di risorse. Una condivisione di risorse specifica le risorse da condividere e i partecipanti con cui condividerle. I partecipanti possono includere:

- Specifico Account AWS all'interno o all'esterno dell'organizzazione del proprietario in AWS Organizations
- Un'unità organizzativa all'interno della sua organizzazione in AWS Organizations
- La sua intera organizzazione in AWS Organizations

Per ulteriori informazioni in merito AWS RAM, consulta la Guida AWS RAM per l'utente.

Utilizzando AWS Resource Access Manager per condividere i piani tra più account in ARC, è possibile utilizzare un piano con diversi piani diversi Account AWS. Quando si sceglie di condividere un piano, un altro Account AWS piano specificato dall'utente può eseguire il piano per eseguire il ripristino dell'applicazione.

AWS RAM è un servizio che aiuta AWS i clienti a condividere in modo sicuro le risorse tra Account AWS i clienti. Con AWS RAM, puoi condividere risorse all'interno di un'organizzazione o di unità organizzative (OUs) in AWS Organizations, utilizzando ruoli e utenti IAM. AWS RAM è un modo centralizzato e controllato per condividere un piano.

Quando si condivide un piano, è possibile ridurre il numero totale di piani richiesti dall'organizzazione. Con un piano condiviso, è possibile allocare il costo totale di esecuzione del piano tra diversi team, per massimizzare i vantaggi di ARC a costi inferiori. La condivisione dei piani tra gli account può anche semplificare il processo di onboarding di più applicazioni su ARC, soprattutto se si dispone di un gran numero di applicazioni distribuite su più account e team operativi.

Per iniziare con la condivisione tra account in ARC, devi creare una condivisione di risorse i n. AWS RAM La condivisione delle risorse specifica i partecipanti autorizzati a condividere il piano di proprietà del tuo account.

Questo argomento spiega come condividere le tue risorse e come utilizzare le risorse condivise con te.

Indice

- Prerequisiti per la condivisione dei piani

- Condivisione di un piano
- Annullamento della condivisione di un piano condiviso
- Identificazione di un piano condiviso
- Responsabilità e autorizzazioni per i piani condivisi
- Costi di fatturazione
- Quote

Prerequisiti per la condivisione dei piani

- Per condividere un piano, devi possederlo nel tuo Account AWS. Ciò significa che la risorsa deve essere allocata o assegnata all'account. Non puoi condividere un piano che è stato condiviso con te.
- Per condividere un piano con la tua organizzazione o un'unità organizzativa AWS Organizations, devi abilitare la condivisione con AWS Organizations. Per ulteriori informazioni, consulta Abilitare la condivisione con AWS Organizations nella Guida per l'utente di AWS RAM .

Condivisione di un piano

Quando condividi un piano, i partecipanti che hai specificato per condividere il piano possono visualizzare e, se concedi autorizzazioni aggiuntive, eseguire il piano.

Per condividere un piano, è necessario aggiungerlo a una condivisione di risorse. Una condivisione di risorse è una risorsa AWS RAM che consente di condividere le risorse tra Account AWS. Una condivisione di risorse specifica le risorse da condividere e i partecipanti con cui vengono condivise. Per condividere un piano, puoi creare una nuova condivisione di risorse o aggiungere la risorsa a una condivisione di risorse esistente. Per creare una nuova condivisione di risorse, puoi utilizzare la AWS RAM console o utilizzare le operazioni AWS RAM API con AWS Command Line Interface o AWS SDKs.

Se fai parte di un'organizzazione AWS Organizations e la condivisione all'interno dell'organizzazione è abilitata, ai partecipanti dell'organizzazione viene automaticamente concesso l'accesso al piano condiviso. In caso contrario, i partecipanti ricevono un invito a partecipare alla condivisione delle risorse e ottengono l'accesso al piano condiviso dopo aver accettato l'invito.

Puoi condividere un piano di tua proprietà utilizzando la AWS RAM console o utilizzando le operazioni AWS RAM API con AWS CLI o SDKs.

Per condividere un piano di tua proprietà utilizzando la AWS RAM console

Vedi Creazione di una condivisione di risorse nella Guida AWS RAM per l'utente.

Per condividere un piano di tua proprietà utilizzando il AWS CLI

Utilizza il comando create-resource-share.

Concessione delle autorizzazioni per condividere i piani

La condivisione dei piani tra più account richiede le seguenti autorizzazioni aggiuntive affinché il principale IAM condivida il piano utilizzando: AWS RAM

```
# read and execute plan permissions
"arc-region-switch:GetPlan",
"arc-region-switch:GetPlanInRegion",
"arc-region-switch:GetPlanExecution",
"arc-region-switch:ListPlanExecutionEvents",
"arc-region-switch:ListPlanExecutions",
"arc-region-switch:ListRoute53HealthChecks",
"arc-region-switch:GetPlanEvaluationStatus",
"arc-region-switch:StartPlanExecution",
"arc-region-switch:CancelPlanExecution",
"arc-region-switch:UpdatePlanExecution",
"arc-region-switch:UpdatePlanExecutionStep"
```

Il proprietario che condivide il piano deve disporre delle seguenti autorizzazioni. Se si tenta di condividere un piano AWS RAM senza disporre di queste autorizzazioni, viene restituito un errore.

```
"arc-region-switch:PutResourcePolicy" # Permission only apis
"arc-region-switch:DeleteResourcePolicy" # Permission only apis
"arc-region-switch:GetResourcePolicy" # Permission only apis
```

Per ulteriori informazioni sul modo in cui AWS Resource Access Manager utilizza IAM, consulta How AWS Resource Access Manager uses IAM nella Guida per l'AWS RAM utente.

Annullamento della condivisione di un piano condiviso

Quando annulli la condivisione di un piano, ai partecipanti e ai proprietari si applica quanto segue:

- I partecipanti non possono più visualizzare o eseguire il piano non condiviso.

Per annullare la condivisione di un piano condiviso di tua proprietà, rimuovilo dalla condivisione delle risorse. Puoi farlo utilizzando la AWS RAM console o utilizzando le operazioni AWS RAM API con AWS CLI o SDKs.

Per annullare la condivisione di un piano condiviso di tua proprietà utilizzando la console AWS RAM

Consulta Aggiornamento di una condivisione di risorse nella Guida per l'utente di AWS RAM .

Per annullare la condivisione di un piano condiviso di tua proprietà utilizzando il AWS CLI

Utilizza il comando disassociate-resource-share.

Identificazione di un piano condiviso

I proprietari e i partecipanti possono identificare i piani condivisi visualizzando le informazioni in AWS RAM. Possono inoltre ottenere informazioni sulle risorse condivise utilizzando la console ARC e AWS CLI.

In generale, per saperne di più sulle risorse che hai condiviso o che sono state condivise con te, consulta le informazioni nella Guida per l' AWS Resource Access Manager utente:

- In qualità di proprietario, puoi visualizzare tutte le risorse che condividi con altri utilizzando AWS RAM. Per ulteriori informazioni, vedi Visualizzazione delle risorse condivise in AWS RAM.
- Come partecipante, puoi visualizzare tutte le risorse condivise con te utilizzando AWS RAM. Per ulteriori informazioni, vedi Visualizzazione delle risorse condivise in AWS RAM.

In qualità di proprietario, puoi determinare se stai condividendo un piano visualizzando le informazioni nelle operazioni dell'API Console di gestione AWS o utilizzando le operazioni dell'API AWS Command Line Interface con ARC.

Per identificare se un piano di tua proprietà è condiviso utilizzando la console

Nella Console di gestione AWS pagina dei dettagli di un piano, vedi lo stato di condivisione del piano.

In qualità di partecipante, quando un piano viene condiviso con te, in genere devi accettare la condivisione per poter accedere al piano.

Responsabilità e autorizzazioni per i piani condivisi

Autorizzazioni per i proprietari

I partecipanti possono visualizzare o eseguire il piano (se dispongono delle autorizzazioni corrette).

Autorizzazioni per i partecipanti

Quando condividi un piano di tua proprietà con altri Account AWS, i partecipanti possono visualizzare o eseguire il piano (se dispongono delle autorizzazioni corrette).

Quando condividi un piano utilizzando AWS RAM, un partecipante dispone, per impostazione predefinita, di autorizzazioni di sola lettura. Per visualizzare un elenco di autorizzazioni di sola lettura per il cambio di regione, consulta. Autorizzazioni di sola lettura I partecipanti necessitano di autorizzazioni aggiuntive per eseguire un piano di cambio di regione. I partecipanti che devono eseguire i piani necessitano di autorizzazioni aggiuntive. Tieni presente che non puoi concedere l'autorizzazione a un AWS RAM partecipante per le seguenti operazioni:

- `ApprovePlanExecutionStep`
- `UpdatePlan`

Costi di fatturazione

Al proprietario di un piano in ARC vengono fatturati i costi associati al piano. Non sono previsti costi aggiuntivi, per i proprietari del piano o per i partecipanti, per la creazione di risorse ospitate in un piano.

Per informazioni dettagliate ed esempi sui prezzi, consulta la pagina dei prezzi di Amazon Application Recovery Controller (ARC).

Quote

Tutte le risorse create in un piano condiviso vengono conteggiate ai fini delle quote assegnate al proprietario del piano.

Per un elenco delle quote del piano di cambio di regione, consulta. Quote per il cambio di regione

Identity and Access Management per lo switch di regione in ARC

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

Indice

- Come funziona Region Switch in ARC con IAM
- Esempi di politiche basate sull'identità per Region Switch in ARC

Come funziona Region Switch in ARC con IAM

Prima di utilizzare IAM per gestire l'accesso ad ARC, scopri quali funzionalità IAM sono disponibili per l'uso con ARC.

Prima di utilizzare IAM per gestire l'accesso al Region switch in Amazon Application Recovery Controller (ARC), scopri quali funzionalità IAM sono disponibili per l'uso con Region switch.

Funzionalità IAM che puoi utilizzare con lo switch di regione in Amazon Application Recovery Controller (ARC)

Funzionalità IAM	Supporto per switch di regione
Policy basate sull'identità	Sì
Policy basate su risorse	Sì
Operazioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione delle policy	Sì
ACLs	Sì
ABAC (tag nelle policy)	Sì
Credenziali temporanee	Sì
Autorizzazioni del principale	Sì
Ruoli di servizio	No
Ruoli collegati al servizio	No

Per avere una visione generale di alto livello di come AWS i 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 Region Switch

Supporta le policy basate sull'identità: sì

Le policy basate sull'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 di IAM.

Con le policy basate sull'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. 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 IAM.

Per visualizzare esempi di politiche basate sull'identità ARC, vedere. Esempi di policy basate sull'identità in Amazon Application Recovery Controller (ARC)

Politiche basate sulle risorse all'interno di Region Switch

Supporta le policy basate sulle risorse: sì

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 di 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.

Azioni politiche per il cambio di regione

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 entità 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 in una policy. Includere le operazioni in una policy per concedere le autorizzazioni di eseguire l'operazione associata.

Le azioni politiche in ARC for Region switch utilizzano i seguenti prefissi prima dell'azione:

```
arc-region-switch
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola. Ad esempio, quanto segue:

```
"Action": [
      "arc-region-switch:action1",
      "arc-region-switch:action2"
         ]
```

È possibile specificare più azioni tramite caratteri jolly (*). Ad esempio, per specificare tutte le azioni che iniziano con la parola `Describe`, includi la seguente azione:

```
"Action": "arc-region-switch:Describe*"
```

Per visualizzare esempi di politiche basate sull'identità ARC per Region Switch, vedere. Esempi di politiche basate sull'identità per Region Switch in ARC

Risorse politiche per Region Switch

Supporta le risorse relative alle policy: sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità 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. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). Per le azioni che non supportano le autorizzazioni a livello di risorsa, si utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

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

Per visualizzare esempi di politiche basate sull'identità ARC per Region Switch, vedere. Esempi di politiche basate sull'identità per Region Switch in ARC

Chiavi relative alle condizioni politiche per il cambio di regione

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 entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento `Condition` specifica quando le istruzioni vengono eseguite in base a criteri definiti. 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. 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 esempi di politiche ARC basate sull'identità per Region Switch, vedere. Esempi di politiche basate sull'identità per Region Switch in ARC

Accedete agli elenchi di controllo (ACLs) in Region Switch

Supporti ACLs: Sì

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.

Controllo degli accessi basato sugli attributi (ABAC) con interruttore di regione

Supporta ABAC (tag nelle policy): sì

Il controllo degli accessi basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base ad attributi chiamati tag. Puoi allegare tag a entità e AWS risorse IAM, quindi progettare politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag sulla risorsa.

Per controllare l'accesso basato su tag, fornire 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 Sì. Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per maggiori informazioni su ABAC, consulta Definizione delle autorizzazioni con autorizzazione ABAC nella Guida per l'utente di 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 Region switch

Supporta le credenziali temporanee: sì

Le credenziali temporanee forniscono un accesso a breve termine alle AWS risorse e vengono create automaticamente quando si utilizza la federazione o si cambia ruolo. AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza temporanee in IAM e Servizi AWS compatibili con IAM nella Guida per l'utente IAM.

Autorizzazioni principali multiservizio per Region Switch

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

Quando utilizzi un'entità IAM (utente o ruolo) per eseguire azioni in AWS, sei considerato un principale. Le policy concedono autorizzazioni a un'entità. Quando si utilizzano alcuni servizi, è possibile eseguire un'azione che attiva un'altra azione in un servizio diverso. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni.

Ruoli di servizio per Region Switch

Supporta i ruoli di servizio: no

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.

Ruoli collegati al servizio per Region Switch

Supporta i ruoli collegati ai servizi: no

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'operazione 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 al servizio, ma non modificarle.

Per ulteriori informazioni su come creare e gestire i ruoli collegati ai servizi, consulta Servizi AWS supportati da IAM. Trova un servizio nella tabella che include un `Yes` nella colonna Service-linked role (Ruolo collegato ai servizi). Scegli il collegamento Sì per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Esempi di politiche basate sull'identità per Region Switch in ARC

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare risorse ARC. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM.

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 di IAM.

Per dettagli sulle azioni e sui tipi di risorse definiti da ARC, incluso il formato di ARNs per ogni tipo di risorsa, consulta Azioni, risorse e chiavi di condizione per Amazon Application Recovery Controller (ARC) nel Service Authorization Reference.

Argomenti

- Best practice per le policy
- Pianifica la politica di affidabilità dei ruoli di esecuzione
- Autorizzazioni di accesso complete
- Autorizzazioni di sola lettura
- Autorizzazioni per blocchi di esecuzione
- CloudWatch allarmi per le autorizzazioni di integrità dell'applicazione
- Autorizzazioni per l'esecuzione automatica dei report di esecuzione del piano
- Autorizzazioni relative alle risorse per più account
- Autorizzazioni complete per il ruolo di esecuzione del piano

Best practice per le policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare le risorse ARC nel tuo account. Queste operazioni possono comportare costi aggiuntivi per l' Account AWS. Quando si creano o modificano policy basate sull'identità, seguire 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 maggiori informazioni, consulta Policy gestite da AWS o Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente di IAM.

- Applicazione delle autorizzazioni con privilegio minimo - Quando si impostano le autorizzazioni con le policy IAM, concedere 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 privilegio minimo. Per maggiori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso - Per limitare l'accesso ad azioni e risorse è possibile aggiungere una condizione alle 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 CloudFormation. Per maggiori informazioni, consultare la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente di IAM.
- Utilizzo dello strumento di analisi degli accessi IAM per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali - Lo strumento di analisi degli accessi IAM convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio (JSON) della policy IAM e alle best practice di IAM. Lo strumento di analisi degli accessi IAM offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per maggiori informazioni, consultare Convalida delle policy per il Sistema di analisi degli accessi IAM nella Guida per l'utente di 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, aggiungere le condizioni MFA alle policy. Per maggiori informazioni, consultare Protezione dell'accesso API con MFA nella Guida per l'utente di IAM.

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

Pianifica la politica di affidabilità dei ruoli di esecuzione

Questa è la politica di fiducia richiesta per il ruolo di esecuzione del piano, in modo che ARC possa eseguire un piano di cambio di regione.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
```

```
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "arc-region-switch.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Autorizzazioni di accesso complete

La seguente policy IAM garantisce l'accesso completo a tutti gli switch di regione: APIs

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "arc-region-switch.amazonaws.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "arc-region-switch:CreatePlan",
        "arc-region-switch:UpdatePlan",
        "arc-region-switch:GetPlan",
        "arc-region-switch:ListPlans",
        "arc-region-switch:DeletePlan",
        "arc-region-switch:GetPlanInRegion",
        "arc-region-switch:ListPlansInRegion",
        "arc-region-switch:ApprovePlanExecutionStep",
        "arc-region-switch:GetPlanEvaluationStatus",
        "arc-region-switch:GetPlanExecution",
```

```
        "arc-region-switch:StartPlanExecution",
        "arc-region-switch:CancelPlanExecution",
        "arc-region-switch:ListRoute53HealthChecks",
        "arc-region-switch:ListRoute53HealthChecksInRegion",
        "arc-region-switch:ListPlanExecutions",
        "arc-region-switch:ListPlanExecutionEvents",
        "arc-region-switch:ListTagsForResource",
        "arc-region-switch:TagResource",
        "arc-region-switch:UntagResource",
        "arc-region-switch:UpdatePlanExecution",
        "arc-region-switch:UpdatePlanExecutionStep"
      ],
      "Resource": "*"
    }
  ]
}
```

Autorizzazioni di sola lettura

La seguente policy IAM concede autorizzazioni di accesso in sola lettura per Region Switch:

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "arc-region-switch:GetPlan",
        "arc-region-switch:ListPlans",
        "arc-region-switch:GetPlanInRegion",
        "arc-region-switch:ListPlansInRegion",
        "arc-region-switch:GetPlanEvaluationStatus",
        "arc-region-switch:GetPlanExecution",
        "arc-region-switch:ListRoute53HealthChecks",
        "arc-region-switch:ListRoute53HealthChecksInRegion",
        "arc-region-switch:ListPlanExecutions",
        "arc-region-switch:ListPlanExecutionEvents",
        "arc-region-switch:ListTagsForResource"
      ],
      "Resource": "*"
```

```
    }
  ]
}
```

Autorizzazioni per blocchi di esecuzione

Le seguenti sezioni forniscono esempi di policy IAM che forniscono le autorizzazioni richieste per blocchi di esecuzione specifici da aggiungere a un piano di cambio di regione.

Indice

- Politica di esempio per i blocchi di esecuzione di EC2 Auto Scaling
- Esempio di policy di esempio per la scalabilità delle risorse di Amazon EKS
- Policy di esempio del blocco di esecuzione della scalabilità del servizio Amazon ECS
- Il routing ARC controlla la politica di esempio dei blocchi di esecuzione
- Politica di esempio dei blocchi di esecuzione di Aurora Global Database
- Politica di esempio per i blocchi di esecuzione di Amazon DocumentDB Global Cluster
- Policy di esempio per i blocchi di esecuzione di Amazon RDS
- Esempio di politica di approvazione manuale, blocco di esecuzione
- Politica di esempio del blocco di esecuzione Lambda ad azione personalizzata
- Politica di esempio del blocco di esecuzione del controllo dello stato di Route 53
- Esempio di politica di esempio per l'esecuzione del piano di cambio di regione

Politica di esempio per i blocchi di esecuzione di EC2 Auto Scaling

Di seguito è riportato un esempio di policy da allegare se aggiungi blocchi di esecuzione a un piano di cambio di regione per i gruppi EC2 Auto Scaling.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "autoscaling:DescribeAutoScalingGroups"
```

```
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "autoscaling:UpdateAutoScalingGroup"
      ],
      "Resource": [
        "arn:aws:autoscaling:us-
east-1:123456789012:autoScalingGroup:123d456e-123e-1111-abcd-
EXAMPLE22222:autoScalingGroupName/app-asg-primary",
        "arn:aws:autoscaling:us-
west-2:123456789012:autoScalingGroup:1234a321-123e-1234-aabb-
EXAMPLE33333:autoScalingGroupName/app-asg-secondary"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource": "*"
    }
  ]
}
```

Esempio di policy di esempio per la scalabilità delle risorse di Amazon EKS

Di seguito è riportato un esempio di policy da allegare se aggiungi blocchi di esecuzione a un piano di switch di regione per la scalabilità delle risorse di Amazon EKS.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "eks:DescribeCluster"
      ],
```

```
      "Resource": [
        "arn:aws:eks:us-east-1:123456789012:cluster/app-eks-primary",
        "arn:aws:eks:us-west-2:123456789012:cluster/app-eks-secondary"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "eks:ListAssociatedAccessPolicies"
      ],
      "Resource": [
        "arn:aws:eks:us-east-1:123456789012:access-entry/app-eks-primary/*",
        "arn:aws:eks:us-west-2:123456789012:access-entry/app-eks-secondary/*"
      ]
    }
  ]
}
```

Nota: oltre a questa policy IAM, il ruolo di esecuzione del piano deve essere aggiunto alle voci di accesso del cluster Amazon EKS con la policy di `AmazonArcRegionSwitchScalingPolicy` accesso. Per ulteriori informazioni, consulta Configura le autorizzazioni di accesso EKS.

Policy di esempio del blocco di esecuzione della scalabilità del servizio Amazon ECS

Di seguito è riportato un esempio di policy da allegare se aggiungi blocchi di esecuzione a un piano di switch di regione per la scalabilità del servizio Amazon ECS.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ecs:DescribeServices",
        "ecs:UpdateService"
      ],
      "Resource": [
        "arn:aws:ecs:us-east-1:123456789012:service/app-cluster-primary/app-
service",
```

```
        "arn:aws:ecs:us-west-2:123456789012:service/app-cluster-secondary/app-
service"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ecs:DescribeClusters"
      ],
      "Resource": [
        "arn:aws:ecs:us-east-1:123456789012:cluster/app-cluster-primary",
        "arn:aws:ecs:us-west-2:123456789012:cluster/app-cluster-secondary"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ecs:ListServices"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:RegisterScalableTarget"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource": "*"
    }
  ]
}
```

Il routing ARC controlla la politica di esempio dei blocchi di esecuzione

Nota: il blocco di esecuzione dei controlli di routing di Amazon ARC richiede che tutte le politiche di controllo del servizio (SCPs) applicate al ruolo di esecuzione del piano consentano l'accesso alle seguenti regioni per questi servizi:

- `route53-recovery-control-config: us-west-2`
- `route53-recovery-cluster: us-west-2, us-east-1, eu-west-1, ap-southeast-2, ap-northeast-1`

Di seguito è riportato un esempio di policy da allegare se aggiungi blocchi di esecuzione a un piano di switch di regione per i controlli di routing ARC.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "route53-recovery-control-config:DescribeControlPanel",
        "route53-recovery-control-config:DescribeCluster"
      ],
      "Resource": [
        "arn:aws:route53-recovery-control::123456789012:controlpanel/
abcd1234abcd1234abcd1234abcd1234",
        "arn:aws:route53-recovery-
control::123456789012:cluster/4b325d3b-0e28-4dcf-ba4a-EXAMPLE11111"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "route53-recovery-cluster:GetRoutingControlState",
        "route53-recovery-cluster:UpdateRoutingControlStates"
      ],
      "Resource": [
        "arn:aws:route53-recovery-
control::123456789012:controlpanel/1234567890abcdef1234567890abcdef/
routingcontrol/abcdef1234567890",
```

```
        "arn:aws:route53-recovery-
control::123456789012:controlpanel/1234567890abcdef1234567890abcdef/
routingcontrol/1234567890abcdef"
      ]
    }
  ]
}
```

È possibile recuperare l'ID del pannello di controllo del routing e l'ID del cluster utilizzando la CLI. Per ulteriori informazioni, consulta Configura i componenti di controllo del routing.

Politica di esempio dei blocchi di esecuzione di Aurora Global Database

Di seguito è riportato un esempio di policy da allegare se si aggiungono blocchi di esecuzione a un piano di switch di regione per i database Aurora.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "rds:DescribeGlobalClusters",
        "rds:DescribeDBClusters"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "rds:FailoverGlobalCluster",
        "rds:SwitchoverGlobalCluster"
      ],
      "Resource": [
        "arn:aws:rds::123456789012:global-cluster:app-global-db",
       "arn:aws:rds:us-east-1:123456789012:cluster:app-db-primary",
        "arn:aws:rds:us-west-2:123456789012:cluster:app-db-secondary"
      ]
    }
  ]
```

```
}
```

Politica di esempio per i blocchi di esecuzione di Amazon DocumentDB Global Cluster

Di seguito è riportato un esempio di policy da allegare se aggiungi blocchi di esecuzione a un piano di switch di regione per i cluster globali di Amazon DocumentDB.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "rds:DescribeGlobalClusters",
        "rds:DescribeDBClusters",
        "rds:FailoverGlobalCluster",
        "rds:SwitchoverGlobalCluster"
      ],
      "Resource": "*"
    }
  ]
}
```

Policy di esempio per i blocchi di esecuzione di Amazon RDS

Di seguito è riportato un esempio di policy da allegare se aggiungi blocchi di esecuzione a un piano di switch di regione per la promozione di repliche di lettura di Amazon RDS o la creazione di repliche tra regioni.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "rds:DescribeDBInstances",
        "rds:PromoteReadReplica",
        "rds:CreateDBInstanceReadReplica",
        "rds:ModifyDBInstance"
      ],
      "Resource": "*"
    }
```

```
  ]
}
```

Esempio di politica di approvazione manuale, blocco di esecuzione

Di seguito è riportato un esempio di politica da allegare se si aggiungono blocchi di esecuzione a un piano di cambio di regione per le approvazioni manuali.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "arc-region-switch:ApprovePlanExecutionStep"
      ],
      "Resource": "arn:aws:arc-region-switch::123456789012:plan/sample-
plan:0123abc"
    }
  ]
}
```

Politica di esempio del blocco di esecuzione Lambda ad azione personalizzata

Di seguito è riportato un esempio di policy da allegare se si aggiungono blocchi di esecuzione a un piano di switch di regione per le funzioni Lambda.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "lambda:GetFunction",
        "lambda:InvokeFunction"
      ],
```

```
      "Resource": [
        "arn:aws:lambda:us-east-1:123456789012:function:app-recovery-primary",
        "arn:aws:lambda:us-west-2:123456789012:function:app-recovery-secondary"
      ]
    }
  ]
}
```

Politica di esempio del blocco di esecuzione del controllo dello stato di Route 53

Di seguito è riportato un esempio di policy da allegare se si aggiungono blocchi di esecuzione a un piano di switch di regione per i controlli di integrità di Route 53.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "route53:ListResourceRecordSets"
      ],
      "Resource": [
        "arn:aws:route53:::hostedzone/Z1234567890ABCDEFGHIJ"
      ]
    }
  ]
}
```

Esempio di politica di esempio per l'esecuzione del piano di cambio di regione

Di seguito è riportato un esempio di politica da allegare se si aggiungono blocchi di esecuzione a un piano di cambio di regione per eseguire piani secondari.

JSON

```
{
  "Version":"2012-10-17",
```

```
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "arc-region-switch:StartPlanExecution",
        "arc-region-switch:GetPlanExecution",
        "arc-region-switch:CancelPlanExecution",
        "arc-region-switch:UpdatePlanExecution",
        "arc-region-switch:ListPlanExecutions"
      ],
      "Resource": [
        "arn:aws:arc-region-switch::123456789012:plan/child-plan-1/abcde1",
        "arn:aws:arc-region-switch::123456789012:plan/child-plan-2/fghij2"
      ]
    }
  ]
}
```

CloudWatch allarmi per le autorizzazioni di integrità dell'applicazione

Di seguito è riportato un esempio di policy da allegare agli CloudWatch allarmi di accesso relativi allo stato delle applicazioni, utilizzati per determinare il tempo di ripristino effettivo.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource": [
        "arn:aws:cloudwatch:us-east-1:123456789012:alarm:app-health-primary",
        "arn:aws:cloudwatch:us-west-2:123456789012:alarm:app-health-secondary"
      ]
    }
  ]
}
```

Autorizzazioni per l'esecuzione automatica dei report di esecuzione del piano

Di seguito è riportato un esempio di politica da allegare se si configura la generazione automatica di report per un piano di cambio di regione. Questa politica include le autorizzazioni per scrivere report su Amazon S3, CloudWatch accedere ai dati degli allarmi e recuperare informazioni sui piani figlio per i piani genitori.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::your-bucket-name/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmHistory"
      ],
      "Resource": [
        "arn:aws:cloudwatch:us-east-1:123456789012:alarm:app-health-primary"
        "arn:aws:cloudwatch:us-west-2:123456789012:alarm:app-health-secondary"
      ],
    },
    {
      "Effect": "Allow",
      "Action": [
        "arc-region-switch:GetPlanExecution",
        "arc-region-switch:ListPlanExecutionEvents"
      ],
      "Resource": [
        "arn:aws:arc-region-switch:us-east-1:123456789012:plan/child-plan-1/abcde1",
        "arn:aws:arc-region-switch:us-west-2:123456789012:plan/child-plan-2/fghij2"
      ],
    }
  ]
}
```

Nota: se configuri una AWS KMS chiave gestita dal cliente per la crittografia dei bucket Amazon S3, devi anche aggiungere le autorizzazioni `kms:GenerateDataKey` e `kms:Encrypt` le autorizzazioni per la chiave.

Autorizzazioni relative alle risorse per più account

Se le risorse si trovano in account diversi, avrai bisogno di un ruolo su più account. Di seguito è riportato un esempio di politica di fiducia per un ruolo tra account.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:role/RegionSwitchExecutionRole"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "sts:ExternalId": "UniqueExternalId123"
        }
      }
    }
  ]
}
```

E quanto segue è l'autorizzazione per il ruolo di esecuzione del piano ad assumere questo ruolo tra account diversi:

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
```

```
      "Resource": "arn:aws:iam::987654321098:role/RegionSwitchCrossAccountRole",
      "Condition": {
        "StringEquals": {
          "sts:ExternalId": "UniqueExternalId123"
        }
      }
    }
  ]
}
```

Autorizzazioni complete per il ruolo di esecuzione del piano

La creazione di una politica completa che includa le autorizzazioni per tutti i blocchi di esecuzione richiederebbe una politica piuttosto ampia. In pratica, dovreste includere solo le autorizzazioni per i blocchi di esecuzione che utilizzate nei vostri piani specifici.

Di seguito è riportato un esempio di politica che è possibile utilizzare come punto di partenza per una politica relativa al ruolo di esecuzione del piano. Assicurati di aggiungere le politiche aggiuntive necessarie per i blocchi di esecuzione specifici che includi nel tuo piano. Includi solo le autorizzazioni necessarie per i blocchi di esecuzione specifici che utilizzi nel tuo piano, per seguire il principio del privilegio minimo

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iam:SimulatePrincipalPolicy",
            "Resource": "arn:aws:iam::123456789012:role/
RegionSwitchExecutionRole"
        },
        {
            "Effect": "Allow",
            "Action": [
                "arc-region-switch:GetPlan",
                "arc-region-switch:GetPlanExecution",
                "arc-region-switch:ListPlanExecutions"
            ],
```

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

Registrazione e monitoraggio per Region Switch in ARC

Puoi utilizzare Amazon e Amazon CloudWatch EventBridge per monitorare il cambio di regione in Amazon Application Recovery Controller (ARC), per ricevere avvisi, analizzare i modelli e aiutare a risolvere i problemi. AWS CloudTrail

Argomenti

- Registrazione delle chiamate API Region Switch utilizzando AWS CloudTrail
- Utilizzo del cambio di regione in ARC con Amazon EventBridge

Registrazione delle chiamate API Region Switch utilizzando AWS CloudTrail

Lo switch di regione Amazon Application Recovery Controller (ARC) è integrato con AWS CloudTrail un servizio che fornisce un registro delle azioni intraprese da un utente, un ruolo o un AWS servizio in ARC. CloudTrail acquisisce tutte le chiamate API per ARC come eventi. Le chiamate acquisite includono chiamate dalla console ARC e chiamate in codice alle operazioni dell'API ARC.

Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per ARC. 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, è possibile determinare la richiesta che è stata effettuata ad ARC, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e ulteriori dettagli.

Per ulteriori informazioni CloudTrail, consulta la Guida AWS CloudTrail per l'utente.

Informazioni ARC in CloudTrail

CloudTrail è abilitato sul tuo account al Account AWS momento della creazione dell'account. Quando si verifica un'attività in ARC, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi AWS di servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare eventi recenti in Account AWS. Per ulteriori informazioni, consulta Lavorare con la cronologia CloudTrail degli eventi.

Per una registrazione continua degli eventi del tuo Account AWS, compresi gli eventi per ARC, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando si crea un percorso nella console, questo sarà valido in tutte le Regioni AWS. Il trail registra gli eventi di tutte le regioni della AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica della creazione di un percorso
- CloudTrail servizi e integrazioni supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di CloudTrail registro da più regioni e ricezione di file di CloudTrail registro da più account

Tutte le azioni ARC vengono registrate CloudTrail e documentate nel TBD API REFERENCE LINK. Ad esempio, le chiamate a TBD e le TBD TBD azioni generano voci nei file di registro. CloudTrail

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con credenziali utente root o AWS Identity and Access Management (IAM).
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro AWS servizio.

Per ulteriori informazioni, consulta Elemento CloudTrail userIdentity.

Visualizzazione degli eventi del cambio di regione nella cronologia degli eventi

CloudTrail consente di visualizzare gli eventi recenti nella cronologia degli eventi. La maggior parte degli eventi per le richieste API di cambio di regione si svolgono nella regione in cui si lavora con un piano di cambio di regione, ad esempio dove si crea un piano o si esegue un piano. Tuttavia, alcune azioni di cambio di regione eseguite nella console ARC vengono eseguite utilizzando le operazioni dell'API del piano di controllo, anziché le operazioni sul piano dati. Per le operazioni sul piano di controllo, è possibile visualizzare gli eventi negli Stati Uniti orientali (Virginia settentrionale). Per

informazioni su quali chiamate API sono operazioni del piano di controllo, consultaOperazioni API di cambio di regione.

Comprensione delle voci dei file di registro ARC

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'`StartPlanExecution`azione del cambio di regione.


```
{
    "eventVersion": "1.11",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:role/admin",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROA33L3W36EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/admin",
                "accountId": "111122223333",
                "userName": "EXAMPLENAME"
            },
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2025-07-06T17:38:05Z"
            }
        }
    },
    "eventTime": "2025-07-06T18:08:03Z",
    "eventSource": "arc-region-switch.amazonaws.com",
    "eventName": "StartPlanExecution",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.50",
```

```
    "userAgent": "Boto3/1.17.101 Python/3.8.10 Linux/4.14.231-180.360.amzn2.x86_64
 exec-env/AWS_Lambda_python3.8 Botocore/1.20.102",
    "requestParameters": {
        "planArn": "arn:aws:arc-region-switch::555555555555:plan/
CloudTrailIntegTestPlan:bbbbb",
        "targetRegion": "us-east-1",
        "action": "activate"    }
    "responseElements": {
        "executionId": "us-east-1/ddddddddEXAMPLE",
        "plan": "arn:aws:arc-region-switch::555555555555:plan/
CloudTrailIntegTestPlan:bbbbb",
        "planVersion": "1",
        "activateRegion": "us-east-1"    },
    "requestID": "fd42dcf7-6446-41e9-b408-d096example",
    "eventID": "4b5c42df-1174-46c8-be99-d67aexample",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management",
      "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "us-east-1.arc.amazon.aws"
}
```


Utilizzo del cambio di regione in ARC con Amazon EventBridge

Con Amazon EventBridge, puoi configurare regole basate sugli eventi che monitorano le risorse dello switch di regione in Amazon Application Recovery Controller (ARC) e quindi avviare azioni mirate che utilizzano altri servizi. AWS Ad esempio, puoi impostare una regola per l'invio di notifiche e-mail segnalando un argomento di Amazon SNS ogni volta che un piano di cambio di regione completa l'esecuzione.

Puoi creare regole in Amazon EventBridge per agire sui seguenti eventi di cambio di regione ARC:

- Esecuzione del piano di cambio di regione. L'evento specifica che è stato eseguito (eseguito) un piano di cambio di regione.
- Valutazione del piano di cambio di regione. L'evento specifica che la valutazione di un piano di cambio di regione è stata completata.

Per acquisire eventi ARC specifici che ti interessano, definisci modelli specifici dell'evento che EventBridge puoi utilizzare per rilevare gli eventi. I pattern di eventi hanno la stessa struttura degli eventi a cui corrispondono. Il modello cita i campi che desideri abbinare e fornisce i valori che stai cercando.

Gli eventi vengono emessi secondo il principio del massimo sforzo. Vengono trasmessi da ARC a quasi EventBridge in tempo reale in normali circostanze operative. Tuttavia, possono verificarsi situazioni che potrebbero ritardare o impedire la consegna di un evento.

Per informazioni su come EventBridge le regole funzionano con i modelli di eventi, consulta Eventi e modelli di eventi in EventBridge.

Monitora una risorsa di cambio di regione con EventBridge

Con EventBridge, puoi creare regole che definiscono le azioni da intraprendere quando ARC emette eventi per le risorse di cambio di regione.

Per digitare o copiare e incollare un pattern di eventi nella EventBridge console, nella console, seleziona l'opzione Inserisci la mia opzione. Per aiutarti a determinare i modelli di eventi che potrebbero esserti utili, questo argomento include esempi di modelli di cambio di regione.

Per creare una regola per un evento risorsa

1. Apri la EventBridge console Amazon all'indirizzo https://console.aws.amazon.com/events/.
2. Regione AWS Per creare la regola, scegli la regione in cui hai creato il piano per cui desideri monitorare gli eventi.
3. Scegliere Create rule (Crea regola).
4. Immettere un Name (Nome) per la regola e, facoltativamente, una descrizione.
5. Per Event bus, lascia il valore predefinito, predefinito.
6. Scegli Next (Successivo).
7. Per il passo Build event pattern, per Event source, lascia il valore predefinito, AWS events.
8. In Evento di esempio, scegli Inserisci il mio.
9. Per gli eventi di esempio, digita o copia e incolla un modello di evento. Per alcuni esempi, consultate la sezione successiva.

Esempio di modelli di cambio di regione

I modelli di eventi hanno la stessa struttura degli eventi a cui corrispondono. Il modello cita i campi che desideri abbinare e fornisce i valori che stai cercando.

È possibile copiare e incollare i modelli di eventi da questa sezione EventBridge per creare regole da utilizzare per monitorare le azioni e le risorse ARC.

I seguenti modelli di eventi forniscono esempi che è possibile utilizzare EventBridge per la funzionalità di cambio di regione in ARC.

- Seleziona tutti gli eventi da Region Switch for PlanExecution.

```
{
    "source": [ "aws.arc-region-switch" ],
    "detail-type": [ "ARC Region switch Plan Execution" ]
}
```

- Seleziona tutti gli eventi da Region Switch for PlanEvaluation.

```
     {
     "source": [ "aws.arc-region-switch" ],
     "detail-type": [ "ARC Region Switch Plan Evaluation" ]
     }
```

Di seguito è riportato un esempio di evento ARC per l'esecuzione di un piano di cambio di regione:

```
{
   "version": "0",
   "id": "1111111-bbbb-aaaa-cccc-dddddEXAMPLE", # Random uuid
   "detail-type": "ARC Region Switch Plan Execution",
   "source": "aws.arc-region-switch",
   "account": "111122223333",
   "time": "2023-11-16T23:38:14Z",
   "region": "us-east-1",
   "resources": ["arn:aws:arc-region-switch::111122223333:plan/aaaaaExample"], #
 planArn
   "detail": {
    "version": "0.0.1",
    "eventType": "ExecutionStarted",
    "executionId": "bbbbbbEXAMPLE",
    "executionAction": "activating/deactivating {region}",
```

```
    "idempotencyKey": "1111111-2222-3333-4444-5555555555", # As there is a possibility
 of dual logging
   }
}
```

Di seguito è riportato un esempio di evento ARC per un'esecuzione a livello di fase del piano di cambio di regione:

```
{
   "version": "0",
   "id": "1111111-bbbb-aaaa-cccc-dddddEXAMPLE", # Random uuid
   "detail-type": "ARC Region Switch Plan Execution",
   "source": "aws.arc-region-switch",
   "account": "111122223333",
   "time": "2023-11-16T23:38:14Z",
   "region": "us-east-1",
   "resources": ["arn:aws:arc-region-switch::111122223333:plan/aaaaaExample"], #
 planArn
   "detail": {
    "version": "0.0.1",
    "eventType": "StepStarted",
    "executionId": "bbbbbbEXAMPLE",
    "executionAction": "activating/deactivating {region}",
    "idempotencyKey": "1111111-2222-3333-4444-5555555555", # As there is a possibility
 of dual logging
    "stepDetails" : {
     "stepName": "Routing control step",
     "resource": ["arn:aws:route53-recovery-control::111122223333:controlpanel/
abcdefghiEXAMPLE/routingcontrol/jklmnopqrsEXAMPLE"]
    }
   }
}
```

Di seguito è riportato un esempio di evento ARC per un avviso di valutazione del piano di cambio di regione.

Per la valutazione di un piano di cambio di regione, viene emesso un evento quando viene restituito un avviso. Se l'avviso non viene cancellato, viene emesso un evento relativo all'avviso solo una volta ogni 24 ore. Quando l'evento viene cancellato, non vengono emessi altri eventi per quell'avviso.

```
{
   "version": "0",
```

```
   "id": "05d4d2d5-9c76-bfea-72d2-d4614802adb4", # Random uuid
   "detail-type": "ARC Region Switch Plan Execution",
   "source": "aws.arc-region-switch",
   "account": "111122223333",
   "time": "2023-11-16T23:38:14Z",
   "region": "us-east-1",
   "resources": ["arn:aws:arc-region-switch::111122223333:plan/a2b89be4821bfd1d"],
   "detail": {
     "version": "0.0.1",
     "idempotencyKey": "1111111-2222-3333-4444-5555555555",
     "metadata": {
        "evaluationTime" : "timestamp",
        "warning" : "There is a plan evaluation warning for arn:aws:arc-region-
switch::111122223333:plan/a2b89be4821bfd1d. Navigate to the Region switch console to
 resolve."
     }
   }
}
```

Specificare un gruppo di CloudWatch log da utilizzare come destinazione

Quando si crea una EventBridge regola, è necessario specificare la destinazione a cui vengono inviati gli eventi corrispondenti alla regola. Per un elenco degli obiettivi disponibili per EventBridge, vedi Target disponibili nella EventBridge console. Uno degli obiettivi che puoi aggiungere a una EventBridge regola è un gruppo di CloudWatch log Amazon. Questa sezione descrive i requisiti per aggiungere gruppi di CloudWatch log come destinazioni e fornisce una procedura per aggiungere un gruppo di log quando si crea una regola.

Per aggiungere un gruppo di CloudWatch log come destinazione, è possibile effettuare una delle seguenti operazioni:

- Creare un nuovo gruppo di log
- Scegli un gruppo di log esistente

Se specifichi un nuovo gruppo di log utilizzando la console quando crei una regola, crea EventBridge automaticamente il gruppo di log per te. Assicurati che il gruppo di log che usi come destinazione per la EventBridge regola inizi con`/aws/events`. Se desideri scegliere un gruppo di log esistente, tieni presente che solo i gruppi di log che iniziano con `/aws/events` appaiono come opzioni nel menu a discesa. Per ulteriori informazioni, consulta Creare un nuovo gruppo di log nella Amazon CloudWatch User Guide.

Se crei o utilizzi un gruppo di CloudWatch log da utilizzare come destinazione utilizzando CloudWatch operazioni esterne alla console, assicurati di impostare le autorizzazioni correttamente. Se utilizzi la console per aggiungere un gruppo di log a una EventBridge regola, la politica basata sulle risorse per il gruppo di log viene aggiornata automaticamente. Tuttavia, se si utilizza AWS Command Line Interface o un AWS SDK per specificare un gruppo di log, è necessario aggiornare la politica basata sulle risorse per il gruppo di log. La seguente politica di esempio illustra le autorizzazioni che è necessario definire in una politica basata sulle risorse per il gruppo di log:

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Action": [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "events.amazonaws.com",
          "delivery.logs.amazonaws.com"
        ]
      },
      "Resource": "arn:aws:logs:us-east-1:222222222222:log-group:/aws/events/
*:*",
      "Sid": "TrustEventsToStoreLogEvent"
    }
  ]
}
```

Non è possibile configurare una politica basata sulle risorse per un gruppo di log utilizzando la console. Per aggiungere le autorizzazioni richieste a una politica basata sulle risorse, utilizza l'operazione API. CloudWatch PutResourcePolicy Quindi, puoi utilizzare il comando describe-resource-policiesCLI per verificare che la tua politica sia stata applicata correttamente.

Per creare una regola per un evento di risorsa e specificare un target per un gruppo di CloudWatch log

1. Apri la EventBridge console Amazon all'indirizzo https://console.aws.amazon.com/events/.
2. Scegli Regione AWS quello in cui vuoi creare la regola.
3. Scegli Crea regola e inserisci tutte le informazioni su quella regola, come lo schema dell'evento o i dettagli della pianificazione.

   Per ulteriori informazioni sulla creazione di EventBridge regole di preparazione, consulta Monitorare una risorsa per il controllo di prontezza con. EventBridge
4. Nella pagina Seleziona destinazione, scegli CloudWatchcome obiettivo.
5. Scegli un gruppo di CloudWatch log dal menu a discesa.

Quote per il cambio di regione

Il cambio di regione in Amazon Application Recovery Controller (ARC) è soggetto alle seguenti quote.

Entità	Quota
Numero di piani per account	10 Puoi richiedere un aumento della quota.
Numero di blocchi di esecuzione per piano	100
Numero di blocchi di esecuzione del piano Region Switch per piano	25
Numero di blocchi di esecuzione parallela per fase	20
Numero di CloudWatch allarmi per condizione di attivazione	10

Esempi di codice per l'utilizzo di Application Recovery Controller AWS SDKs

I seguenti esempi di codice mostrano come utilizzare Application Recovery Controller con un kit di sviluppo AWS software (SDK).

Le azioni sono estratti di codice da programmi più grandi e devono essere eseguite nel contesto. Sebbene le azioni mostrino come richiamare le singole funzioni del servizio, è possibile visualizzarle contestualizzate negli scenari correlati.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di questo servizio con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Esempi di codice

- Esempi di base per l'utilizzo di Application Recovery Controller AWS SDKs
  - Azioni per l'utilizzo di Application Recovery Controller AWS SDKs
    - Utilizzalo GetRoutingControlState con un AWS SDK
    - Utilizzare UpdateRoutingControlState con un SDK AWS

Esempi di base per l'utilizzo di Application Recovery Controller AWS SDKs

I seguenti esempi di codice mostrano come utilizzare le nozioni di base di Amazon Route 53 Application Recovery Controller con AWS SDKs.

Esempi

- Azioni per l'utilizzo di Application Recovery Controller AWS SDKs
  - Utilizzalo GetRoutingControlState con un AWS SDK
  - Utilizzare UpdateRoutingControlState con un SDK AWS

Azioni per l'utilizzo di Application Recovery Controller AWS SDKs

I seguenti esempi di codice mostrano come eseguire singole azioni di Application Recovery Controller con AWS SDKs. Ogni esempio include un collegamento a GitHub, dove sono disponibili le istruzioni per la configurazione e l'esecuzione del codice.

Gli esempi seguenti includono solo le azioni più comunemente utilizzate. Per un elenco completo, consulta la documentazione di riferimento dell'API del sistema di controllo Amazon Route 53 per il ripristino di applicazioni.

Esempi

- Utilizzalo GetRoutingControlState con un AWS SDK
- Utilizzare UpdateRoutingControlState con un SDK AWS

Utilizzalo **`GetRoutingControlState`** con un AWS SDK

Gli esempi di codice seguenti mostrano come utilizzare `GetRoutingControlState`.

Java

SDK per Java 2.x

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
    public static GetRoutingControlStateResponse
 getRoutingControlState(List<ClusterEndpoint> clusterEndpoints,
            String routingControlArn) {
        // As a best practice, we recommend choosing a random cluster endpoint to
 get or
        // set routing control states.
        // For more information, see
        // https://docs.aws.amazon.com/r53recovery/latest/dg/route53-arc-best-
practices.html#route53-arc-best-practices.regional
        Collections.shuffle(clusterEndpoints);
        for (ClusterEndpoint clusterEndpoint : clusterEndpoints) {
            try {
```

```
                System.out.println(clusterEndpoint);
                Route53RecoveryClusterClient client =
 Route53RecoveryClusterClient.builder()
                        .endpointOverride(URI.create(clusterEndpoint.endpoint()))
                        .region(Region.of(clusterEndpoint.region())).build();
                return client.getRoutingControlState(
                        GetRoutingControlStateRequest.builder()
                                .routingControlArn(routingControlArn).build());
            } catch (Exception exception) {
                System.out.println(exception);
            }
        }
        return null;
    }
```

- Per i dettagli sull'API, GetRoutingControlStateconsulta AWS SDK for Java 2.x API Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
import boto3


def create_recovery_client(cluster_endpoint):
    """
    Creates a Boto3 Route 53 Application Recovery Controller client for the
 specified
    cluster endpoint URL and AWS Region.

    :param cluster_endpoint: The cluster endpoint URL and Region.
    :return: The Boto3 client.
    """
```

```
    return boto3.client(
        "route53-recovery-cluster",
        endpoint_url=cluster_endpoint["Endpoint"],
        region_name=cluster_endpoint["Region"],
    )



def get_routing_control_state(routing_control_arn, cluster_endpoints):
    """
    Gets the state of a routing control. Cluster endpoints are tried in
    sequence until the first successful response is received.

    :param routing_control_arn: The ARN of the routing control to look up.
    :param cluster_endpoints: The list of cluster endpoints to query.
    :return: The routing control state response.
    """

    # As a best practice, we recommend choosing a random cluster endpoint to get
 or set routing control states.
    # For more information, see https://docs.aws.amazon.com/r53recovery/latest/
dg/route53-arc-best-practices.html#route53-arc-best-practices.regional
    random.shuffle(cluster_endpoints)
    for cluster_endpoint in cluster_endpoints:
        try:
            recovery_client = create_recovery_client(cluster_endpoint)
            response = recovery_client.get_routing_control_state(
                RoutingControlArn=routing_control_arn
            )
            return response
        except Exception as error:
            print(error)
            raise error
```

- Per i dettagli sull'API, consulta GetRoutingControlState AWSSDK for Python (Boto3) API Reference.

SAP ABAP

SDK per SAP ABAP

> **Note**
>
> C'è altro da fare. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
    CONSTANTS cv_pfl TYPE /aws1/rt_profile_id VALUE 'ZCODE_DEMO'.
    DATA lo_exception TYPE REF TO /aws1/cx_rt_generic.
    DATA lo_session TYPE REF TO /aws1/cl_rt_session_base.
    DATA lo_client TYPE REF TO /aws1/if_r5v.
    DATA lt_endpoints TYPE TABLE OF string.
    DATA lv_endpoint TYPE string.
    DATA lv_region TYPE /aws1/rt_region_id.

    " Parse the comma-separated cluster endpoints
    " Expected format: "https://endpoint1.com|us-west-2,https://endpoint2.com|us-
east-1"
    SPLIT iv_cluster_endpoints AT ',' INTO TABLE lt_endpoints.

    " As a best practice, shuffle cluster endpoints to distribute load
    " For more information, see https://docs.aws.amazon.com/r53recovery/latest/
dg/route53-arc-best-practices.html#route53-arc-best-practices.regional
    " For simplicity, we'll try them in order (shuffling can be added if needed)

    " Try each endpoint in order
    LOOP AT lt_endpoints INTO lv_endpoint.
      TRY.
          " Parse endpoint and region from the format "url|region"
          DATA(lv_pos) = find( val = lv_endpoint sub = '|' ).
          IF lv_pos > 0.
            DATA(lv_url) = substring( val = lv_endpoint len = lv_pos ).
            lv_region = substring( val = lv_endpoint off = lv_pos + 1 ).
          ELSE.
            " If no region specified, use default
            lv_url = lv_endpoint.
            lv_region = 'us-east-1'.
          ENDIF.
```

```
        " Create session for this region
        lo_session = /aws1/cl_rt_session_aws=>create( cv_pfl ).

        " Create client with the specific endpoint
        lo_client = create_recovery_client(
          iv_endpoint = lv_url
          iv_region   = lv_region
          io_session  = lo_session ).

        " Try to get the routing control state
        oo_result = lo_client->getroutingcontrolstate(
          iv_routingcontrolarn = iv_routing_control_arn ).

        " If successful, return the result
        RETURN.

      CATCH /aws1/cx_r5vendpttmpyunavailex INTO DATA(lo_endpoint_ex).
        " This endpoint is temporarily unavailable, try the next one
        lo_exception = lo_endpoint_ex.
        CONTINUE.

      CATCH /aws1/cx_r5vaccessdeniedex
            /aws1/cx_r5vinternalserverex
            /aws1/cx_r5vresourcenotfoundex
            /aws1/cx_r5vthrottlingex
            /aws1/cx_r5vvalidationex
            /aws1/cx_rt_generic INTO lo_exception.
        " For other errors, re-raise immediately
        RAISE EXCEPTION lo_exception.
    ENDTRY.
  ENDLOOP.

  " If we get here, all endpoints failed - re-raise the last exception
  IF lo_exception IS BOUND.
    RAISE EXCEPTION lo_exception.
  ENDIF.
```

- Per i dettagli sulle API, GetRoutingControlStateconsulta AWS SDK for SAP ABAP API reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di questo servizio con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzare **`UpdateRoutingControlState`** con un SDK AWS

Gli esempi di codice seguenti mostrano come utilizzare `UpdateRoutingControlState`.

Java

SDK per Java 2.x

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
    public static UpdateRoutingControlStateResponse
 updateRoutingControlState(List<ClusterEndpoint> clusterEndpoints,
            String routingControlArn,
            String routingControlState) {
        // As a best practice, we recommend choosing a random cluster endpoint to
 get or
        // set routing control states.
        // For more information, see
        // https://docs.aws.amazon.com/r53recovery/latest/dg/route53-arc-best-
practices.html#route53-arc-best-practices.regional
        Collections.shuffle(clusterEndpoints);
        for (ClusterEndpoint clusterEndpoint : clusterEndpoints) {
            try {
                System.out.println(clusterEndpoint);
                Route53RecoveryClusterClient client =
 Route53RecoveryClusterClient.builder()
                        .endpointOverride(URI.create(clusterEndpoint.endpoint()))
                        .region(Region.of(clusterEndpoint.region()))
                        .build();
                return client.updateRoutingControlState(
                        UpdateRoutingControlStateRequest.builder()

 .routingControlArn(routingControlArn).routingControlState(routingControlState).build());
            } catch (Exception exception) {
```

```
                System.out.println(exception);
            }
        }
        return null;
    }
```

- Per i dettagli sull'API, UpdateRoutingControlStateconsulta AWS SDK for Java 2.x API Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
import boto3


def create_recovery_client(cluster_endpoint):
    """
    Creates a Boto3 Route 53 Application Recovery Controller client for the
 specified
    cluster endpoint URL and AWS Region.

    :param cluster_endpoint: The cluster endpoint URL and Region.
    :return: The Boto3 client.
    """
    return boto3.client(
        "route53-recovery-cluster",
        endpoint_url=cluster_endpoint["Endpoint"],
        region_name=cluster_endpoint["Region"],
    )



def update_routing_control_state(
```

```
    routing_control_arn, cluster_endpoints, routing_control_state
):
    """
    Updates the state of a routing control. Cluster endpoints are tried in
    sequence until the first successful response is received.

    :param routing_control_arn: The ARN of the routing control to update the
 state for.
    :param cluster_endpoints: The list of cluster endpoints to try.
    :param routing_control_state: The new routing control state.
    :return: The routing control update response.
    """

    # As a best practice, we recommend choosing a random cluster endpoint to get
 or set routing control states.
    # For more information, see https://docs.aws.amazon.com/r53recovery/latest/
dg/route53-arc-best-practices.html#route53-arc-best-practices.regional
    random.shuffle(cluster_endpoints)
    for cluster_endpoint in cluster_endpoints:
        try:
            recovery_client = create_recovery_client(cluster_endpoint)
            response = recovery_client.update_routing_control_state(
                RoutingControlArn=routing_control_arn,
                RoutingControlState=routing_control_state,
            )
            return response
        except Exception as error:
            print(error)
```

- Per i dettagli sull'API, consulta UpdateRoutingControlState AWSSDK for Python (Boto3) API Reference.

SAP ABAP

SDK per SAP ABAP

> **Note**
>
> C'è altro da fare. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
    CONSTANTS cv_pfl TYPE /aws1/rt_profile_id VALUE 'ZCODE_DEMO'.
    DATA lo_exception TYPE REF TO /aws1/cx_rt_generic.
    DATA lo_session TYPE REF TO /aws1/cl_rt_session_base.
    DATA lo_client TYPE REF TO /aws1/if_r5v.
    DATA lt_endpoints TYPE TABLE OF string.
    DATA lv_endpoint TYPE string.
    DATA lv_region TYPE /aws1/rt_region_id.

    " Parse the comma-separated cluster endpoints
    " Expected format: "https://endpoint1.com|us-west-2,https://endpoint2.com|us-
east-1"
    SPLIT iv_cluster_endpoints AT ',' INTO TABLE lt_endpoints.

    " As a best practice, shuffle cluster endpoints to distribute load
    " For more information, see https://docs.aws.amazon.com/r53recovery/latest/
dg/route53-arc-best-practices.html#route53-arc-best-practices.regional
    " For simplicity, we'll try them in order (shuffling can be added if needed)

    " Try each endpoint in order
    LOOP AT lt_endpoints INTO lv_endpoint.
      TRY.
          " Parse endpoint and region from the format "url|region"
          DATA(lv_pos) = find( val = lv_endpoint sub = '|' ).
          IF lv_pos > 0.
            DATA(lv_url) = substring( val = lv_endpoint len = lv_pos ).
            lv_region = substring( val = lv_endpoint off = lv_pos + 1 ).
          ELSE.
            " If no region specified, use default
            lv_url = lv_endpoint.
            lv_region = 'us-east-1'.
          ENDIF.
```

```
        " Create session for this region
        lo_session = /aws1/cl_rt_session_aws=>create( cv_pfl ).

        " Create client with the specific endpoint
        lo_client = create_recovery_client(
          iv_endpoint = lv_url
          iv_region   = lv_region
          io_session  = lo_session ).

        " Try to update the routing control state
        oo_result = lo_client->updateroutingcontrolstate(
          iv_routingcontrolarn     = iv_routing_control_arn
          iv_routingcontrolstate   = iv_routing_control_state
          it_safetyrulestooverride = it_safety_rules_override ).

        " If successful, return the result
        RETURN.

      CATCH /aws1/cx_r5vendpttmpyunavailex INTO DATA(lo_endpoint_ex).
        " This endpoint is temporarily unavailable, try the next one
        lo_exception = lo_endpoint_ex.
        CONTINUE.

      CATCH /aws1/cx_r5vaccessdeniedex
            /aws1/cx_r5vconflictexception
            /aws1/cx_r5vinternalserverex
            /aws1/cx_r5vresourcenotfoundex
            /aws1/cx_r5vthrottlingex
            /aws1/cx_r5vvalidationex
            /aws1/cx_rt_generic INTO lo_exception.
        " For other errors, re-raise immediately
        RAISE EXCEPTION lo_exception.
    ENDTRY.
  ENDLOOP.

  " If we get here, all endpoints failed - re-raise the last exception
  IF lo_exception IS BOUND.
    RAISE EXCEPTION lo_exception.
  ENDIF.
```

- Per i dettagli sulle API, UpdateRoutingControlStateconsulta AWS SDK for SAP ABAP API reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di questo servizio con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Sicurezza in Amazon Application Recovery Controller

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 in Cloud AWS. AWS fornisce inoltre servizi che è possibile 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 informazioni sui programmi di conformità che si applicano ad Amazon Application Recovery Controller, consulta AWS Services in Scope by Compliance Program AWS .
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. L'utente è anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della propria azienda e le leggi e normative vigenti.

Questa documentazione aiuta a capire come applicare il modello di responsabilità condivisa quando si utilizza ARC. I seguenti argomenti mostrano come configurare ARC per soddisfare gli obiettivi di sicurezza e conformità. Imparerai anche come utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere le tue risorse ARC.

Argomenti

- Protezione dei dati in Amazon Application Recovery Controller
- Identity and Access Management per Amazon Application Recovery Controller (ARC)
- Registrazione e monitoraggio in ARC
- Convalida della conformità per Amazon Application Recovery Controller
- Resilienza in Amazon Application Recovery Controller
- Sicurezza dell'infrastruttura in Amazon Application Recovery Controller

Protezione dei dati in Amazon Application Recovery Controller

Il modello di responsabilità AWS condivisa modello si applica alla protezione dei dati in Amazon Application Recovery Controller. 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 maggiori informazioni sulla privacy dei dati, consulta le Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al AWS Modello di responsabilità condivisa e GDPR nel AWS Blog sulla sicurezza.

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. Suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- SSL/TLS Da utilizzare per comunicare con AWS le risorse. 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 ARC o altri utenti 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 si fornisce un URL a un server esterno,

suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la richiesta al server.

Crittografia dei dati a riposo

Le informazioni di configurazione del cliente archiviate da Amazon Application Recovery Controller sono crittografate quando sono inutilizzate.

Crittografia dei dati in transito

Le richieste e le risposte dei clienti per Amazon Application Recovery Controller vengono crittografate durante il trasporto attraverso il servizio utilizzando TLS.

Identity and Access Management per Amazon Application Recovery Controller (ARC)

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

Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia in base al tuo ruolo:

- Utente del servizio: richiedi le autorizzazioni all'amministratore se non riesci ad accedere alle funzionalità (consulta Risoluzione dei problemi di identità e accesso ad Amazon Application Recovery Controller (ARC))
- Amministratore del servizio: determina l'accesso degli utenti e invia le richieste di autorizzazione (consulta In che modo le funzionalità di Amazon Application Recovery Controller (ARC) funzionano con IAM)
- Amministratore IAM: scrivi policy per gestire l'accesso (consulta Esempi di policy basate sull'identità in Amazon Application Recovery Controller (ARC))

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi autenticarti come utente IAM o assumendo un ruolo IAM. Utente root dell'account AWS

Puoi accedere come identità federata utilizzando credenziali provenienti da una fonte di identità come AWS IAM Identity Center (IAM Identity Center), autenticazione Single Sign-On o credenziali. Google/ Facebook Per ulteriori informazioni sull'accesso, consulta Come accedere all' Account AWS nella Guida per l'utente di Accedi ad AWS .

Per l'accesso programmatico, AWS fornisce un SDK e una CLI per firmare crittograficamente le richieste. Per ulteriori informazioni, consulta AWS Signature Version 4 per le richieste API nella Guida per l'utente di IAM.

Account AWS utente root

Quando si crea un Account AWS, si inizia con un'identità di accesso denominata utente Account AWS root che ha accesso completo a tutte Servizi AWS le risorse. Consigliamo vivamente di non utilizzare l'utente root per le attività quotidiane. Per le attività che richiedono le credenziali dell'utente root, consulta Attività che richiedono le credenziali dell'utente root nella Guida per l'utente IAM.

Identità federata

Come procedura ottimale, richiedi agli utenti umani di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente della directory aziendale, del provider di identità Web o Directory Service che accede Servizi AWS utilizzando le credenziali di una fonte di identità. Le identità federate assumono ruoli che forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, si consiglia di utilizzare AWS IAM Identity Center. Per ulteriori informazioni, consulta Che cos'è il Centro identità IAM? nella Guida per l'utente di AWS IAM Identity Center .

Utenti e gruppi IAM

Un utente IAM è una identità che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ti consigliamo di utilizzare credenziali temporanee invece di utenti IAM con credenziali a lungo termine. Per ulteriori informazioni, consulta Richiedere agli utenti umani di utilizzare la

federazione con un provider di identità per accedere AWS utilizzando credenziali temporanee nella Guida per l'utente IAM.

Un gruppo IAM specifica una raccolta di utenti IAM e semplifica la gestione delle autorizzazioni per gestire gruppi di utenti di grandi dimensioni. Per ulteriori informazioni, consulta Casi d'uso per utenti IAM nella Guida per l'utente di IAM.

Ruoli IAM

Un ruolo IAM è un'identità con autorizzazioni specifiche che fornisce credenziali temporanee. Puoi assumere un ruolo passando da un ruolo utente a un ruolo IAM (console) o chiamando un'operazione AWS CLI o AWS API. Per ulteriori informazioni, consulta Metodi per assumere un ruolo nella Guida per l'utente di IAM.

I ruoli IAM sono utili per l'accesso degli utenti federati, le autorizzazioni utente IAM temporanee, l'accesso multi-account, l'accesso multi-servizio e le applicazioni in esecuzione su Amazon EC2. Per maggiori informazioni, consultare Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Gestione dell'accesso tramite policy

Puoi controllare l'accesso AWS creando policy e associandole a AWS identità o risorse. Una policy definisce le autorizzazioni quando è associata a un'identità o a una risorsa. AWS valuta queste politiche quando un preside effettua una richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per maggiori informazioni sui documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente IAM.

Utilizzando le policy, gli amministratori specificano chi ha accesso a cosa definendo quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Un amministratore IAM crea le policy IAM e le aggiunge ai ruoli, che gli utenti possono quindi assumere. Le policy IAM definiscono le autorizzazioni indipendentemente dal metodo utilizzato per eseguirle.

Policy basate sull'identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile collegare a un'identità (utente, gruppo o ruolo). Tali policy controllano le operazioni autorizzate per l'identità, nonché le risorse e le condizioni in cui possono essere eseguite. Per informazioni su come

creare una policy basata su identità, consultare Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente IAM.

Le policy basate su identità possono essere policy in linea (con embedding direttamente in una singola identità) o policy gestite (policy autonome collegate a più identità). Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scegliere tra policy gestite e policy in linea nella Guida per l'utente di IAM.

Policy basate sulle risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi includono le policy di trust dei ruoli IAM e le policy dei bucket di Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. In una policy basata sulle risorse è obbligatorio specificare un'entità principale.

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

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi che possono impostare le autorizzazioni massime concesse dai tipi di policy più comuni:

- Limiti delle autorizzazioni: imposta il numero massimo di autorizzazioni che una policy basata su identità ha la possibilità di concedere a un'entità IAM. Per ulteriori informazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente di IAM.
- Politiche di controllo del servizio (SCPs): specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa in. AWS Organizations Per ulteriori informazioni, consultare Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations .
- Politiche di controllo delle risorse (RCPs): imposta le autorizzazioni massime disponibili per le risorse nei tuoi account. Per ulteriori informazioni, consulta Politiche di controllo delle risorse (RCPs) nella Guida per l'AWS Organizations utente.
- Policy di sessione: policy avanzate passate come parametro quando si crea una sessione temporanea per un ruolo o un utente federato. Per maggiori informazioni, consultare Policy di sessione nella Guida per l'utente IAM.

Più tipi di policy

Quando a una richiesta si applicano più tipi di policy, 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 Logica di valutazione delle policy nella IAM User Guide.

In che modo le funzionalità di Amazon Application Recovery Controller (ARC) funzionano con IAM

Per informazioni su come ogni funzionalità di Amazon Application Recovery Controller (ARC) funziona con IAM, consulta i seguenti argomenti:

- IAM per lo spostamento zonale
- IAM per lo spostamento automatico zonale
- IAM per il controllo del routing
- IAM per il controllo di prontezza
- IAM per il cambio di regione

Esempi di policy basate sull'identità in Amazon Application Recovery Controller (ARC)

Per vedere esempi di policy basate sull'identità per ogni funzionalità in Amazon Application Recovery Controller (ARC), consulta i seguenti argomenti nei AWS Identity and Access Management capitoli per ciascuna funzionalità:

- Esempi di policy basate sull'identità per lo spostamento automatico zonale in ARC
- Esempi di politiche basate sull'identità per il cambiamento di zona in ARC
- Esempi di policy basate sull'identità per il controllo del routing in ARC
- Esempi di policy basate sull'identità per il controllo di idoneità in ARC

AWS politiche gestite per Amazon Application Recovery Controller (ARC)

Per informazioni sulle politiche AWS gestite per le funzionalità ARC con politiche gestite, inclusa una politica gestita per un ruolo collegato ai servizi, consulta i seguenti argomenti:

- Policy gestite per lo spostamento automatico zonale

- Policy gestite per il controllo del routing
- Policy gestite per il controllo della prontezza

Aggiornamenti alle politiche AWS gestite per Amazon Application Recovery Controller (ARC)

Visualizza i dettagli sugli aggiornamenti alle politiche AWS gestite per le funzionalità in ARC 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 documenti ARC.

Modifica	Descrizione	Data
AmazonApplicationRecoveryControllerRegionSwitchPlanExecutionPolicy: nuova policy	Amazon Application Recovery Controller (ARC) ha rilasciato una nuova policy gestita che concede le autorizzazioni per l'esecuzione e la valutazione del piano di switch di regione. Questa policy fornisce l'accesso in sola lettura alle informazioni sul piano di cambio di regione, allo stato di esecuzione e ai dati di CloudWatch monitoraggio di Amazon. Include anche l'autorizzazione a simulare le principali politiche IAM per la valutazione del piano.	3 novembre 2025
AWSZonalAutoshiftPracticeRunSLRPolicy politica gestita: politica aggiornata	Aggiunge la dichiarazione politica `Autoshift PracticeCheckPermissions` con le autorizzazioni `autoscaling:DescribeAutoScalingGroups`	30 giugno 2025

Modifica	Descrizione	Data
	e `elasticloadbalancing:DescribeTargetHealth` per supportare `elasticloadbalancing:DescribeTargetHealth` i controlli bilanciati della capacità. `ec2:DescribeInstances` Per ulteriori informazioni, consulta Come funzionano gli autoshift e le esecuzioni pratiche zonali.	
AWSServiceRoleForPercPracticePolicy— Nuova politica	ARC ha aggiunto un nuovo ruolo collegato ai servizi per l'autoshift e le esecuzioni pratiche. ARC utilizza le autorizzazioni abilitate dal ruolo collegato al servizio per monitorare gli CloudWatch allarmi Amazon forniti dai clienti e Health Dashboard gli eventi dei clienti per le sessioni di prova e per avviare le sessioni di prova. Per ulteriori informazioni sul nuovo ruolo collegato ai servizi, consulta. Autorizzazioni di ruolo collegate ai servizi per AWSServiceRoleForZonalAutoshiftPracticeRun	30 novembre 2023

Modifica	Descrizione	Data
AmazonRoute53 RecoveryControlConfigReadOnlyAccess — Politica aggiornata	Aggiunge le autorizzazioni per`GetResourcePolicy` , per supportare la restituzione di dettagli sulle politiche AWS Resource Access Manager delle risorse per le risorse condivise.	18 ottobre 2023

Route53 RecoveryReadinessServiceRolePolicy — Politica aggiornata	ARC ha aggiunto nuove autorizzazioni per richieder e informazioni sulle istanze Amazon EC2.
	
	ARC utilizza le seguenti autorizzazioni per supportare il polling delle istanze Amazon EC2, eseguire controlli di fattibilità e determinare lo stato di disponibilità delle istanze.
	
	`ec2:DescribeVpnGateways`
	
	`ec2:DescribeCustomerGateways`
		17 febbraio 2023

Modifica	Descrizione	Data
RecoveryReadinessServiceRolePolicyRoute53: politica aggiornata	ARC ha aggiunto una nuova autorizzazione per interrogare informazioni sulle funzioni Lambda. ARC utilizza la seguente autorizzazione per interrogare informazioni sulle funzioni Lambda per eseguire controlli di preparazione e determinare lo stato di preparazione delle funzioni. `lambda:ListProvisionedConcurrencyConfigs`	31 agosto 2022
AmazonRoute53 RecoveryControlConfigFullAccess — Politica aggiornata	Sono state rimosse le autorizzazioni Amazon Route 53 dalla policy e è stata aggiunta una nota che elenca le autorizzazioni opzionali.	26 maggio 2022
AmazonRoute53 RecoveryControlConfigFullAccess — Politica aggiornata	Sono state aggiunte le autorizzazioni Amazon Route 53 richieste mancanti alla policy.	15 aprile 2022
AmazonRoute53 RecoveryClusterReadOnlyAccess — Politica aggiornata	ARC ha aggiunto una nuova autorizzazione per consentire il controllo del routing delle inserzioni ARNs con elevata disponibilità. `route53-recovery-cluster:ListRoutingControls`	15 marzo 2022

Modifica	Descrizione	Data
AmazonRoute53 RecoveryControlConfigReadOnlyAccess — Politica aggiornata	ARC ha aggiunto una nuova autorizzazione per consentire l'elenco dei tag per una risorsa. `route53-recovery-control-config:ListTagsForResources`	20 dicembre 2021
Route53 RecoveryReadinessServiceRolePolicy — Politica aggiornata	ARC ha aggiunto una nuova autorizzazione per richiedere informazioni su Amazon API Gateway. ARC utilizza l'autorizzazione per richiedere informazioni su API Gateway per eseguire controlli di disponibilità e determinare lo stato di disponibilità. `apigateway:GET`	28 ottobre 2021

Modifica	Descrizione	Data
AmazonRoute53 RecoveryReadinessReadOnlyAccess — Aggiunte nuove autorizzazioni	ARC ha aggiunto due nuove autorizzazioni a AmazonRoute 53: RecoveryReadinessReadOnlyAccess ARC utilizza `route53-recovery-readiness:GetArchitectureRecommendations` e `route53-recovery-readiness:GetCellReadinessSummary` consente l'accesso in sola lettura a queste azioni per garantire la disponibilità al ripristino.	15 ottobre 2021

Modifica	Descrizione	Data

Route53 RecoveryReadinessServiceRolePolicy — Politica aggiornata	ARC ha aggiunto nuove autorizzazioni per interrogare informazioni sulle funzioni Lambda.
	
	ARC utilizza le seguenti autorizzazioni per interrogare informazioni sulle funzioni Lambda per eseguire controlli di preparazione e determinare lo stato di preparazione di tali funzioni.
	
	`lambda:GetFunctionConcurrency`
	
	`lambda:GetFunctionConfiguration`
	
	`lambda:GetProvisionedConcurrencyConfig`
	
	`lambda:ListAliases`
	
	`lambda:ListVersionsByFunction`
	
	`lambda:ListEventSourceMappings`
	
	`lambda:ListFunctions`
		8 ottobre 2021

Modifica	Descrizione	Data
Route53 RecoveryReadinessServiceRolePolicy — Aggiunte nuove politiche gestite	ARC ha aggiunto le seguenti nuove politiche gestite: AmazonRoute53 RecoveryReadinessFullAccess AmazonRoute53 RecoveryReadinessReadOnlyAccess AmazonRoute53 RecoveryClusterFullAccess AmazonRoute53 RecoveryClusterReadOnlyAccess AmazonRoute53 RecoveryControlConfigFullAccess AmazonRoute53 RecoveryControlConfigReadOnlyAccess	18 agosto 2021
ARC ha iniziato a tracciare le modifiche	ARC ha iniziato a tenere traccia delle modifiche per le sue politiche AWS gestite.	27 luglio 2021

Risoluzione dei problemi di identità e accesso ad Amazon Application Recovery Controller (ARC)

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con Amazon Application Recovery Controller (ARC) e IAM.

Argomenti

- Non sono autorizzato a eseguire un'azione in ARC
- Non sono autorizzato a eseguire iam: PassRole
- Voglio consentire a persone esterne a me di accedere Account AWS alle mie risorse ARC

Non sono autorizzato a eseguire un'azione in ARC

Se ti Console di gestione AWS dice che non sei autorizzato a eseguire un'azione, devi contattare l'amministratore per ricevere assistenza. L'amministratore è la persona che ti ha fornito le credenziali.

L'errore di esempio seguente si verifica quando l'utente `mateojackson` IAM prova a utilizzare la console per visualizzare i dettagli relativi a una risorsa *`my-example-widget`* fittizia ma non dispone di autorizzazioni `route53-recovery-readiness:`*`GetWidget`* fittizie.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 route53-recovery-readiness:GetWidget on resource: my-example-widget
```

In questo caso, Mateo chiede al suo amministratore di aggiornare le policy per poter accedere alla risorsa *`my-example-widget`* mediante l'operazione `route53-recovery-readiness:`*`GetWidget`*.

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 ad ARC.

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.

L'errore di esempio seguente si verifica quando un utente IAM denominato `marymajor` tenta di utilizzare la console per eseguire un'azione in ARC. Tuttavia, l'azione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per trasmettere 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 mie risorse ARC

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 maggiori informazioni, consulta gli argomenti seguenti:

- Per sapere se ARC supporta queste funzionalità, consulta. In che modo le funzionalità di Amazon Application Recovery Controller (ARC) funzionano con IAM
- Per scoprire come fornire l'accesso alle tue risorse attraverso Account AWS le risorse di tua proprietà, 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 di IAM.

Accedi allo shift zonale di Amazon Application Recovery Controller (ARC) utilizzando un endpoint di interfaccia ()AWS PrivateLink

Puoi utilizzarlo AWS PrivateLink per creare una connessione privata tra il tuo VPC e lo spostamento zonale di Amazon Application Recovery Controller (ARC). Puoi accedere a ARC zonal shift come se fosse nel tuo VPC, senza l'uso di un gateway Internet, un dispositivo NAT, una connessione VPN o una connessione. Direct Connect Le istanze nel tuo VPC non necessitano di indirizzi IP pubblici per accedere allo spostamento zonale ARC.

Stabilisci questa connessione privata creando un endpoint di interfaccia attivato da AWS PrivateLink. In ciascuna sottorete viene creata un'interfaccia di rete endpoint da abilitare per l'endpoint di interfaccia. Si tratta di interfacce di rete gestite dai richiedenti che fungono da punto di ingresso per il traffico destinato allo spostamento zonale ARC.

Per ulteriori informazioni, consulta Access Servizi AWS through nella Guida. AWS PrivateLinkAWS PrivateLink

Considerazioni sullo spostamento zonale ARC

Prima di configurare un endpoint di interfaccia per lo spostamento zonale ARC, consulta le considerazioni nella Guida.AWS PrivateLink

ARC zonal shift supporta l'effettuazione di chiamate a tutte le sue azioni API tramite l'endpoint dell'interfaccia.

Crea un endpoint di interfaccia per ARC zonal shift

Puoi creare un endpoint di interfaccia per ARC zonal shift utilizzando la console Amazon VPC o il (). AWS Command Line Interface AWS CLI Per ulteriori informazioni, consulta la sezione Creazione di un endpoint di interfaccia nella Guida per l'utente di AWS PrivateLink .

Crea un endpoint di interfaccia per ARC zonal shift utilizzando il seguente nome di servizio:

```
com.amazonaws.region.arc-zonal-shift
```

Se abiliti il DNS privato per l'endpoint dell'interfaccia, puoi effettuare richieste API a ARC zonal shift utilizzando il nome DNS regionale predefinito. Ad esempio, `arc-zonal-shift.us-east-1.amazonaws.com`.

Creazione di una policy dell' endpoint per l'endpoint dell'interfaccia

Una policy dell'endpoint è una risorsa IAM che è possibile allegare all'endpoint dell'interfaccia. La policy predefinita per gli endpoint consente l'accesso completo a ARC zonal shift tramite l'endpoint dell'interfaccia. Per controllare l'accesso consentito allo spostamento zonale di ARC dal tuo VPC, collega una policy endpoint personalizzata all'endpoint dell'interfaccia.

Una policy di endpoint specifica le informazioni riportate di seguito:

- I principali che possono eseguire azioni (Account AWS, utenti IAM e ruoli IAM).
- Le azioni che possono essere eseguite.
- Le risorse in cui è possibile eseguire le operazioni.

Per ulteriori informazioni, consulta la sezione Controllo dell'accesso ai servizi con policy di endpoint nella Guida di AWS PrivateLink .

Esempio: politica degli endpoint VPC per le azioni di spostamento zonale ARC

Di seguito è riportato l'esempio di una policy dell'endpoint personalizzata. Quando alleghi questa policy all'endpoint dell'interfaccia, concede l'accesso alle azioni di spostamento zonale ARC elencate per tutti i principali su tutte le risorse.

```
{
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [
            "arc-zonal-shift:ListManagedResources",
            "arc-zonal-shift:StartZonalShift",
            "arc-zonal-shift:CancelZonalShift"
         ],
         "Resource":"*"
      }
   ]
}
```

`Resource`Possono anche essere elencati come. `arn:aws:elasticloadbalancing:us-east-1:111122223333:loadbalancer/app/Testing/1111111ecd42dc05`

Registrazione e monitoraggio in ARC

Il monitoraggio è una parte importante per mantenere la disponibilità e le prestazioni di ARC e delle vostre AWS soluzioni. È necessario raccogliere i dati di monitoraggio da tutte le parti della AWS soluzione in modo da poter eseguire più facilmente il debug di un errore multipunto, se si verifica. AWS fornisce diversi strumenti per monitorare le risorse e le attività di ARC e rispondere a potenziali incidenti, ad esempio, e AWS CloudTrail Amazon. CloudWatch

Per informazioni sul monitoraggio di ciascuna funzionalità in ARC, consulta i seguenti argomenti:

- Registrazione e monitoraggio dello spostamento zonale
- Registrazione e monitoraggio per lo spostamento automatico zonale
- Registrazione e monitoraggio per il controllo del routing
- Registrazione e monitoraggio per Region Switch
- Registrazione e monitoraggio per il controllo di prontezza

Convalida della conformità per Amazon Application Recovery Controller

I revisori di terze parti valutano la sicurezza e la conformità di Amazon Application Recovery Controller nell'ambito di diversi programmi di AWS conformità. Sono inclusi SOC, PCI e HIPAA.

Per sapere se un Servizio AWS programma rientra nell'ambito di specifici programmi di conformità, consulta Servizi AWS la sezione Scope by Compliance Program Servizi AWS e scegli il programma di conformità che ti interessa. Per informazioni generali, consulta Programmi di AWS conformità Programmi di di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Scaricamento dei report in AWS Artifact .

La vostra responsabilità di conformità durante l'utilizzo Servizi AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. Per ulteriori informazioni sulla responsabilità di conformità durante l'utilizzo Servizi AWS, consulta la Documentazione AWS sulla sicurezza.

Resilienza in Amazon Application Recovery Controller

L'infrastruttura AWS globale è costruita attorno a Regioni AWS zone di disponibilità. Regioni AWS forniscono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti. Con le zone di disponibilità è possibile progettare e gestire applicazioni e database che eseguono automaticamente il failover tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture a data center singolo o multiplo tradizionali.

Per ulteriori informazioni sulle zone di disponibilità, vedere Global Regioni AWS Infrastructure.AWS

Oltre all'infrastruttura AWS globale, ARC offre diverse funzionalità per supportare le esigenze di resilienza e backup dei dati.

Sicurezza dell'infrastruttura in Amazon Application Recovery Controller

In quanto servizio gestito, è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi AWS di sicurezza e su come AWS protegge l'infrastruttura, consulta AWS Cloud Security. Per

progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Utilizzate chiamate API AWS pubblicate per accedere ad ARC attraverso la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), 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.

Cronologia dei documenti per l'Amazon Application Recovery Controller (ARC) Developer Guide

Le seguenti voci descrivono importanti modifiche apportate alla documentazione di Amazon Application Recovery Controller (ARC).

- Versione: più recente
- Ultimo aggiornamento della documentazione: 31 marzo 2026

Modifica	Descrizione	Data
Readiness Check, modifica della disponibilità	La funzionalità di controllo della disponibilità in Amazon Application Recovery Controller (ARC) non sarà più aperta ai nuovi clienti a partire dal 30 aprile 2026. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta Amazon Application Recovery Controller (ARC) readiness check availability change.	31 marzo 2026
Nuova politica gestita per l'esecuzione del piano di cambio di regione	Amazon Application Recovery Controller (ARC) ha rilasciato una nuova policy gestita che concede le autorizzazioni per l'esecuzione e la valutazione del piano di cambio di regione. `AmazonApplicationRecoveryControllerR`	3 novembre 2025

Modifica	Descrizione	Data
	`egionSwitchPlanExecutionPolicy` Per ulteriori informazioni, consulta gli aggiornamenti di Amazon Application Recovery Controller (ARC) alle policy AWS gestite.	
Ora puoi utilizzare il trasferimento zonale AWS PrivateLink tra il tuo VPC e Amazon Application Recovery Controller (ARC).	Puoi usare an AWS PrivateLink per creare una connessione privata tra il tuo VPC e lo spostamento zonale di Amazon Application Recovery Controller (ARC). Per ulteriori informazioni, consulta Accedere allo spostamento zonale di Amazon Application Recovery Controller (ARC) utilizzando un endpoint di interfaccia (AWS PrivateLink).	11 agosto 2025
Nuovo servizio di cambio di regione	Il cambio di regione consente ai clienti di orchestrare i passaggi specifici, supportando più account, necessari per far funzionare la propria applicazione multiregionale da un'altra. Regione AWS Per ulteriori informazioni, consulta Region switch in ARC.	1 agosto 2025

Modifica	Descrizione	Data
Miglioramenti alle corse di pratica	Ora puoi iniziare le esercitazioni su richiesta in ARC. Inoltre, le prove pratiche ora includono la verifica della capacità sufficiente AZs in altri paesi della regione. Per ulteriori informazioni, vedi Come funziona.	30 giugno 2025
Aggiorna una politica gestita	Aggiorna la politica `AWSZonalAutoshiftPracticeRunSLRPolicy` gestita aggiungendo la dichiarazione sulla politica `AutoshiftPracticeCheckPermissions` con le autorizzazioni `autoscaling:DescribeAutoScalingGroups` e `elasticloadbalancing:DescribeTargetHealth` per supportare `elasticloadbalancing:DescribeTargetHealth` i controlli bilanciati della capacità. `ec2:DescribeInstances` Per ulteriori informazioni, consulta la politica AWSZonalAutoshiftPracticeRunSLRPolicy gestita.	30 giugno 2025

Modifica	Descrizione	Data
Aggiornamenti ai tipi di eccezione per lo spostamento automatico zonale	Ora puoi interagire con lo spostamento automatico zonale in base alla risorsa. Per ulteriori informazioni, vedi Come funziona.	21 aprile 2025
Prova l'autoshift zonale ARC con AWS FIS	Puoi utilizzarlo AWS FIS per testare in che modo ARC zonal autoshift ripristin i automaticamente la tua applicazione durante un'interr uzione di corrente AZ Per ulteriori informazioni, vedere Testing zonal autoshift with. AWS FIS	26 marzo 2025
ARC ora supporta gli IPv6 endpoint per i controlli di routing e lo spostamento di zona.	ARC ora supporta gli IPv6 endpoint per i controlli di routing e lo spostamento di zona. Per ulteriori informazioni, consulta Configurare i componenti di controllo del routing.	21 novembre 2024
Capacità di spostamento zonale per i gruppi Amazon EC2 Auto Scaling	ARC ora supporta lo spostamento zonale per i gruppi Amazon EC2 Auto Scaling. Per ulteriori informazioni, consulta Support for Amazon EC2 Auto Scaling groups.	18 novembre 2024

Modifica	Descrizione	Data
Capacità di spostamento zonale per Amazon EKS	Puoi avviare uno spostamento di zona per un cluster Amazon EKS oppure puoi consentire di farlo AWS per te abilitando lo spostamento automatico di zona. Questa modifica aggiorna il flusso del traffico di east-to-west rete nel cluster in modo da prendere in considerazione solo gli endpoint di rete per i Pod in esecuzione sui nodi di lavoro in condizioni di integrità. AZs Per ulteriori informazioni, consulta Support for Amazon Elastic Kubernetes Service.	22 ottobre 2024
Capacità di spostamento zonale per Network Load Balancers	ARC ora supporta lo spostamento zonale per i Network Load Balancer con configurazioni abilitate tra zone o disabilitate tra zone. Per ulteriori informazioni, consulta Support for Network Load Balancers.	11 ottobre 2024

Modifica	Descrizione	Data
Notifiche di Autoshift Observer	Con le notifiche autoshift observer, puoi configurare lo spostamento automatico zonale in modo che ti avvisi, tramite EventBridge Amazon, AWS ogni volta che avvia uno spostamento automatico per spostare il traffico lontano da una zona di disponibilità potenzialmente compromessa. Non è necessario configurare alcuna risorsa specifica con lo spostamento automatico zonale per abilitare queste notifiche separate. Per ulteriori informazioni, consulta Usare lo spostamento automatico zonale con Amazon. EventBridge	12 luglio 2024

Modifica	Descrizione	Data
Riorganizzazione dei documenti per ciascuna funzionalità	Riorganizza il contenuto della guida per gli sviluppatori in modo che venga suddiviso in guide secondarie per gli sviluppatori. Cioè, ora ci sono sezioni separate che contengono informazioni complete per ogni funzionalità di ARC: zonal shift e zonal autoshift per il ripristino Multi-AZ, e il controllo del routing e il controllo della prontezza per il ripristino multiregionale. Per ulteriori informazioni, consulta Cos'è Amazon Application Recovery Controller (ARC).	30 aprile 2024
Aggiunge la funzionalità di spostamento automatico zonale	Aggiunge una nuova funzionalità in ARC che AWS autorizza a spostare il traffico di risorse per un'applicazione da una zona di disponibilità, per conto dell'utente, per contribuire a ridurre i tempi di ripristino durante gli eventi. Per ulteriori informazioni, consulta Zonal autoshift in Amazon Application Recovery Controller (ARC).	30 novembre 2023

Modifica	Descrizione	Data
Aggiunge un nuovo ruolo collegato al servizio	Aggiunge un nuovo ruolo collegato al servizio, per le esercitazioni di AWSServiceRoleForZonalAutoshiftPracticeRunautoshift zonale. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi per AWSServiceRoleForZonalAutoshiftPracticeRun.	30 novembre 2023
Aggiunge il supporto multiaccount per i cluster	Aggiunge il supporto per più account per i cluster in ARC with AWS Resource Access Manager, in modo da poter utilizzare in modo semplice e sicuro un cluster per ospitare pannelli di controllo e controlli di routing di proprietà di diversi account. AWS Per ulteriori informazioni, consulta Support cross-account per i cluster in ARC.	18 ottobre 2023

Modifica	Descrizione	Data
Aggiorna una politica gestita	Aggiorna la politica `AmazonRoute53RecoveryControlConfigReadOnly` gestita per cui aggiungere autorizzazioni `GetResourcePolicy`, per supportare la restituzione di dettagli sulle politiche AWS Resource Access Manager delle risorse per le risorse condivise. Per ulteriori informazioni, consulta le politiche AWS gestite.	19 settembre 2023
Ruolo collegato al servizio aggiornato	Sono state aggiunte nuove autorizzazioni `ec2:DescribeVpnGateways` e `ec2:DescribeCustomerGateways`, al ruolo collegato ai servizi per ARC, è stato supportato il polling delle istanze Amazon EC2. Per ulteriori informazioni, consulta Using service-linked roles for ARC.	17 febbraio 2023

Modifica	Descrizione	Data
Versione GA per il cambiamento di zona	Supporta la versione GA di zonal shift for ARC, che include il controllo degli accessi basato sugli attributi (ABAC) per le risorse gestite registrate in ARC per lo spostamento zonale. Per ulteriori informazioni, vedere Controllo degli accessi basato sugli attributi (ABAC) con ARC.	10 gennaio 2023
Aggiunto un nuovo spostamento zonale Multi-AZ	Aggiunto contenuto che descrive un nuovo servizio in ARC, zonal shift, per applicazioni Multi-AZ. È possibile avviare uno spostamento zonale per spostare temporaneamente il traffico di una risorsa di bilanciamento del carico lontano da una zona di disponibilità. Per ulteriori informazioni, consulta Spostamento zonale in ARC.	28 novembre 2022

Modifica	Descrizione	Data
Ruolo collegato al servizio aggiornato	È stata aggiunta una nuova autorizzazione`lambda:ListProvisionedConcurrencyConfigs` , al ruolo collegato al servizio per ARC per interrogare informazioni sulle funzioni Lambda. Per ulteriori informazioni, vedere Utilizzo dei ruoli collegati ai servizi per ARC.	31 agosto 2022
Policy gestite e aggiornate	È stata aggiornata la policy `AmazonRoute53RecoveryControlConfigFullAccess` gestita per rimuovere le autorizzazioni di Amazon Route 53 ed elencarle come opzionali. Per ulteriori informazioni, consulta le politiche AWS gestite per Amazon Application Recovery Controller (ARC).	26 maggio 2022
Policy gestite e aggiornate	È stata aggiornata la policy `AmazonRoute53RecoveryControlConfigFullAccess` gestita per includere le autorizzazioni Amazon Route 53 richieste. Per ulteriori informazioni, consulta le politiche AWS gestite per Amazon Application Recovery Controller (ARC).	15 aprile 2022

Modifica	Descrizione	Data
Aggiunto un esempio CLI per la nuova API dei controlli di routing delle liste	Sono stati aggiunti esempi di comandi CLI e raccomand azioni sulle migliori pratiche per il nuovo funzionamento dell'API List Routing Controls inclusa nell'API del piano dati ARC estremamente affidabile. Per ulteriori informazioni, consulta Elencare e aggiornar e i controlli e gli stati del routing.	31 marzo 2022
È stato aggiunto il supporto per ignorare le regole di sicurezza	È stato aggiunto il supporto per l'annullamento delle regole di sicurezza, che consente di aggirare le misure di controllo del routing applicate con le regole di sicurezza configura te. Le sostituzioni delle regole di sicurezza potrebbero essere necessarie, ad esempio, in uno scenario di «rottura del vetro» durante il failover per il disaster recovery. Per ulteriori informazioni, consulta Ignorare le regole di sicurezza per reindirizzare il traffico.	2 marzo 2022

Modifica	Descrizione	Data
È stato aggiunto un supporto aggiuntivo per l'etichettatura	È stato aggiunto il supporto per l'etichettatura di risorse aggiuntive in ARC, inclusi cluster, pannelli di controllo, controlli di routing e regole di sicurezza. Per ulteriori informazioni, consulta Tagging in Amazon Application Recovery Controller (ARC).	20 dicembre 2021
Policy gestite e aggiornate	È stata aggiornata la politica `AmazonRoute53RecoveryControlConfigReadOnly` gestita per aggiungere il permesso di elencare i tag di una risorsa. Per ulteriori informazioni, consulta le politiche AWS gestite per Amazon Application Recovery Controller (ARC)	20 dicembre 2021

Modifica	Descrizione	Data
È stato aggiunto il supporto per avvisi in tempo reale con EventBridge	È stato aggiunto il supporto per EventBridge, il che significa che ora puoi aggiungere regole per ricevere avvisi e agire in base alle modifiche dello stato di preparazione ARC, ad esempio quando uno stato passa da READY a NOT READY. Per ulteriori informazioni, consulta Usare ARC con Amazon EventBridge.	20 dicembre 2021
Sono stati aggiunti esempi di codice dello stato di controllo del routing	Sono stati aggiunti esempi di codice per illustrare l'utilizzo in sequenza degli endpoint del cluster quando si utilizzano le operazioni API per ottenere o aggiornare gli stati di controllo del routing. Per ulteriori informazioni, consulta esempi di API per Amazon Application Recovery Controller (ARC).	16 novembre 2021

Modifica	Descrizione	Data
Sono state aggiunte nuove autorizzazioni a una policy di sola lettura	Sono state aggiunte due nuove autorizzazioni alla politica: e. `AmazonRoute53RecoveryReadinessReadOnlyAccess` `route53-recovery-readiness:GetArchitectureRecommendations` `route53-recovery-readiness:GetCellReadinessSummary` Per ulteriori informazioni, consulta le politiche AWS gestite per Amazon Application Recovery Controller (ARC).	9 novembre 2021
È stato aggiunto il supporto per il tipo di risorsa Amazon API Gateway	È stato aggiunto un nuovo tipo di risorsa, Amazon API Gateway, e aggiornato le autorizzazioni dei ruoli collegati ai servizi ARC in modo che ARC possa controllare API Gateway con controlli di fattibilità. Per ulteriori informazioni, consulta Regole di preparazione e tipi di risorse supportati e Utilizzo dei ruoli collegati ai servizi per ARC.	28 ottobre 2021

Modifica	Descrizione	Data
Aggiunto il supporto per il tipo di risorsa delle funzioni Lambda	È stato aggiunto un nuovo tipo di risorsa, funzioni Lambda e sono state aggiornate le autorizzazioni dei ruoli collegati ai servizi ARC in modo che ARC possa controllare le funzioni Lambda con controlli di fattibilità. Per ulteriori informazioni, consulta Regole di preparazione e tipi di risorse supportati e Utilizzo dei ruoli collegati ai servizi per ARC.	8 ottobre 2021
Sono stati aggiunti collegamenti ai modelli Terraform CloudFormation	Sono stati aggiunti collegamenti ai modelli scaricabili CloudFormation e Hashicorp Terraform per aiutarti a iniziare rapidamente a usare Arc. Per ulteriori informazioni, consulta Recovery Readiness with a new application.	13 settembre 2021

Modifica	Descrizione	Data
Sono state aggiunte nuove politiche gestite	Sono state aggiunte le seguenti politiche AWS gestite per ARC: `AmazonRoute53RecoveryReadinessFullAccess` `AmazonRoute53RecoveryReadinessReadOnlyAccess` `AmazonRoute53RecoveryClusterFullAccess` ,`AmazonRoute53RecoveryClusterReadOnlyAccess` ,,`AmazonRoute53RecoveryControlConfigFullAccess` , `eAmazonRoute53RecoveryControlConfigReadOnlyAccess` . Per ulteriori informazioni, consulta le politiche AWS gestite per Amazon Application Recovery Controller (ARC).	18 agosto 2021
Ha iniziato a tracciare le politiche AWS gestite per Amazon Application Recovery Controller (ARC)	Gli aggiornamenti per le politiche gestite verranno monitorati dalla data di rilascio iniziale in poi. Per ulteriori informazioni, consulta le politiche AWS gestite per Amazon Application Recovery Controller (ARC).	27 luglio 2021

Modifica	Descrizione	Data
Versione iniziale di Amazon Application Recovery Controller (ARC)	ARC migliora la disponibilità delle applicazioni coordinando centralmente i failover all'interno di una AWS regione o tra più regioni. ARC fornisce controlli di fattibilità per garantire che le applicazioni siano scalabili per gestire il traffico di failover e configurate per aggirare i guasti. Fornisce inoltre un controllo del routing estremamente affidabile in modo da poter ripristinare le applicazioni reindirizzando il traffico, ad esempio, tra zone o regioni di disponibilità. Per ulteriori informazioni, consulta Cos'è ARC? .	27 luglio 2021

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.