aws

Guía para desarrolladores

Controlador de recuperación de aplicaciones de Amazon (ARC)

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Controlador de recuperación de aplicaciones de Amazon (ARC): Guía para desarrolladores

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon, de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas registradas que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

Table of Contents

¿Qué es ARC? 1
Recuperación de zonas de disponibilidad múltiple 1
Recuperación multirregional 2
Compare las capacidades multizona de disponibilidad y multirregión 4
Recuperación en zonas de disponibilidad múltiples 7
Cambio de zona 7
Cómo funciona un cambio de zona 8
Regiones de AWS 9
Componentes de cambio de zona 14
Planos de datos y control 16
Precios 17
Prácticas recomendadas 17
Operaciones de la API 19
Ejemplos de uso de las operaciones de la CLI 20
Recursos admitidos 24
Iniciar, actualizar o cancelar un cambio zonal 36
Registro y supervisión 38
IAM para el cambio zonal 43
Cambio automático de zona 54
Cómo funciona el cambio de zona 56
Regiones de AWS 66
Componentes del cambio automático de zona 67
Planos de datos y control 70
Precios 70
Prácticas recomendadas 71
Operaciones de la API 75
Ejemplos de uso de las operaciones de la CLI 77
Habilitar el cambio automático zonal y trabajar con él 83
Probando el cambio automático zonal con AWS FIS 88
Registro y supervisión 90
Identity and Access Management 101
Recuperación multirregional 117
Control de enrutamiento 117
Acerca del control de enrutamiento 118

AWS Regiones 121
Componentes 122
Planos de datos y control 125
Etiquetado 126
Precios 127
Cómo empezar con la recuperación multirregional 127
Prácticas recomendadas 129
Operaciones de la API 133
Ejemplos de uso de las operaciones de la CLI 137
Trabajar con componentes de control de enrutamiento 155
Registro y supervisión 175
Identity and Access Management 180
Cuotas 194
Verificación de preparación 195
¿Qué es la verificación de disponibilidad? 196
AWS Regiones 205
Componentes 205
Planos de datos y control 208
Etiquetado 208
Precios 209
Configure una aplicación resiliente 209
Prácticas recomendadas 210
Operaciones de la API 211
Ejemplos de uso de las operaciones de la CLI 214
Trabaje con grupos de recuperación y verificaciones de preparación 224
Monitorear el estado de preparación 230
Obtención de recomendaciones de arquitectura 231
Crear autorizaciones multicuenta 233
Reglas de preparación, tipos de recursos y ARNS 235
Registro y supervisión 257
Identity and Access Management 271
Cuotas 287
Cambio de región 288
Acerca de Region Switch 289
Prácticas recomendadas 297
Tutorial: Active/passive planificar 299

Operaciones de la API 306
Trabajando con el conmutador de región 308
Paneles 335
Compatibilidad entre cuentas 335
Identity and Access Management 341
Registro y supervisión 361
Cuotas 370
Ejemplos de código 371
Conceptos básicos 371
Acciones 372
Seguridad 378
Protección de los datos 379
Cifrado en reposo 380
Cifrado en tránsito 380
Identity and Access Management 380
Público 380
Autenticación con identidades 381
Administración de acceso mediante políticas 385
Cómo funcionan las capacidades de Amazon Application Recovery Controller (ARC) con IAM 388
Ejemplos de políticas basadas en identidades 388
AWS políticas gestionadas 388
Solución de problemas 395
Registro y supervisión 397
Validación de conformidad 398
Resiliencia 399
Seguridad de la infraestructura 400
Historial de documentos 401
..... cdxix

¿Qué es ARC?

Amazon Application Recovery Controller (ARC) le ayuda a preparar y completar una recuperación más rápida de las aplicaciones que se ejecutan en la infraestructura de nube AWS global.

ARC ofrece las siguientes capacidades:

- Recuperación en varias zonas de disponibilidad (AZ), que incluye el cambio zonal y el cambio automático zonal, que le permiten recuperarse de las deficiencias en una zona de disponibilidad única al trasladar temporalmente el tráfico de una zona de zona deteriorada a una zona en buen estado.
- Recuperación multirregional, que incluye el control de enrutamiento y el cambio de región para la recuperación de aplicaciones regionales, así como la comprobación de la disponibilidad para la supervisión de las aplicaciones.

Recuperación de zonas de disponibilidad múltiple

Cambio de zona

Puede utilizar el cambio zonal ARC para aislar y recuperarse rápidamente de las deficiencias de una sola zona de disponibilidad (AZ). El cambio zonal desplaza temporalmente el tráfico de un recurso compatible de una zona de disponibilidad deteriorada a uno AZs en buen estado en la misma región. AWS Iniciar un cambio zonal ayuda a que la aplicación se recupere rápidamente, por ejemplo, de una implementación de código incorrecto por parte de un desarrollador o de una avería en una AWS única zona de disponibilidad. Alejar el tráfico de la zona con problemas de zona reduce el impacto para los clientes que utilizan su aplicación en la zona con problemas de zona.

Puedes iniciar un cambio zonal para cualquier recurso compatible de tu cuenta en una AWS región. Los cambios zonales son manuales y temporales. Al iniciar un turno zonal, debe especificar un vencimiento (prorrogable) de hasta tres días. Para habilitar el cambio zonal para los recursos compatibles, consulte. Recursos admitidos

Cambio automático zonal

El cambio automático zonal ARC autoriza AWS a desviar el tráfico de una zona de disponibilidad deteriorada para obtener los recursos compatibles, en su nombre, a otro en buen estado AZs en la misma región. AWS AWS inicia un cambio automático zonal cuando la telemetría interna indica que hay una avería en una zona de una región que podría afectar a los clientes. AWS La telemetría

interna incorpora métricas de varias fuentes, incluida la AWS red y los servicios Amazon EC2 y Elastic Load Balancing.

Los cambios automáticos zonales son temporales. AWS finaliza un cambio automático zonal cuando los indicadores de telemetría internos muestran que ya no hay ningún problema o problema potencial.

Para obtener más información sobre estas funciones, consulte los capítulos siguientes:

- Cambio zonal en ARC
- Cambio automático zonal en ARC

Recuperación multirregional

Cambio de región

El conmutador regional de ARC proporciona una solución centralizada, automatizada y observable para la recuperación de aplicaciones en varias regiones. El cambio de región le ayuda a planificar y coordinar la recuperación de sus aplicaciones en todas sus aplicaciones Regiones de AWS, a fin de garantizar la continuidad empresarial y reducir los gastos operativos.

Puede usar Region Switch para organizar tareas de recuperación complejas y a gran escala para los recursos de sus aplicaciones, en varias AWS cuentas. Si una Región de AWS falla, los planes que cree con el cambio de región pueden conmutar por error o transferir sus recursos a otra región, de modo que su aplicación pueda seguir funcionando sin problemas. Región de AWS

Control de enrutamiento

Los controles de enrutamiento extremadamente confiables de ARC permiten la recuperación en varias regiones para que sus aplicaciones puedan conmutar por error el tráfico DNS del Sistema de Nombres de Dominio entre AWS regiones.

Si su aplicación está diseñada para funcionar desde varias AWS regiones, puede utilizar el control de enrutamiento ARC para realizar la conmutación por error entre regiones. El control de enrutamiento le permite conmutar por error el tráfico de una AWS región con problemas a una AWS región en buen estado, de modo que puede garantizar que su aplicación mantenga la disponibilidad. El control de enrutamiento incluye reglas de seguridad, que ayudan a protegerlo de resultados imprevistos al imponer barreras que usted defina. Por ejemplo, puede imponer una regla de seguridad que establezca que solo una de las réplicas de su aplicación, activa o en espera, esté habilitada y en uso.

Verificación de disponibilidad

La comprobación de disponibilidad de ARC supervisa continuamente las cuotas de AWS recursos, la capacidad y las políticas de enrutamiento de la red, y puede notificarle los cambios que puedan afectar a su capacidad de realizar la conmutación por error a una aplicación réplica y de recuperarse de una avería en la región. Las comprobaciones continuas de disponibilidad garantizan que pueda mantener sus aplicaciones multirregionales en un estado escalado y configurado para gestionar el tráfico de conmutación por error. La comprobación de disponibilidad resulta útil al configurar ARC por primera vez y durante el funcionamiento normal de la aplicación. La comprobación de disponibilidad no está destinada a utilizarse en la ruta crítica para la conmutación por error durante un evento.

Para obtener más información sobre estas capacidades, consulte los capítulos siguientes:

- Conmutador de región en ARC
- Control de enrutamiento en ARC
- Verificación de disponibilidad en ARC

Compare las capacidades de recuperación multizona y multirregión en ARC

El cambio zonal, el cambio automático zonal, el control de enrutamiento y el cambio regional de Amazon Application Recovery Controller (ARC) pueden lograr una recuperación rápida y ayudarlo a garantizar la resiliencia de sus aplicaciones. AWS Estas funciones están altamente disponibles y ayudan a respaldar la recuperación en situaciones en las que la aplicación experimenta un aumento de la latencia o una reducción de la disponibilidad. Estas funciones también ayudan a recuperar las aplicaciones rápidamente al desviar el tráfico de las deficiencias aisladas, lo que limita el impacto y el tiempo perdido por las deficiencias.

El control de enrutamiento y el cambio de región se centran en AWS aplicaciones que se encuentran en varias Regiones de AWS regiones, mientras que el cambio zonal y el cambio automático zonal solo admiten el cambio de tráfico para los recursos compatibles con aplicaciones multizona de disponibilidad.

La información de la siguiente tabla incluye algunas de las características clave de las capacidades de resiliencia del ARC. Estas descripciones pueden ayudarle a comprender mejor cómo una opción específica puede ser la mejor opción para las necesidades de su aplicación.

Control de enrutamiento	Cambio de región	Cambio de zona	Cambio automático de zona
Regional Redirige el tráfico de una AWS región a otra (principalmente)	Regional Redirige el tráfico de una AWS región a otra (principalmente)	De zona Aleja el tráfico de una zona de disponibilidad El tráfico se dirige a otras zonas de disponibilidad de la región, no a un objetivo específico	De zona Aleja el tráfico de una zona de disponibilidad El tráfico se dirige a otras zonas de disponibilidad de la región, no a un objetivo específico
Requiere configuración	Requiere configuración	Puede requerir configuración	Requiere configuración

Control de enrutamiento	Cambio de región	Cambio de zona	Cambio automático de zona
Requiere configuración y puesta en marcha	Requiere configuración y puesta en marcha	Es necesario suscribirse a algunos recursos compatibles Para obtener más información, consulte Recursos admitidos	Debe estar habilitado para un recurso compatible Para obtener más información, consulte Recursos admitidos
Iniciado por el cliente El cliente determina cuándo redirigir el tráfico	Iniciado por el cliente El cliente determina cuándo redirigir el tráfico	Iniciado por el cliente El cliente determina cuándo comenzar un cambio de zona	Iniciado por AWS AWS desvía el tráfico de aplicaciones de una zona de disponibilidad en su nombre
De pago Requiere cargos separados para el control de rutas	De pago Los planes de cambio de región requieren cargos separados	Incluido con los servicios (sin cargo adicional) Los recursos compatibles incluyen la creación de cambios zonales para AZs alejar el tráfico	Incluido con los servicios (sin cargo adicional) Entre los recursos compatibles, se incluye iniciar los turnos automáticos para AZs alejar el tráfico desde su nombre
No caduca El tráfico se puede redirigir a una réplica indefinidamente	No caduca La aplicación se puede cambiar a una réplica indefinidamente	Temporal Todos los cambios zonales deben estar configurados para que caduquen	Temporal AWS inicia y finaliza los cambios automáticos

Para obtener más información acerca de cada una de estas funciones, consulte los siguientes capítulos:

- Cambio zonal en ARC
- Cambio automático zonal en ARC
- Control de enrutamiento en ARC
- Conmutador de región en ARC

Utilice el cambio zonal y el cambio automático zonal para recuperar aplicaciones en ARC

En esta sección se explica cómo utilizar las capacidades de Amazon Application Recovery Controller (ARC) para recuperar de forma fiable el AWS recurso en caso de un problema en una zona de disponibilidad (AZ) afectada. El cambio zonal y el cambio automático zonal desplazan temporalmente el tráfico de un recurso compatible lejos de una zona de disponibilidad deteriorada, lo que reduce el tiempo de recuperación de las aplicaciones.

La principal diferencia entre el cambio zonal y el cambio automático zonal es que uno es un cambio de tráfico manual que usted controla y el otro desvía el tráfico de una zona de tráfico automáticamente en su nombre.

- Con el cambio zonal, se desplaza manualmente el tráfico hacia un recurso compatible dentro y Región de AWS fuera de una zona de disponibilidad.
- Con el cambio automático zonal, el tráfico de un recurso compatible se aleja automáticamente de una zona de disponibilidad deteriorada y se redirige a una zona en buen estado AZs en la misma región. AWS

En los siguientes temas se describen las capacidades de cambio zonal y cambio automático zonal y cómo utilizarlas.

Temas

- Cambio zonal en ARC
- Cambio automático zonal en ARC

Cambio zonal en ARC

El cambio zonal de Amazon Application Recovery Controller (ARC) le permite desviar el tráfico de un recurso compatible de una zona de disponibilidad (AZ) deteriorada Región de AWS a otro en buen estado AZs en la misma región. Al desviar el tráfico de sus recursos desde una zona de disponibilidad deteriorada, se reduce la duración y la gravedad del impacto provocado por los cortes de energía o los problemas de hardware o software en una zona de disponibilidad dañada, además de ayudar a mitigar los problemas y a recuperar rápidamente la aplicación. Puede optar por cambiar

el tráfico, por ejemplo, si una implementación incorrecta provoca problemas de latencia o porque la zona de disponibilidad está deteriorada.

Debe optar por utilizar los recursos para poder utilizar el cambio zonal. Para obtener más información, consulta Recursos admitidos.

Antes de iniciar un cambio zonal, debe preescalar la aplicación y asegurarse de que tiene la capacidad suficiente para desviar el tráfico de una zona de disponibilidad. Tras la preescalación, puede elegir la zona de disponibilidad de la que desea alejarse y el recurso hacia el que desviar el tráfico y, a continuación, iniciar el cambio zonal. Puede cancelar el turno en cualquier momento para que el tráfico comience a regresar a la zona de disponibilidad original. Para obtener más información, consulte Prácticas recomendadas para los cambios de zona en ARC

Todos los cambios zonales son mitigaciones temporales. Cuando empiezas un turno zonal, estableces una caducidad inicial, de un minuto a tres días (72 horas), que puedes prorrogar si necesitas continuar con el cambio de tráfico.

En escenarios específicos, el cambio zonal no desvía el tráfico de la AZ. Para obtener más información, consulte Recursos admitidos.

Cómo funciona un cambio de zona

Al iniciar un cambio zonal para un recurso compatible, el tráfico del recurso se aleja de la zona de disponibilidad (AZ) que especificó. Los recursos compatibles con ARC proporcionan integraciones que marcan la AZ especificada como insalubre, lo que provoca que el tráfico se desvíe de la AZ dañada.

El tráfico comienza a cambiar: al iniciar un cambio zonal en ARC, es posible que el tráfico no salga inmediatamente de la zona de disponibilidad. Las conexiones existentes y en curso en la zona de disponibilidad pueden tardar poco en completarse, según el comportamiento del cliente y la reutilización de la conexión. La configuración del DNS y otros factores, incluidas las conexiones existentes, pueden completarse en solo unos minutos, pero pueden tardar más. Para obtener más información, consulte Garantizar que los cambios de tráfico finalicen rápidamente.

Finaliza el turno de tráfico: cuando un turno zonal vence o se cancela, ARC toma medidas para detener los cambios de tráfico e invierte el proceso para iniciar un cambio de tráfico. Ahora, la AZ recuperada se reconoce como disponible para el recurso y el tráfico vuelve a fluir hacia la AZ.

Debe configurar todos los turnos zonales para que caduquen cuando comience los turnos. Inicialmente, puede configurar un turno zonal para que caduque en un máximo de tres días (72

horas). Sin embargo, puede actualizar un cambio de zona para establecer un nuevo vencimiento en cualquier momento. También puede cancelar un cambio de zona antes de que caduque, si está preparado para restablecer el tráfico en la zona de disponibilidad.

Cuando el tráfico no se desplaza: en escenarios específicos, un cambio zonal no desplaza el tráfico de la zona de disponibilidad. Por ejemplo, supongamos que inicias un cambio zonal para un balanceador de cargas cuando los grupos objetivo del balanceador de cargas AZs no tienen ninguna instancia o si todas las instancias están en mal estado. En este escenario, el balanceador de cargas se encuentra en un estado de apertura por error y, al iniciar un cambio zonal, no se desvía el tráfico.

Antes de iniciar un cambio zonal para un recurso, asegúrate de que se cumplen todas las condiciones para que el cambio zonal se realice correctamente. AWS los recursos gestionan los cambios zonales de forma diferente. Para obtener más información acerca de la asistencia con el cambio de zona, consulte Recursos admitidos.

Región de AWS disponibilidad para el cambio zonal

Para obtener información detallada sobre el soporte regional y los puntos de enlace de servicio para Amazon Application Recovery Controller (ARC), consulte los puntos de enlace y las cuotas de Amazon Application Recovery Controller (ARC) en la Referencia general de Amazon Web Services.

El cambio zonal y el cambio automático zonal están disponibles actualmente en la lista que aparece aquí. Regiones de AWS El cambio zonal y el cambio automático zonal también están disponibles en las regiones de China, es decir, en la región de China (Pekín) y en la región de China (Ningxia). Los recursos que utilizan Amazon Application Recovery Controller (ARC) pueden tener consideraciones adicionales. Para obtener más información, consulta Recursos admitidos.

Nombre de la región	Región	Punto de conexión	Protocolo	
Este de EE. UU. (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	
Este de EE. UU.	us-east-1	arc-zonal-shift.us-east-1.amazonaws.com	HTTPS	
		arc-zonal-shift-fips.us-east-1.api.aws	HTTPS	

Nombre de la región	Región	Punto de conexión	Protocolo
(Norte de Virginia)		arc-zonal-shift.us-east-1.api.aws	HTTPS
Oeste de EE. UU. (Norte de California)	us-west-1	arc-zonal-shift.us-west-1.amazonaws.com arc-zonal-shift-fips.us-west-1.api.aws arc-zonal-shift.us-west-1.api.aws	HTTPS HTTPS HTTPS
Oeste de EE. UU. (Oregón)	us-west-2	arc-zonal-shift.us-west-2.amazonaws.com arc-zonal-shift-fips.us-west-2.api.aws arc-zonal-shift.us-west-2.api.aws	HTTPS HTTPS HTTPS
África (Ciudad del Cabo)	af-south-1	arc-zonal-shift.af-south-1.amazonaws.com arc-zonal-shift.af-south-1.api.aws	HTTPS HTTPS
Asia-Pacífico (Hong Kong)	ap-east-1	arc-zonal-shift.ap-east-1.amazonaws.com arc-zonal-shift.ap-east-1.api.aws	HTTPS HTTPS
Asia-Pacífico (Hyderabad)	ap-south-2	arc-zonal-shift.ap-south-2.amazonaws.com arc-zonal-shift.ap-south-2.api.aws	HTTPS HTTPS
Asia-Pacífico (Yakarta)	ap-southeast-3	arc-zonal-shift.ap-southeast-3.amazonaws.com arc-zonal-shift.ap-southeast-3.api.aws	HTTPS HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
Asia-Pacífico (Malasia)	ap-southeast-5	arc-zonal-shift.ap-southeast-5.amazonaws.com arc-zonal-shift.ap-southeast-5.api.aws	HTTPS HTTPS
Asia-Pacífico (Melbourne)	ap-southeast-4	arc-zonal-shift.ap-southeast-4.amazonaws.com arc-zonal-shift.ap-southeast-4.api.aws	HTTPS HTTPS
Asia-Pacífico (Bombay)	ap-south-1	arc-zonal-shift.ap-south-1.amazonaws.com arc-zonal-shift.ap-south-1.api.aws	HTTPS HTTPS
Asia-Pacífico (Osaka)	ap-northeast-3	arc-zonal-shift.ap-northeast-3.amazonaws.com arc-zonal-shift.ap-northeast-3.api.aws	HTTPS HTTPS
Asia-Pacífico (Seúl)	ap-northeast-2	arc-zonal-shift.ap-northeast-2.amazonaws.com arc-zonal-shift.ap-northeast-2.api.aws	HTTPS HTTPS
Asia-Pacífico (Singapur)	ap-southeast-1	arc-zonal-shift.ap-southeast-1.amazonaws.com arc-zonal-shift.ap-southeast-1.api.aws	HTTPS HTTPS
Asia-Pacífico (Sídney)	ap-southeast-2	arc-zonal-shift.ap-southeast-2.amazonaws.com arc-zonal-shift.ap-southeast-2.api.aws	HTTPS HTTPS
Asia-Pacífico (Taipéi)	ap-east-2	arc-zonal-shift.ap-east-2.amazonaws.com arc-zonal-shift.ap-east-2.api.aws	HTTPS HTTPS

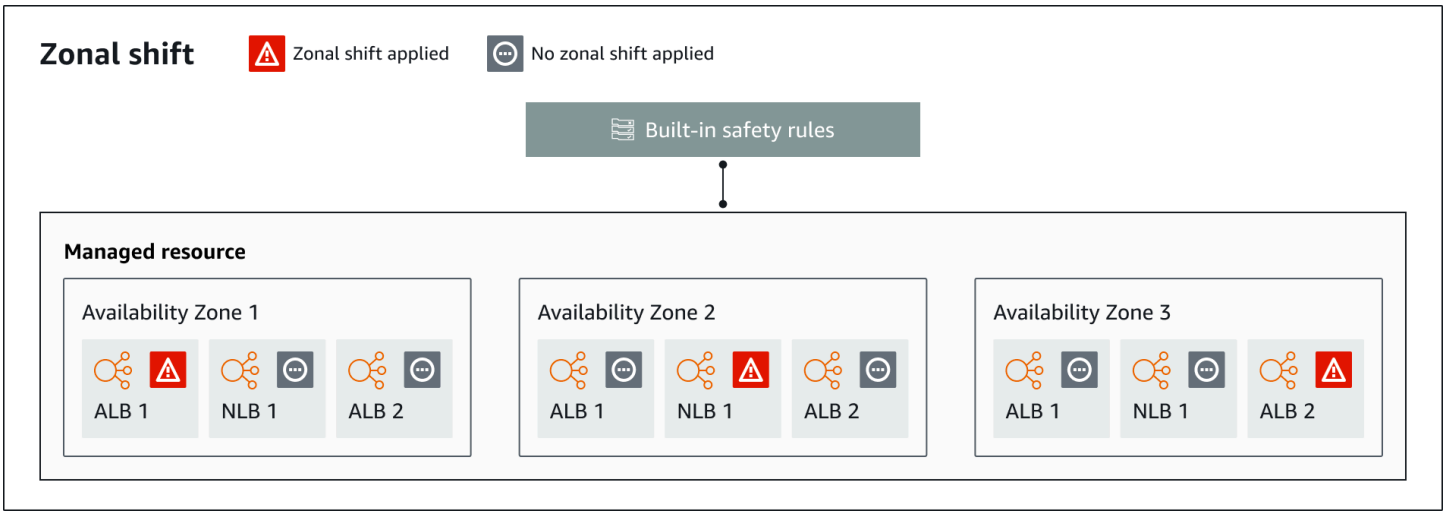
Nombre de la región	Región	Punto de conexión	Protocolo
Asia-Pacífico (Tailandia)	ap-southeast-7	arc-zonal-shift.ap-southeast-7.amazonaws.com	HTTPS
		arc-zonal-shift.ap-southeast-7.api.aws	HTTPS
Asia-Pacífico (Tokio)	ap-northeast-1	arc-zonal-shift.ap-northeast-1.amazonaws.com	HTTPS
		arc-zonal-shift.ap-northeast-1.api.aws	HTTPS
Canadá (centro)	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
Oeste de Canadá (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 (Fráncfort)	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
Europa (Londres)	eu-west-2	arc-zonal-shift.eu-west-2.amazonaws.com	HTTPS
		arc-zonal-shift.eu-west-2.api.aws	HTTPS
Europa (Milán)	eu-south-1	arc-zonal-shift.eu-south-1.amazonaws.com	HTTPS
		arc-zonal-shift.eu-south-1.api.aws	HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
Europa (París)	eu-west-3	arc-zonal-shift.eu-west-3.amazonaws.com arc-zonal-shift.eu-west-3.api.aws	HTTPS HTTPS
Europa (España)	eu-south-2	arc-zonal-shift.eu-south-2.amazonaws.com arc-zonal-shift.eu-south-2.api.aws	HTTPS HTTPS
Europa (Estocolmo)	eu-north-1	arc-zonal-shift.eu-north-1.amazonaws.com arc-zonal-shift.eu-north-1.api.aws	HTTPS HTTPS
Europa (Zúrich)	eu-central-2	arc-zonal-shift.eu-central-2.amazonaws.com arc-zonal-shift.eu-central-2.api.aws	HTTPS HTTPS
Israel (Tel Aviv)	il-central-1	arc-zonal-shift.il-central-1.amazonaws.com arc-zonal-shift.il-central-1.api.aws	HTTPS HTTPS
México (central)	mx-central-1	arc-zonal-shift.mx-central-1.amazonaws.com arc-zonal-shift.mx-central-1.api.aws	HTTPS HTTPS
Medio Oriente (Baréin)	me-south-1	arc-zonal-shift.me-south-1.amazonaws.com arc-zonal-shift.me-south-1.api.aws	HTTPS HTTPS
Medio Oriente (EAU)	me-central-1	arc-zonal-shift.me-central-1.amazonaws.com arc-zonal-shift.me-central-1.api.aws	HTTPS HTTPS
América del Sur (São Paulo)	sa-east-1	arc-zonal-shift.sa-east-1.amazonaws.com arc-zonal-shift.sa-east-1.api.aws	HTTPS HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
AWS GovCloud (Este de EE. UU.)	us-gov-east-1	arc-zonal-shift.us-gov-east-1.amazonaws.com	HTTPS
		arc-zonal-shift-fips.us-gov-east-1.api.aws	HTTPS
		arc-zonal-shift.us-gov-east-1.api.aws	HTTPS
AWS GovCloud (Estados Unidos-Oeste)	us-gov-west-1	arc-zonal-shift.us-gov-west-1.amazonaws.com	HTTPS
		arc-zonal-shift-fips.us-gov-west-1.api.aws	HTTPS
		arc-zonal-shift.us-gov-west-1.api.aws	HTTPS

Componentes de cambio de zona

El siguiente diagrama ilustra un ejemplo de un cambio zonal que desvía el tráfico de una zona de disponibilidad en un. Región de AWS Las comprobaciones integradas en el cambio zonal impiden iniciar otro cambio zonal para un recurso cuando ya tiene un turno activo.



Los siguientes son componentes de la capacidad de cambio zonal de ARC.

Cambio de zona

Usted inicia un cambio zonal para un recurso administrado en su AWS cuenta con el fin de alejar temporalmente el tráfico de una zona de disponibilidad en una zona de disponibilidad y colocarlo Región de AWS en buen estado AZs en la región, a fin de recuperarse rápidamente de un problema en una zona de disponibilidad. Para obtener más información sobre los recursos compatibles para el cambio zonal, consulta. Recursos admitidos

Controles de seguridad integrados

Las comprobaciones integradas en el ARC evitan que se produzca más de un cambio de tráfico para un recurso a la vez. Es decir, solo un cambio zonal, una sesión de práctica o un cambio automático para el recurso iniciados por el cliente pueden desviar activamente el tráfico de una zona de disponibilidad. Por ejemplo, si inicia un cambio de zona para un recurso cuando se ha desviado en ese momento con el cambio automático, el cambio de zona tendrá prioridad. Para obtener más información, consulte Cambio automático zonal en ARC y Resultados de las ejecuciones de práctica.

Identificador de recursos

El identificador de un recurso que se va a incluir en un cambio zonal. El identificador de recurso es un nombre de recurso de Amazon (ARN).

En el caso de un cambio zonal, solo puede elegir los recursos de su cuenta para un AWS servicio compatible con ARC. Para obtener más información sobre los recursos compatibles para el cambio zonal, consulte. Recursos admitidos

Administrar recursos

Algunos AWS recursos deben activar manualmente el cambio zonal y otros se habilitan automáticamente. Para obtener más información sobre los recursos compatibles para el cambio zonal, consulte. Recursos admitidos

Nombre del recurso

El nombre de un recurso en ARC que puede especificar para un cambio zonal.

Estado (estado de cambio zonal)

Estado de un cambio zonal. `Status`Para un cambio de zona, puede tener uno de los siguientes valores:

- ACTIVO: El cambio zonal se inicia y se activa.
- CADUCADO: el cambio zonal ha caducado (se ha superado el tiempo de caducidad).

- CANCELADO: Se canceló el cambio zonal.

Estado aplicado

Un estado aplicado indica si hay un cambio en vigor para un recurso. El turno que tiene el estado `APPLIED` determina la zona de disponibilidad en la que se ha desviado el tráfico de aplicaciones para un recurso y cuándo finaliza ese turno.

Tipo de turno

Define el tipo de cambio zonal. `shiftType`Puede tener los siguientes valores:

- ZONAL_SHIFT
- ZONAL_AUTOSHIFT
- PRACTICE_RUN
- FIS_EXPERIMENT

Hora de caducidad (hora de caducidad)

El tiempo de caducidad (tiempo de vencimiento) de un cambio de zona. Todos los cambios de zona son temporales. En el caso de un cambio zonal, puede configurar inicialmente un cambio zonal para que esté activo durante un máximo de tres días (72 horas).

Al iniciar un cambio zonal, debe especificar cuánto tiempo desea que esté activo, que ARC convierte en un tiempo de caducidad (tiempo de caducidad). También puede cancelar un cambio de zona antes de que caduque, si está preparado para restablecer el tráfico en la zona de disponibilidad. O bien, puede ampliar un cambio de zona iniciado por el cliente actualizándolo para especificar otro periodo de tiempo en el que vence.

Puede cancelar las tandas de práctica de cambios zonales que forman parte del cambio automático zonal.

Planos de datos y control para el cambio zonal

Al planificar la conmutación por error y la recuperación ante desastres, tenga en cuenta la resistencia de sus mecanismos de conmutación por error. Le recomendamos que se asegure de que los mecanismos de los que depende durante la conmutación por error estén altamente disponibles, de modo que pueda utilizarlos cuando los necesite en caso de desastre. Por lo general, debería utilizar funciones de plano de datos para sus mecanismos siempre que pueda, a fin de obtener la máxima fiabilidad y tolerancia a los fallos. Teniendo esto en cuenta, es importante entender cómo se divide la

funcionalidad de un servicio entre planos de control y planos de datos, y cuándo se puede confiar en una fiabilidad extrema con el plano de datos de un servicio.

Como ocurre con la mayoría de los AWS servicios, los planos de control y los planos de datos admiten la funcionalidad de la capacidad de cambio zonal. Si bien ambos están diseñados para ser fiables, un plano de control está optimizado para garantizar la coherencia de los datos, mientras que un plano de datos está optimizado para garantizar la disponibilidad. Un plano de datos está diseñado para ser resistente, de modo que puede mantener la disponibilidad incluso durante eventos disruptivos, cuando un plano de control podría no estar disponible.

En general, un plano de control permite realizar funciones de administración básicas, como crear, actualizar y eliminar recursos del servicio. Un plano de datos proporciona la funcionalidad principal de un servicio.

Para obtener más información sobre los planos de datos, los planos de control y cómo AWS se crean servicios para cumplir los objetivos de alta disponibilidad, consulte el artículo Static stability using Availability Zones en Amazon Builders' Library.

Los precios del cambio zonal en ARC

Para el cambio zonal, puede iniciar un cambio zonal para los recursos compatibles, a fin de recuperar su aplicación en caso de un problema en una zona de disponibilidad. El uso de la no supone ningún cargo adicional.

Para obtener información detallada sobre los precios de ARC y ejemplos de precios, consulta los precios de ARC.

Prácticas recomendadas para los cambios de zona en ARC

Recomendamos las siguientes prácticas recomendadas para utilizar los cambios zonales para la recuperación en zonas de disponibilidad múltiples (Multi-AZ) en ARC.

Temas

- Planificación de la capacidad y escalado previo
- Limite el tiempo que los clientes permanecen conectados a sus terminales
- Pruebe con antelación los turnos zonales iniciales
- Asegúrese de que todas las zonas de disponibilidad estén en buen estado y reciban tráfico
- Utilice las operaciones de la API del plano de datos para la recuperación ante desastres

- Mueva el tráfico con un cambio zonal solo temporalmente

Planificación y preescalamiento de la capacidad

Asegúrese de haber planificado y escalado previamente, o de escalar automáticamente, la capacidad suficiente para adaptarse a la carga adicional que se impone en las zonas de disponibilidad al iniciar un cambio de zona. Con una arquitectura orientada a la recuperación, una recomendación habitual es escalar previamente la capacidad de cómputo con el fin de incluir suficiente margen para atender los picos de tráfico cuando una de las (normalmente) tres réplicas esté fuera desconectada.

Cuando se inicia un cambio zonal para un recurso compatible y el tráfico se aleja de una zona de disponibilidad, se elimina la capacidad que la aplicación utilizaba para atender las solicitudes. Debe asegurarse de haber planificado un traslado del tráfico fuera de una zona de disponibilidad y de poder seguir atendiendo las solicitudes en las zonas restantes AZs.

Limite el tiempo que los clientes permanecen conectados a sus terminales

Cuando Amazon Application Recovery Controller (ARC) desvía el tráfico de una zona afectada, por ejemplo, mediante el cambio zonal o el cambio automático zonal, el mecanismo que utiliza ARC para mover el tráfico de las aplicaciones es una actualización del DNS. Una actualización del DNS provoca que todas las conexiones nuevas se dirijan lejos de la ubicación dañada.

Sin embargo, los clientes con conexiones abiertas preexistentes pueden seguir realizando solicitudes a la ubicación dañada hasta que los clientes se vuelvan a conectar. Para garantizar una recuperación rápida, le recomendamos que limite el tiempo que los clientes permanecen conectados a sus terminales.

Pruebe los turnos zonales iniciales con antelación

Inicie cambios de zona para probar periódicamente a desviar el tráfico de las zonas de disponibilidad para la aplicación. Planifique y ejecute el inicio de cambios de zona, preferiblemente tanto en entornos de prueba como de producción, como parte de las pruebas de conmutación por error periódicas para recuperar las aplicaciones en caso de un desastre. Las pruebas periódicas son fundamentales para garantizar que está preparado y tiene la confianza necesaria para mitigar los problemas cuando se produce un incidente operativo.

Asegúrese de que todas las zonas de disponibilidad estén en buen estado y reciban tráfico

Los cambios de zona funcionan marcando un recurso, es decir, una réplica de una aplicación, como incorrecto en una zona de disponibilidad. Esto significa que es fundamental garantizar que

los recursos de las aplicaciones estén en buen estado y que absorban activamente el tráfico en las zonas de disponibilidad de una región. Le recomendamos que tenga paneles para realizar un seguimiento de esto, que incluyan, por ejemplo, las métricas de Elastic Load Balancing para los destinos incorrectos y los bytes procesados por zona de disponibilidad.

Considere la posibilidad de supervisar el estado de sus recursos desde una segunda región adyacente. Las ventajas de este enfoque son que puede ser más representativo de la experiencia de los usuarios finales y, además, reduce el riesgo de que tanto la aplicación como la supervisión se vean afectadas por el mismo desastre al mismo tiempo.

Utilice las operaciones de la API del plano de datos para la recuperación ante desastres

Para iniciar un cambio zonal cuando necesite recuperar una aplicación rápidamente y con pocas dependencias, le recomendamos que utilice la API AWS Command Line Interface o la API con acciones de cambio zonal y, de ser posible, con credenciales almacenadas previamente. También puede iniciar cambios zonales en el AWS Management Console, para facilitar su uso. Sin embargo, cuando la recuperación rápida y fiable es fundamental, las operaciones del plano de datos son una mejor opción. Para obtener más información, consulte la Guía de referencia de la API de cambio de zona.

Mueva el tráfico con un cambio zonal solo temporalmente

Un cambio de zona desvía el tráfico de una zona de disponibilidad de forma temporal para mitigar una alteración. Debe restaurar el servicio del recurso de la aplicación en cuanto haya tomado medidas para corregir un problema. Esto garantiza que toda la aplicación se restaure a su estado original, totalmente redundante y resiliente.

Operaciones de la API de cambio de zona

En la siguiente tabla se enumeran las operaciones de la API ARC que puede utilizar mediante el cambio zonal, que aleja el tráfico de una zona de disponibilidad para las aplicaciones Multi-AZ. En la tabla también se incluyen enlaces a la documentación pertinente.

Para ver ejemplos de cómo utilizar las operaciones habituales de la API de cambio de zona con la AWS Command Line Interface, consulte Ejemplos de uso de la función AWS CLI con cambio zonal.

Acción	Uso de la consola ARC	Uso de la API ARC
Comenzar un cambio de zona	Consulte Comenzar un cambio de zona	Consulte StartZonalShift.

Acción	Uso de la consola ARC	Uso de la API ARC
Actualizar un cambio de zona	Consulte Actualizar o cancelar un cambio zonal	Consulte UpdateZonalShift.
Enumere los cambios zonales	Consulte Cambio zonal en ARC	Consulte ListZonalShifts.
Descripción de recursos administrados	Consulte Recursos admitidos	Consulte ListManagedResources.
Obtenga un recurso gestionado	Consulte Recursos admitidos	Consulte GetManagedResource.
Cancelar un cambio de zona	Consulte Actualizar o cancelar un cambio zonal	Consulte CancelZonalShift.

Ejemplos de uso de la función AWS CLI con cambio zonal

En esta sección, se proporcionan ejemplos de aplicaciones sobre el uso del cambio zonal AWS Command Line Interface para trabajar con la capacidad de cambio zonal en Amazon Application Recovery Controller (ARC) mediante operaciones de API. Los ejemplos tienen como objetivo ayudarlo a desarrollar una comprensión básica de cómo trabajar con el cambio zonal mediante la CLI.

El cambio zonal en ARC le permite mover temporalmente el tráfico de los recursos compatibles fuera de una zona de disponibilidad para que su aplicación pueda seguir funcionando con normalidad con otras zonas de disponibilidad de una. Región de AWS

Todos los cambios de zona son temporales y deben configurarse inicialmente para que caduquen en un plazo de tres días. Sin embargo, puede actualizar un cambio de zona para establecer un nuevo vencimiento.

Para obtener más información sobre el uso de AWS CLI, consulte la Referencia de comandos.AWS CLI Para obtener una lista de las acciones de la API de cambio de zona y enlaces a más información, consulte Operaciones de la API de cambio de zona.

Iniciar un cambio de zona

Puede iniciar un cambio de zona con la CLI mediante el comando `start-zonal-shift`.

```
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"
}
```

Obtenga un recurso gestionado

Puede obtener información sobre un recurso administrado con la CLI mediante el comando `get-managed-resource`.

```
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"
        }
    ]
}
```

Descripción de recursos administrados

Puede enumerar los recursos administrados de su cuenta con la CLI mediante el comando `list-managed-resources`.

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

Enumere los cambios zonales

Puede enumerar los cambios de zona de su cuenta con la CLI mediante el 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"
        }
    ]
}
```

Actualizar un cambio de zona

Puede actualizar un cambio de zona con la CLI mediante el comando `update-zonal-shift`.

```
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"
}
```

Cancelar un cambio de zona

Puede actualizar un cambio de zona con la CLI mediante el comando `cancel-zonal-shift`.

```
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"
}
```

Recursos admitidos

Amazon Application Recovery Controller (ARC) actualmente admite la activación de los siguientes recursos para el cambio zonal y el cambio automático zonal:

- Grupos de Amazon EC2 Auto Scaling

- Amazon Elastic Kubernetes Service
- Equilibrador de carga de aplicacióncon el balanceo de carga entre zonas activado o desactivado
- Equilibrador de carga de redcon el equilibrio de carga entre zonas activado o desactivado

Para conocer los requisitos específicos de los balanceadores de carga de red y los balanceadores de carga de aplicaciones, consulte los temas adicionales de esta sección.

Revise las siguientes condiciones para trabajar con cambios zonales, cambios automáticos zonales y recursos en ARC:

- Un recurso debe estar activo y aprovisionado por completo para desplazar el tráfico hacia él. Antes de iniciar un cambio zonal para un recurso, asegúrate de que se trata de un recurso gestionado en ARC. Por ejemplo, consulte la lista de recursos administrados o utilice la `get-managed-resource` operación con el identificador del recurso. AWS Management Console
- Para iniciar un cambio zonal con un recurso, debe implementarse en la zona de disponibilidad y en el Región de AWS lugar en el que comience el turno. Asegúrese de iniciar un cambio zonal en la misma región en la que se encuentra la zona de destino de la que desea alejarse y de que el recurso al que va a transferir el tráfico también esté en la misma zona y región.
- Asegúrese de tener los permisos de IAM correctos para utilizar el cambio zonal con un recurso. Para obtener más información, consulte IAM y permisos para el cambio de zona.
- Cuando un Network Load Balancer o Application Load Balancer se encuentra en estado abierto por error, el cambio zonal no tendrá efecto. Este es el comportamiento esperado, ya que el cambio zonal no puede forzar a una zona de disponibilidad a estar AZs en mal estado y, a continuación, transferir el tráfico a otra zona de una región cuando el balanceador de cargas no se abre correctamente. Para obtener más información, consulte Uso de la conmutación por error de DNS de Route 53 para su balanceador de carga en la Guía del usuario de balanceadores de carga de red y Uso de la conmutación por error de DNS de Route 53 para su balanceador de carga en la Guía del usuario de balanceadores de carga de aplicaciones.
- Si varios balanceadores de carga reenvían el tráfico a los mismos destinos, un cambio zonal en un balanceador de carga compatible con zonas cruzadas reducirá la capacidad objetivo de todos los balanceadores de carga, incluso si no están desplazados de zona.

Grupos de Amazon EC2 Auto Scaling

Un grupo de Amazon EC2 Auto Scaling contiene una colección de EC2 instancias de Amazon que se tratan como una agrupación lógica con fines de escalado y administración automáticos. Un grupo

de Auto Scaling también le permite utilizar las funciones de Amazon EC2 Auto Scaling, como las sustituciones de chequeos de estado y las políticas de escalado. Tanto el mantenimiento del número de instancias en un grupo de Auto Scaling como el escalado automático son las funciones principales del servicio Amazon EC2 Auto Scaling.

Uso del cambio zonal para los grupos de Auto Scaling

Para habilitar el cambio zonal, utilice uno de los siguientes métodos.

Console

Para habilitar el cambio zonal en un grupo nuevo (consola)

1. Siga las instrucciones de Crear un grupo de Auto Scaling mediante una plantilla de lanzamiento y complete cada paso del procedimiento, hasta el paso 10.
2. En la página Integrar con otros servicios, para el cambio zonal ARC, seleccione la casilla de verificación para habilitar el cambio zonal.
3. Para Comportamiento de Health Check, selecciona Ignorar lo que no es saludable o Reemplazar lo que no es saludable. Si se establece en `replace-unhealthy` esta opción, las instancias en mal estado se sustituirán en la zona de disponibilidad por el cambio zonal activo. Si se establece en esta `ignore-unhealthy` opción, las instancias en mal estado no se sustituirán en la zona de disponibilidad por el cambio zonal activo.
4. Continúe con los pasos de Crear un grupo de Auto Scaling mediante una plantilla de lanzamiento.

AWS CLI

Para habilitar el cambio zonal en un grupo nuevo ()AWS CLI

Agregue el parámetro `--availability-zone-impairment-policy` al comando create-auto-scaling-group.

El `--availability-zone-impairment-policy` parámetro tiene dos opciones:

- ZonalShiftEnabled— Si se establece en`true`, Auto Scaling registra el grupo de Auto Scaling con cambio zonal ARC y usted puede iniciar, actualizar o cancelar un cambio zonal en la consola ARC. Si se establece en`false`, Auto Scaling anula el registro del grupo Auto Scaling del cambio zonal de ARC. Debe tener ya activado el cambio zonal para configurarlo. `false`

- ImpairedZoneHealthCheckBehavior— Si se establece en esta `replace-unhealthy` opción, las instancias en mal estado se sustituirán en la zona de disponibilidad por el cambio zonal activo. Si se establece en esta `ignore-unhealthy` opción, las instancias en mal estado no se reemplazarán en la zona de disponibilidad con el cambio zonal activo.

El siguiente ejemplo habilita el cambio zonal en un nuevo grupo de Auto Scaling denominado*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

Para habilitar el cambio zonal en un grupo existente (consola)

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/y selecciona Auto Scaling Groups en el panel de navegación.
2. En la barra de navegación de la parte superior de la pantalla, elija la misma Región de AWS que utilizó cuando creó el grupo de escalado automático.
3. Seleccione la casilla situada junto al grupo de escalado automático.

   Se abre un panel dividido en la parte inferior de la página.
4. En la pestaña Integraciones, en la sección Cambio zonal de ARC, selecciona Editar.
5. Seleccione la casilla de verificación para activar el cambio zonal.
6. Para Comportamiento de Health Check, selecciona Ignorar lo que no es saludable o Reemplazar lo que no es saludable. Si se establece en `replace-unhealthy` esta opción, las instancias en mal estado se sustituirán en la zona de disponibilidad por el cambio zonal

activo. Si se establece en esta `ignore-unhealthy` opción, las instancias en mal estado no se sustituirán en la zona de disponibilidad por el cambio zonal activo.

7. Elija Actualizar.

AWS CLI

Para habilitar el cambio zonal en un grupo existente ()AWS CLI

Agregue el parámetro `--availability-zone-impairment-policy` al comando update-auto-scaling-group.

El `--availability-zone-impairment-policy` parámetro tiene dos opciones:

- ZonalShiftEnabled— Si se establece en`true`, Auto Scaling registra el grupo de Auto Scaling con cambio zonal ARC y usted puede iniciar, actualizar o cancelar un cambio zonal en la consola ARC. Si se establece en`false`, Auto Scaling anula el registro del grupo Auto Scaling del cambio zonal de ARC. Debe tener ya activado el cambio zonal para configurarlo. `false`
- ImpairedZoneHealthCheckBehavior— Si se establece en esta `replace-unhealthy` opción, las instancias en mal estado se sustituirán en la zona de disponibilidad por el cambio zonal activo. Si se establece en esta `ignore-unhealthy` opción, las instancias en mal estado no se reemplazarán en la zona de disponibilidad con el cambio zonal activo.

El siguiente ejemplo habilita el cambio zonal en el grupo de Auto Scaling especificado.

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

Para activar un cambio zonal, consulte. Iniciar, actualizar o cancelar un cambio zonal

Cómo funciona el cambio zonal para los grupos de Auto Scaling

Suponga que tiene un grupo de Auto Scaling con las siguientes zonas de disponibilidad:

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

- us-east-1c

Observa errores us-east-1a y desencadena un cambio zonal. Los siguientes comportamientos se producen cuando se desencadena un cambio zonal. us-east-1a

- Ampliación: Auto Scaling lanzará todas las nuevas solicitudes de capacidad en las zonas de disponibilidad en buen estado (us-east-1byus-east-1c).
- Escalado dinámico: Auto Scaling impedirá que las políticas de escalado reduzcan la capacidad deseada. Auto Scaling no impedirá que las políticas de escalado aumenten la capacidad deseada.
- Actualización de instancias: Auto Scaling prolongará el tiempo de espera de cualquier proceso de actualización de instancias que se retrase durante un cambio zonal activo.

Deterioro de la selección del comportamiento de la zona de disponibilidad	Comportamiento de Health Check
Reemplace lo poco saludable	Las instancias que parezcan estar en mal estado se reemplazarán en todas las zonas de disponibilidad (us-east-1a us-east-1b , yus-east-1c).
Ignore el estado	Los casos que parezcan insalubres se sustituir án por us-east-1b yus-east-1c . Las instancias de la zona de disponibilidad no se reemplazarán con el cambio zonal activo (us-east-1a).

Mejores prácticas para usar el cambio zonal

Para mantener una alta disponibilidad de sus aplicaciones al utilizar el cambio zonal, le recomendamos las siguientes prácticas recomendadas.

- Supervise EventBridge las notificaciones para determinar si se está produciendo un deterioro continuo de la zona de disponibilidad. Para obtener más información, consulte Automatización de Amazon EC2 Auto Scaling con Event Bridge.
- Utilice políticas de escalado con los umbrales adecuados para asegurarse de que tiene la capacidad suficiente para tolerar la pérdida de una zona de disponibilidad.

- Establezca una política de mantenimiento de instancias con un porcentaje mínimo de mantenimiento de 100. Con esta configuración, Auto Scaling espera a que una nueva instancia esté lista para usarse antes de cerrar una instancia en mal estado.

Para los clientes preescalados, también recomendamos lo siguiente:

- Selecciona Ignorar el estado incorrecto como comportamiento de comprobación de estado para la zona de disponibilidad alterada, ya que no es necesario sustituir la instancia en mal estado durante el caso de deterioro.
- Utilice el cambio automático zonal en ARC para sus grupos de Auto Scaling. La función de cambio automático zonal Controlador de recuperación de aplicaciones (ARC) de Amazon permite AWS desviar el tráfico de un recurso fuera de una zona de disponibilidad cuando se AWS detecta un deterioro en una zona de disponibilidad. Para obtener más información, consulte Cambio automático zonal en ARC en la Guía para desarrolladores de Amazon Application Recovery Controller (ARC).

Para los clientes con balanceadores de carga entre zonas desactivados, también recomendamos:

- Usa el balanceado solo para la distribución de tu zona de disponibilidad.
- Si está utilizando el cambio zonal tanto en su grupo de Auto Scaling como en sus balanceadores de carga, asegúrese de cancelar primero el cambio zonal en su grupo de Auto Scaling. A continuación, espere hasta que la capacidad esté equilibrada en todas las zonas de disponibilidad antes de cancelar el cambio zonal en el equilibrador de carga.
- Debido a la posibilidad de que la capacidad se desequilibre cuando se habilita el cambio zonal y se utiliza un balanceador de carga desactivado entre zonas, Auto Scaling tiene una validación adicional. Si sigue las prácticas recomendadas, puede reconocer esta posibilidad `skip-zonal-shift-validation` marcando la casilla de verificación de la casilla de verificación o marcando la casilla correspondiente a, AWS Management Console o. `CreateAutoScalingGroup` `UpdateAutoScalingGroup` `AttachTrafficSources`

Amazon Elastic Kubernetes Service

Amazon EKS ofrece características que le permiten hacer que sus aplicaciones sean más resistentes a eventos como el deterioro del estado o el deterioro de una zona de disponibilidad (AZ). Al ejecutar sus cargas de trabajo en un clúster de Amazon EKS, puede mejorar aún más la tolerancia a errores

y la recuperación de las aplicaciones del entorno de aplicaciones mediante el cambio zonal o el cambio automático zonal.

Uso del cambio zonal para Amazon Elastic Kubernetes Service

Para habilitar el cambio zonal, utilice uno de los siguientes métodos. Para obtener más información, consulte Habilitar el cambio zonal de Amazon EKS para evitar que las zonas de disponibilidad se vean afectadas.

Console

Para habilitar el cambio zonal en un nuevo clúster de Amazon EKS (consola)

1. Busque el nombre y la región del clúster Amazon EKS que desea registrar en ARC.
2. Abra la consola Amazon EKS en https://console.aws.amazon.com/eks/home#/clusters.
3. Seleccione el clúster.
4. Seleccione la pestaña Información general en la página Información del clúster.
5. En el encabezado Cambio de zona, seleccione el botón Administrar.
6. Seleccione activar o desactivar para EKS Zonal Shift.

AWS CLI

Para habilitar el cambio zonal en un nuevo clúster de Amazon EKS ()AWS CLI

- Escriba el siguiente comando:

```
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
```

Para habilitar el cambio zonal en un clúster de Amazon EKS existente ()AWS CLI

- Escriba el siguiente comando:

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

Puede activar un cambio zonal para un clúster de Amazon EKS o puede AWS permitir que lo haga por usted activando el cambio automático zonal. Una vez que el cambio zonal del clúster de Amazon EKS esté habilitado con ARC, puede activar un cambio zonal o habilitar el cambio automático zonal mediante la consola ARC, la AWS CLI o el cambio zonal y el cambio automático zonal. APIs

Para obtener más información sobre cómo activar un cambio zonal, consulte. Iniciar, actualizar o cancelar un cambio zonal

Para obtener más información sobre cómo habilitar Amazon EKS con el cambio zonal, consulte el tema Más información sobre el cambio zonal de ARC en Amazon EKS de la Guía del usuario de Amazon Elastic Kubernetes Service.

Cómo funciona el cambio zonal para Amazon Elastic Kubernetes Service

Durante un cambio zonal de Amazon EKS, ocurrirá automáticamente lo siguiente:

- Se acordonarán todos los nodos de la AZ afectada. Esto evitará que el programador de Kubernetes programe nuevos pods en los nodos de la AZ en mal estado.
- Si utiliza grupos de nodos gestionados, se suspenderá el reequilibrio de la zona de disponibilidad y se actualizará su Grupo de Auto Scaling (ASG) para garantizar que los nuevos nodos de Amazon EKS Data Plane solo se lancen en buen estado. AZs
- Los nodos de la AZ en mal estado no se cerrarán y los pods no se desalojarán de estos nodos. De este modo, se garantiza que, cuando un cambio zonal caduque o se cancele, el tráfico pueda devolverse de forma segura a la zona de disponibilidad, que aún tiene plena capacidad.
- El EndpointSlice controlador localizará todos los puntos terminales del Pod en la zona de distribución defectuosa y los eliminará de la zona correspondiente. EndpointSlices Esto garantizará que solo los puntos finales del Pod que estén en buen estado AZs estén destinados a recibir tráfico de red. Cuando se cancela o caduca un cambio zonal, el EndpointSlice controlador lo actualizará EndpointSlices para incluir los puntos finales en la zona de disponibilidad restaurada.

Para obtener más información, consulta el blog de AWS Containers.

Equilibrador de carga de aplicación

Uso del cambio zonal para los balanceadores de carga de aplicaciones

Para usar Application Load Balancers con desplazamiento zonal, debe habilitar la integración de desplazamiento zonal ARC en los atributos del Application Load Balancer. Application Load Balancer admite el cambio zonal con configuraciones entre zonas habilitadas o inhabilitadas entre zonas.

Antes de habilitar la integración ARC y empezar a utilizar el cambio zonal, revise lo siguiente:

- Puede comenzar un cambio de zona para un equilibrador de carga específico solo para una zona de disponibilidad única. No puede comenzar un cambio de zona para varias zonas de disponibilidad.
- AWS elimina de forma proactiva las direcciones IP del balanceador de carga zonal del DNS cuando varios problemas de infraestructura afectan a los servicios. Compruebe siempre la capacidad actual de la zona de disponibilidad antes de comenzar un cambio de zona.
- Cuando un Equilibrador de carga de aplicación sea el destino de un Equilibrador de carga de red, comience siempre el cambio de zona desde el Equilibrador de carga de red. Si comienza un cambio de zona desde el Equilibrador de carga de aplicación, el Equilibrador de carga de red no reconoce el cambio y continúa enviando tráfico al Equilibrador de carga de aplicación.

Puedes iniciar un cambio zonal para un balanceador de carga en la consola Elastic Load Balancing (en la mayoría de los casos Regiones de AWS) o en la consola ARC.

Console

Para habilitar el cambio zonal en un balanceador de carga (consola)

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En la página de navegación, en Equilibrio de carga, selecciona Load Balancers.
3. Seleccione el nombre de Application Load Balancer.
4. En la pestaña Atributos, seleccione Editar.
5. En Configuración de enrutamiento de la zona de disponibilidad, establezca Integración de cambios de zona ARC como Habilitar.
6. Seleccione Save.

AWS CLI

Para habilitar el cambio zonal en un balanceador de carga ()AWS CLI

- Escriba el siguiente comando:

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

Para obtener más información sobre cómo activar un cambio zonal, consulte. Iniciar, actualizar o cancelar un cambio zonal

Puede usar la `keepalive` opción para configurar cuánto tiempo duran las conexiones. Para obtener más información, consulte la duración de keepalive del cliente HTTP en la Guía del usuario de Application Load Balancer. De forma predeterminada, los balanceadores de carga de aplicaciones establecen el valor de duración de keepalive del cliente HTTP en 3600 segundos o 1 hora. Le sugerimos que reduzca el valor para ajustarlo al objetivo de tiempo de recuperación de su aplicación, por ejemplo, 300 segundos. Cuando elija el tiempo de permanencia activo de un cliente HTTP, tenga en cuenta que este valor es una compensación entre volver a conectarse con más frecuencia, en general, lo que puede afectar a la latencia, y alejar más rápidamente a todos los clientes de una zona de disponibilidad o región con problemas.

Cómo funciona el cambio zonal para los balanceadores de carga de aplicaciones

Cuando se inicia un cambio zonal en un Application Load Balancer con el equilibrio de carga entre zonas activado, todo el tráfico dirigido a los destinos se bloquea en la zona de disponibilidad afectada y se elimina la dirección IP zonal del DNS.

Para obtener más información, consulte Integraciones para su balanceador de carga de aplicaciones en la Guía del usuario de Application Load Balancer.

Equilibrador de carga de red

Uso del cambio zonal para los balanceadores de carga de red

Para usar Network Load Balancers con cambio zonal, debe habilitar la integración de cambio zonal ARC en los atributos del Network Load Balancer. Network Load Balancer admite el cambio zonal con configuraciones entre zonas habilitadas o inhabilitadas entre zonas.

Puede elegir los recursos que desee utilizar para utilizar el cambio zonal y el cambio automático zonal y cuándo quiere salir por error de una zona de disponibilidad reducida. Se admiten balanceadores de carga de red internos y conectados a Internet.

Para habilitar el cambio zonal en su Network Load Balancer habilitado entre zonas, todos los grupos objetivo conectados al balanceador de cargas deben cumplir los siguientes requisitos.

- El equilibrio de carga entre zonas debe estar activado o configurado en. `use_load_balancer_configuration`
  - Para obtener más información sobre el equilibrio de cargas entre zonas del grupo objetivo, consulte Equilibrio de cargas entre zonas para los grupos objetivo.

- El protocolo del grupo objetivo debe ser TCP o TLS.
  - Para obtener más información sobre los protocolos de grupo objetivo de Network Load Balancer, consulte Configuración de enrutamiento.
- La terminación de la conexión para los destinos en mal estado debe estar deshabilitada.
  - Para obtener más información sobre la terminación de la conexión del grupo objetivo, consulte Terminación de la conexión para destinos en mal estado.
- El grupo objetivo no debe tener ningún balanceador de carga de aplicaciones como destino.
  - Para obtener más información sobre los balanceadores de carga de aplicaciones como destinos, consulte Usar balanceadores de carga de aplicaciones como destinos de un Network Load Balancer.

Puedes iniciar un cambio zonal para un Network Load Balancer mediante AWS CLI la consola o AWS el widget Elastic Load Balancing. Cuando un Application Load Balancer es el objetivo de un Network Load Balancer, debe iniciar el cambio zonal desde el Network Load Balancer. Si inicia el cambio zonal desde el Application Load Balancer, el Network Load Balancer no dejará de enviar tráfico al Application Load Balancer y a sus destinos.

Console

Para habilitar el cambio zonal en un balanceador de carga (consola)

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En la página de navegación, en Equilibrio de carga, selecciona Load Balancers.
3. Seleccione el nombre de Network Load Balancer.
4. En la pestaña Atributos, seleccione Editar.
5. En Configuración de enrutamiento de la zona de disponibilidad, establezca Integración de cambios de zona ARC como Habilitar.
6. Seleccione Save.

AWS CLI

Para habilitar el cambio zonal en un balanceador de carga ()AWS CLI

- Escriba el siguiente comando:

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

Para obtener más información sobre cómo activar un cambio zonal, consulte. Iniciar, actualizar o cancelar un cambio zonal

Cómo funciona el cambio zonal para los balanceadores de carga de red

El ARC provoca un error en la comprobación del estado del Network Load Balancer registrado, por lo que el nodo Network Load Balancer de la zona de disponibilidad dañada se elimina del DNS cuando se activa un cambio zonal. El Network Load Balancer deshabilitará los destinos de la zona afectada para que dejen de recibir tráfico, y Elastic Load Balancing trata estos objetivos como objetivos deshabilitados por cambio de zona. Los objetivos en estado deshabilitado siguen recibiendo controles de estado. Cuando los objetivos están en buen estado y el cambio zonal caduca (o se cancela), se reanuda el enrutamiento hacia los objetivos de la zona anteriormente afectada.

Durante un cambio de zona en equilibradores de carga de red con el equilibrio de carga entre zonas habilitado, las direcciones IP del equilibrador de carga de zona se eliminan del DNS. Las conexiones existentes con destinos de la zona de disponibilidad afectada persisten hasta que se cierran de manera orgánica, mientras que las nuevas conexiones dejan de enrutarse a destinos de la zona de disponibilidad afectada.

Para obtener más información, consulte el tema Cambio zonal para su balanceador de carga de red en la Guía del usuario de Network Load Balancer.

Iniciar, actualizar o cancelar un cambio zonal

Esta sección proporciona los procedimientos para trabajar con turnos zonales, incluido el inicio de un cambio zonal y la cancelación de un cambio zonal.

Comenzar un cambio de zona

Los pasos de esta sección explican cómo iniciar un cambio zonal iniciado por el cliente en la consola Amazon Application Recovery Controller (ARC). Para trabajar con el cambio de zona de forma programática, consulta la Guía de referencia de la API del cambio de zona.

Además de iniciar un cambio zonal en ARC, también puedes iniciar un cambio zonal para un balanceador de carga en la consola de Elastic Load Balancing (en las regiones compatibles). Para obtener más información, consulta Cambio zonal en la Guía del usuario de Elastic Load Balancing.

Comenzar un cambio de zona

1. Abra la consola ARC enhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. En Multi-AZ, elija Cambio zonal.
3. En la página de cambio zonal, selecciona Iniciar cambio zonal.
4. Seleccione la zona de disponibilidad de la que desee desviar el tráfico.
5. Seleccione un recurso compatible de la tabla Recursos para desviar el tráfico.
6. En Establecer caducidad de turno zonal, selecciona o introduce una caducidad para el turno zonal. Un cambio de zona se puede configurar desde 1 minuto hasta tres días (72 horas).

   Todos los cambios de zona son temporales. Debe establecer un vencimiento, pero puede actualizar los cambios activos más adelante para establecer un vencimiento nuevo de hasta tres días.
7. Ingrese un comentario. Si lo desea, puede actualizar el cambio de zona más adelante para editar el comentario.
8. Seleccione la casilla de verificación para confirmar que comenzar un cambio de zona reducirá la capacidad disponible de su aplicación al cambiar el tráfico de la zona de disponibilidad.
9. Elija Inicio.

Actualizar o cancelar un cambio zonal

En los pasos de esta sección se explica cómo actualizar un cambio zonal iniciado por usted, o cómo cancelar un cambio zonal, en la consola de Amazon Application Recovery Controller (ARC). Para trabajar con el cambio de zona de forma programática, consulta la Guía de referencia de la API del cambio de zona.

Puede actualizar un cambio zonal para establecer un nuevo vencimiento, o bien editar o reemplazar el comentario del cambio zonal. Puedes cancelar un cambio zonal en cualquier momento antes de que caduque.

Puede cancelar los cambios zonales que usted inicie o los cambios zonales que se AWS inicien para un recurso para una práctica con el cambio automático zonal. Para obtener más información sobre los turnos de práctica en el cambio automático zonal, consulte. Cómo funcionan el cambio automático de zona y las ejecuciones de práctica

Actualizar un cambio de zona

1. Abra la consola ARC en. https://console.aws.amazon.com/route53recovery/home#/dashboard
2. En Multi-AZ, elija Cambio de zona.
3. Seleccione el cambio de zona que desee actualizar y, a continuación, elija Actualizar cambio de zonal.
4. En Establecer vencimiento del cambio de zona, si lo desea, seleccione o ingrese un vencimiento.
5. En Comentario, si lo desea, edite el comentario existente o ingrese uno nuevo.
6. Elija Actualizar.

Cancelar un cambio de zona

1. Abra la consola ARC enhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. En Multi-AZ, elija Cambio de zona.
3. Seleccione el cambio de zona que desee cancelar y, a continuación, elija Cancelar cambio de zonal.
4. En el cuadro de diálogo de confirmación de modo, elija Confirmar.

Registro y supervisión del cambio zonal en Amazon Application Recovery Controller (ARC)

Puede usarlo AWS CloudTrail para monitorear el cambio zonal en Amazon Application Recovery Controller (ARC), para analizar patrones y ayudar a solucionar problemas.

Temas

- Registro de llamadas a la API de cambio zonal mediante AWS CloudTrail

Registro de llamadas a la API de cambio zonal mediante AWS CloudTrail

El cambio zonal de ARC está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en ARC. CloudTrail captura como eventos todas las llamadas a la API relacionadas con el cambio zonal. Las llamadas capturadas incluyen llamadas desde la consola ARC y llamadas en código a las operaciones de la API ARC para el cambio zonal.

Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos para el cambio zonal. Si no configura una ruta, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos.

Con la información recopilada por CloudTrail, puede determinar la solicitud de cambio zonal que se realizó a ARC, la dirección IP desde la que se realizó la solicitud, quién la hizo, cuándo se hizo y detalles adicionales.

Para obtener más información CloudTrail, consulte la Guía del AWS CloudTrail usuario.

Información sobre el cambio zonal en CloudTrail

CloudTrail está habilitada en tu cuenta Cuenta de AWS al crear la cuenta. Cuando se produce una actividad en ARC durante un cambio zonal, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Puede ver, buscar y descargar eventos recientes en su Cuenta de AWS. Para obtener más información, consulte Trabajar con el historial de CloudTrail eventos.

Para obtener un registro continuo de los eventos que se producen en su Cuenta de AWS entorno, incluidos los relacionados con el cambio zonal en ARC, cree un sendero. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las Regiones de AWS. La ruta registra los eventos de todas las regiones de la AWS partición y envía los archivos de registro al bucket de Amazon S3 que especifique. Además, puede configurar otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para más información, consulte los siguientes temas:

- Introducción a la creación de registros de seguimiento
- CloudTrail servicios e integraciones compatibles
- Configuración de las notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de CloudTrail registro de varias regiones y recibir archivos de CloudTrail registro de varias cuentas

Todas las acciones de ARC se registran CloudTrail y se documentan en la Guía de referencia de la API de control de enrutamiento para Amazon Application Recovery Controller. Por ejemplo, las llamadas a las `ListManagedResources` acciones `StartZonalShift` y las acciones generan entradas en los archivos de CloudTrail registro.

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con credenciales de usuario root o AWS Identity and Access Management (IAM).
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro AWS servicio.

Para obtener más información, consulte el elemento userIdentity de CloudTrail .

Visualización de eventos ARC en el historial de eventos

CloudTrail le permite ver los eventos recientes en el historial de eventos. Para obtener más información, consulte Uso del historial de CloudTrail eventos en la Guía del AWS CloudTrail usuario.

Descripción de las entradas de los archivos de registro de cambios zonales

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

En el siguiente ejemplo, se muestra una entrada de CloudTrail registro que demuestra la `ListManagedResources` acción del cambio zonal.


```
{
      "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"
      }
    }
```

El siguiente ejemplo muestra una entrada de CloudTrail registro que muestra la `StartZonalShift` acción con una excepción de conflicto para el cambio zonal.

```
{
      "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 para el cambio zonal en ARC

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a los recursos. AWS Los administradores de IAM controlan quién puede autenticarse (iniciar sesión) y quién puede autorizarse (tener permisos) para usar los recursos de ARC. La IAM es una Servicio de AWS opción que puede utilizar sin coste adicional.

Contenido

- Cómo funciona el cambio zonal con IAM
- IAM y permisos para el cambio de zona
- Ejemplos de políticas basadas en la identidad para el cambio zonal en ARC

Cómo funciona el cambio zonal con IAM

Antes de usar IAM para gestionar el acceso al cambio zonal en Amazon Application Recovery Controller (ARC), infórmese sobre las funciones de IAM disponibles para su uso con el cambio zonal.

Funciones de IAM que puede utilizar con el cambio zonal

Característica de IAM	Soporte de cambio zonal
Políticas basadas en identidades	Sí
Políticas basadas en recursos	No
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política	Sí
ACLs	No
ABAC (etiquetas en políticas)	Parcial
Credenciales temporales	Sí
Permisos de entidades principales	Sí

Característica de IAM	Soporte de cambio zonal
Roles de servicio	No
Roles vinculados al servicio	Sí

Para obtener una visión general y de alto nivel del funcionamiento de AWS los servicios con la mayoría de las funciones de IAM, consulte AWS los servicios que funcionan con IAM en la Guía del usuario de IAM.

Políticas de ARC basadas en la identidad

Compatibilidad con las políticas basadas en identidad: sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está asociada. Para obtener más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de las políticas de JSON de IAM en la Guía del usuario de IAM.

Para ver ejemplos de políticas de ARC basadas en la identidad, consulte. Ejemplos de políticas basadas en identidad en Amazon Application Recovery Controller (ARC)

Políticas basadas en recursos dentro de ARC

Admite políticas basadas en recursos: no

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico.

Acciones políticas para el cambio zonal

Compatibilidad con las acciones de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Las acciones políticas suelen tener el mismo nombre que la operación de AWS API asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de acciones de ARC para el cambio zonal, consulte Acciones definidas por Amazon Route 53 Zonal Shift en la Referencia de autorización de servicio.

Las acciones políticas en ARC para el cambio zonal utilizan los siguientes prefijos antes de la acción:

```
arc-zonal-shift
```

Para especificar varias acciones en una única instrucción, sepárelas con comas. Por ejemplo, los siguientes:

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

Puede utilizar caracteres comodín (*) para especificar varias acciones . Por ejemplo, para especificar todas las acciones que comiencen con la palabra `Describe`, incluya la siguiente acción:

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

Para ver ejemplos de políticas ARC basadas en la identidad para el cambio zonal, consulte. Ejemplos de políticas basadas en la identidad para el cambio zonal en ARC

Recursos de políticas para el cambio zonal

Compatibilidad con los recursos de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puedes realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puedes hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utiliza un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

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

Para ver una lista de los tipos de recursos y sus acciones ARNs, así como las acciones que puede especificar con el ARN de cada recurso, consulte el tema siguiente en la Referencia de autorización de servicios:

- Acciones definidas por Amazon Route 53 - Zonal Shift

Para ver las acciones y los recursos que puede utilizar con una clave de condición, consulte el siguiente tema en la Referencia de autorización de servicio:

- Claves de condición definidas por Amazon Route 53 - Zonal Shift

Para ver ejemplos de políticas de ARC basadas en la identidad para el cambio zonal, consulte. Ejemplos de políticas basadas en la identidad para el cambio zonal en ARC

Condiciones de la política: claves para el cambio zonal

Compatibilidad con claves de condición de políticas específicas del servicio: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puedes realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puedes crear expresiones condicionales que utilizan operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación `AND` lógica. Si especifica varios valores para una única clave de condición, AWS evalúa la condición mediante una `OR` operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puedes utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puedes conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para más información, consulta Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

Para ver una lista de claves de condición de cambio zonal, consulte el siguiente tema en la Referencia de autorización de servicio:

- Claves de condición definidas por Amazon Route 53 - Zonal Shift

Para ver las acciones y los recursos que puede usar con una clave de condición, consulte los siguientes temas de la Referencia de autorización de servicios:

- Acciones definidas por Amazon Route 53 - Zonal Shift
- Tipos de recursos definidos por Amazon Route 53: cambio zonal

Para ver ejemplos de políticas de ARC basadas en la identidad para el cambio zonal, consulte. Ejemplos de políticas basadas en la identidad para el cambio zonal en ARC

Listas de control de acceso () ACLs en ARC

Soporta ACLs: No

Las listas de control de acceso (ACLs) controlan qué directores (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLs son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Control de acceso basado en atributos (ABAC) con ARC

Compatibilidad con ABAC (etiquetas en las políticas): parcial

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos. En AWS, estos atributos se denominan etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a muchos AWS recursos. El etiquetado de entidades y recursos es el primer paso de ABAC. A continuación, designa las políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso al que se intenta acceder.

ABAC es útil en entornos que crecen con rapidez y ayuda en situaciones en las que la administración de las políticas resulta engorrosa.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte Definición de permisos con la autorización de ABAC en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

ARC incluye el siguiente soporte parcial para ABAC:

- El cambio zonal es compatible con ABAC para los recursos gestionados que están registrados en ARC para el cambio zonal. Para obtener más información sobre los recursos gestionados de ABAC para Equilibrador de carga de red y Equilibrador de carga de aplicación, consulte ABAC con Elastic Load Balancing en la Guía del usuario de Elastic Load Balancing.

Uso de credenciales temporales con ARC

Compatibilidad con credenciales temporales: sí

Algunas Servicios de AWS no funcionan cuando inicias sesión con credenciales temporales. Para obtener información adicional, incluida la información sobre cuáles Servicios de AWS funcionan con credenciales temporales, consulta Cómo Servicios de AWS funcionan con IAM en la Guía del usuario de IAM.

Utiliza credenciales temporales si inicia sesión en ellas AWS Management Console mediante cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accedes

AWS mediante el enlace de inicio de sesión único (SSO) de tu empresa, ese proceso crea automáticamente credenciales temporales. También crea credenciales temporales de forma automática cuando inicia sesión en la consola como usuario y luego cambia de rol. Para obtener más información sobre el cambio de roles, consulte Cambio de un usuario a un rol de IAM (consola) en la Guía del usuario de IAM.

Puedes crear credenciales temporales manualmente mediante la AWS CLI API o. AWS A continuación, puede utilizar esas credenciales temporales para acceder AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para obtener más información, consulte Credenciales de seguridad temporales en IAM.

Permisos principales entre servicios para ARC

Admite sesiones de acceso directo (FAS): sí

Cuando utiliza una entidad de IAM (usuario o rol) para realizar acciones en ella AWS, se le considera principal. Las políticas conceden permisos a una entidad principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. En este caso, debe tener permisos para realizar ambas acciones.

Para ver si una acción requiere acciones dependientes adicionales en una política, consulte el siguiente tema en la Referencia de autorización de servicios:

- Cambio de zona de Amazon Route 53

Funciones de servicio para ARC

Compatible con roles de servicio: No

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

Funciones vinculadas al servicio para ARC

Admite roles vinculados a servicios: sí

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio

aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

El cambio zonal no utiliza roles vinculados al servicio.

IAM y permisos para el cambio de zona

En esta sección se proporciona información adicional sobre cómo funcionan los permisos para la función de cambio zonal de Amazon Application Recovery Controller (ARC), especialmente si trabaja con la función de otro AWS servicio, como Elastic Load Balancing. Para obtener más información sobre cómo funcionan las funciones de ARC con la IAM y los permisos en general, consulte la información del tema general. Identity and Access Management para el cambio zonal en ARC

Zonal Shift admite balanceadores de carga de aplicaciones, balanceadores de carga de red, grupos de Amazon EC2 Auto Scaling y Amazon EKS. Puede utilizar las claves de condición de IAM para aplicar una política de permisos de IAM a estos recursos. A continuación, se muestra un ejemplo de política que utiliza una clave de condición con varios recursos de distintos tipos:

```
{
    "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"
}
```

Para obtener más información, consulte Recursos admitidos.

Además de los permisos descritos en el tema general de IAM, lo siguiente se aplica al cambio zonal de IAM y a los permisos:

- Asegúrese de tener los permisos necesarios para trabajar con el cambio zonal en ARC. Para obtener más información, consulte el acceso a la consola de cambios zonales y el acceso a las operaciones de turnos zonales.
- No necesita añadir permisos adicionales de Elastic Load Balancing con IAM para trabajar con los cambios zonales de los recursos del balanceador de carga gestionado en su cuenta en ARC.
- Una política AWS gestionada que proporciona acceso total a Elastic Load Balancing incluye permisos para trabajar con turnos zonales. Si utilizas políticas AWS gestionadas para el acceso a Elastic Load Balancing, no necesitas permisos adicionales en IAM para el cambio zonal para iniciar los turnos zonales para los balanceadores de carga o trabajar con ellos en la consola de Elastic Load Balancing. Para obtener más información, consulte Políticas administradas por AWS para Elastic Load Balancing.

Ejemplos de políticas basadas en la identidad para el cambio zonal en ARC

De forma predeterminada, los usuarios y los roles no tienen permiso para crear o modificar los recursos de ARC. Tampoco pueden realizar tareas mediante la AWS Management Console, AWS Command Line Interface (AWS CLI) o la AWS API. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puedes añadir las políticas de IAM a roles y los usuarios puedes asumirlos.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM (consola) en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos por ARC, incluido el ARNs formato de cada uno de los tipos de recursos, consulte Acciones, recursos y claves de condición de Amazon Application Recovery Controller (ARC) en la Referencia de autorización de servicios.

Temas

- Prácticas recomendadas sobre las políticas
- Ejemplo: acceso a la consola de cambios zonal
- Ejemplo: acciones de la API de cambio zonal

Prácticas recomendadas sobre las políticas

Las políticas basadas en la identidad determinan si alguien puede crear, eliminar o acceder a los recursos de ARC de su cuenta. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulta las políticas administradas por AWS o las políticas administradas por AWS para funciones de tarea en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulta Políticas y permisos en IAM en la Guía del usuario de IAM.
- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo AWS CloudFormation. Para obtener más información, consulta Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utiliza el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Validación de políticas con el Analizador de acceso de IAM en la Guía del usuario de IAM.
- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para exigir la MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para más información, consulte Acceso seguro a la API con MFA en la Guía del usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Ejemplo: acceso a la consola de cambios zonal

Para acceder a la consola Amazon Application Recovery Controller (ARC), debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre los recursos ARC de su propiedad Cuenta de AWS. Si crea una política basada en identidades que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

No es necesario que concedas permisos mínimos de consola a los usuarios que solo realicen llamadas a la API AWS CLI o a la AWS API. En su lugar, permite el acceso únicamente a las acciones que coincidan con la operación de API que intentan realizar.

Para que los usuarios tengan acceso total al uso del cambio zonal en la AWS Management Console, adjunta al usuario una política como la siguiente:

```
{
    "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": "*"
        }
    ]
}
```

Ejemplo: acciones de la API de cambio zonal

La API de cambio zonal aleja temporalmente el tráfico de una zona de disponibilidad para recuperar una aplicación.

Para garantizar que un usuario pueda utilizar las acciones de la API de cambio zonal, adjunta una política que corresponda a las operaciones de la API con las que el usuario debe trabajar, como las siguientes:

```
{
    "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": "*"
        }
    ]
}
```

Cambio automático zonal en ARC

Con el cambio automático zonal, usted autoriza AWS a desviar el tráfico de recursos de una aplicación desde una zona de disponibilidad (AZ) durante los eventos, en su nombre, para reducir el tiempo de recuperación. AWS inicia un cambio automático cuando la telemetría interna indica que hay una alteración en la zona de disponibilidad que podría afectar a los clientes. Cuando se AWS inicia un cambio automático, el tráfico de aplicaciones hacia los recursos que ha configurado para el cambio automático zonal comienza a alejarse de la zona de disponibilidad.

Tenga en cuenta que ARC no inspecciona el estado de los recursos individuales. AWS inicia un cambio automático cuando la AWS telemetría detecta una alteración en la zona de disponibilidad que podría afectar a los clientes. En algunos casos, es posible que el tráfico se desvíe hacia recursos que no se vean afectados.

Con el cambio automático zonal, también autorizas AWS a desviar el tráfico de recursos de una aplicación desde una zona de disponibilidad, en tu nombre, para realizar prácticas habituales. Es necesario realizar ejecuciones de práctica para el cambio automático de zona. Los cambios zonales que ARC inicia para las sesiones de práctica le ayudan a garantizar que desviar el tráfico de una zona de disponibilidad durante un cambio automático sea seguro para su aplicación. Las ejecuciones de práctica prueban de forma periódica que la aplicación puede funcionar con normalidad sin una zona de disponibilidad. Para ello, inicie cambios de zona que desvíen el tráfico de un recurso de una zona de disponibilidad. Las sesiones de práctica se llevan a cabo semanalmente y proporcionan un resultado (por ejemplo, `SUCCEEDED` o) que le ayuda `FAILED` a comprender si la aplicación funciona según lo esperado.

> **Important**
>
> Antes de configurar las ejecuciones de práctica o habilitar el cambio automático zonal, le recomendamos encarecidamente que escale previamente la capacidad de los recursos de la aplicación en todas las zonas de disponibilidad de la región en la que están desplegados los recursos de la aplicación. No debe confiar en el escalado según la demanda cuando comience un cambio automático o una ejecución de práctica. El cambio automático de zona, incluidas las ejecuciones de práctica, funciona de forma independiente y no espera a que se completen las acciones de escalado automático. Confiar en el escalado automático, en lugar del escalado previo, puede provocar que la aplicación tarde más en recuperarse.
> Si utiliza el escalado automático para gestionar los ciclos de tráfico normales, le recomendamos encarecidamente que configure la capacidad mínima del escalado automático para seguir funcionando con normalidad si se pierde una zona de disponibilidad.

Si planea habilitar el cambio automático zonal o configurar ejecuciones de práctica, después de preescalar la capacidad de recursos de la aplicación, compruebe que la aplicación puede funcionar normalmente sin una zona de disponibilidad. Para comprobarlo, inicie un cambio de zona para desviar el tráfico de un recurso de una zona de disponibilidad.

Tras activar el cambio automático zonal, le recomendamos que compruebe, iniciando y evaluando una práctica de cambio zonal bajo demanda, que su aplicación puede seguir funcionando con normalidad si el tráfico se desplaza fuera de una zona de disponibilidad. Luego, la práctica habitual que realiza ARC le ayuda a confirmar, de forma continua, que tiene suficiente capacidad para realizar un cambio automático.

Para garantizar que las pruebas con el cambio zonal sean eficaces, es importante comprobar que el tráfico se agota según lo previsto desde la zona de destino desde la que se va a desplazar. Por ejemplo, tanto los balanceadores de carga de aplicaciones como los balanceadores de carga de red proporcionan métricas por zona de disponibilidad en Amazon CloudWatch que puedes usar para monitorizarlos. En función del tiempo que un servicio y los clientes reutilicen las conexiones, es posible que el tráfico continúe hacia la zona de la que te has desplazado durante más tiempo del esperado. Para obtener más información, consulte Limitar el tiempo que los clientes permanecen conectados a sus puntos de conexión.

Puede activar el cambio automático zonal, para un recurso compatible, en la consola ARC. O bien, en la EC2 consola de Amazon, tienes la opción de habilitar el cambio automático zonal para un recurso de balanceador de carga específico. Para obtener más información sobre cómo habilitar el cambio automático zonal con Elastic Load Balancing, consulta Zonal shift en la Guía del usuario de Elastic Load Balancing.

Los cambios de zona de las ejecuciones de práctica y los cambios automáticos son temporales. Con los cambios automáticos, cuando la zona de disponibilidad afectada se recupera, se AWS detiene el traslado del tráfico de recursos fuera de la zona de disponibilidad. El tráfico de aplicaciones de los clientes vuelve a todas las zonas de disponibilidad de la región. Con una ejecución de práctica, el tráfico se desvía de una zona de disponibilidad para un solo recurso durante unos 30 minutos y, a continuación, vuelve a dirigirse a todas las zonas de disponibilidad de la región.

Puedes configurar EventBridge las notificaciones de Amazon para que te avisen sobre los cambios automáticos y las carreras de práctica. Para obtener más información, consulte Uso del cambio automático zonal con Amazon EventBridge.

Cómo funcionan el cambio automático de zona y las ejecuciones de práctica

La capacidad de cambio automático zonal de Amazon Application Recovery Controller (ARC) AWS permite desviar el tráfico de un recurso fuera de una zona de disponibilidad, en su nombre, cuando se AWS determina que hay un impedimento que podría afectar a los clientes de la zona de disponibilidad. El cambio automático zonal está diseñado para un recurso preescalado en todas las zonas de disponibilidad de una Región de AWS, de forma que una aplicación pueda funcionar con normalidad si se pierde una zona de disponibilidad.

Con el cambio automático zonal, es necesario configurar las ejecuciones de práctica, en las que ARC desplaza periódicamente el tráfico del recurso fuera de una zona de disponibilidad. ARC programa

las ejecuciones de práctica aproximadamente una vez por semana para cada recurso que tenga asociada una configuración de ejecución práctica. Las ejecuciones de práctica para cada recurso se programan de forma independiente.

Para cada sesión de práctica, ARC registra un resultado. Si una ejecución de práctica se ve interrumpida por una condición de bloqueo, el resultado de dicha ejecución no se marcará como correcto. Para obtener más información sobre los resultados de las ejecuciones de práctica, consulte Resultados de las ejecuciones de práctica.

Puedes configurar EventBridge las notificaciones de Amazon para que te envíen información sobre los cambios automáticos y las carreras de práctica. Para obtener más información, consulte Uso del cambio automático zonal con Amazon EventBridge.

Contenido

- Acerca del cambio automático zonal
- Cuando se AWS inicia y se detiene, los cambios automáticos
- Cuando ARC planifique, inicie y finalice, tendrá lugar una sesión de práctica
- Comprobaciones de capacidad para las carreras de práctica
- Notificación para las carreras de práctica y los cambios automáticos
- Prioridad de los cambios zonales
- Detener un cambio automático activo o una ejecución de práctica de un recurso
- Cómo se desvía el tráfico
- Alarmas para las ejecuciones de práctica
- Fechas y periodos bloqueados (UTC)

Acerca del cambio automático zonal

El cambio automático zonal es una capacidad que, en su nombre, AWS desplaza el tráfico de recursos de las aplicaciones fuera de una zona de disponibilidad. AWS inicia un cambio automático cuando la telemetría interna indica que hay un deterioro en la zona de disponibilidad que podría afectar a los clientes. La telemetría interna incorpora métricas de varias fuentes, incluida la AWS red y los servicios Amazon EC2 y Elastic Load Balancing.

Debe habilitar manualmente el cambio automático zonal para los recursos compatibles. AWS

Si despliega y ejecuta AWS aplicaciones en balanceadores de carga en varias regiones (normalmente tres) AZs y las escala previamente para mantener la estabilidad estática, AWS puede

recuperar rápidamente las aplicaciones de los clientes en una zona de disponibilidad al reducir el tráfico con un cambio automático. Al desviar el tráfico de recursos a otras AZs zonas de la región, AWS puede reducir la duración y la gravedad del posible impacto causado por cortes de energía, problemas de hardware o software en una zona de disponibilidad u otros problemas.

Los recursos respaldados por ARC proporcionan integraciones que marcan la AZ especificada como insalubre, lo que provoca que el tráfico se desvíe de la AZ dañada.

Al habilitar el cambio automático zonal para un recurso, también debe configurar una ejecución de práctica para el recurso. AWS realiza ejecuciones de práctica aproximadamente una vez por semana, durante 30 minutos, para asegurarse de que tiene la capacidad suficiente para ejecutar la aplicación sin una de las zonas de disponibilidad de la región.

Al igual que ocurre con el cambio de zona, hay algunas situaciones específicas en las que el cambio automático de zona no desvía el tráfico de la zona de disponibilidad. Por ejemplo, si los grupos objetivo del balanceador de carga AZs no tienen ninguna instancia, o si todas las instancias están en mal estado, entonces el balanceador de carga está en un estado de apertura por error y no puedes cambiar ninguna de ellas. AZs

Para obtener más información sobre el cambio automático de zona, consulte Cambio automático zonal en ARC.

Cuando se AWS inicia y se detiene, los cambios automáticos

Cuando habilita el cambio automático zonal para un recurso, autoriza AWS a desviar el tráfico de recursos de una aplicación desde una zona de disponibilidad durante los eventos, en su nombre, para reducir el tiempo de recuperación.

Para lograrlo, el cambio automático zonal utiliza la AWS telemetría para detectar, lo antes posible, si existe una alteración en la zona de disponibilidad que podría afectar a los clientes. Cuando AWS inicia un cambio automático, el tráfico hacia los recursos configurados comienza a desviarse inmediatamente de la zona de disponibilidad afectada, lo que podría afectar a los clientes.

El cambio automático zonal es una función diseñada para los clientes que han ajustado previamente los recursos de sus aplicaciones para todas las zonas de disponibilidad de una. Región de AWS No debe confiar en el escalado según la demanda cuando comience un cambio automático o una ejecución de práctica.

AWS finaliza un cambio automático cuando determina que la zona de disponibilidad se ha recuperado.

Cuando ARC planifique, inicie y finalice, tendrá lugar una sesión de práctica

ARC programa una sesión de práctica para un recurso semanalmente, durante unos 30 minutos. ARC programa, inicia y gestiona las sesiones de práctica para cada recurso de forma independiente. ARC no agrupa las ejecuciones de práctica para los recursos de la misma cuenta. También puede iniciar usted mismo las sesiones de práctica bajo demanda, para comprobar que la configuración es segura para un evento de cambio automático zonal.

Cuando una ejecución de práctica continúa durante el tiempo previsto, sin interrupción, se marca con un resultado de `SUCCESSFUL`. Hay otros resultados posibles:`FAILED`, `INTERRUPTED` y `PENDING`. Los valores y las descripciones de los resultados se incluyen en la sección Resultados de las ejecuciones de práctica.

Hay algunos escenarios en los que ARC interrumpe una sesión de práctica y la termina. Por ejemplo, si un cambio automático se inicia durante una carrera de práctica, el ARC interrumpe la carrera de práctica y la finaliza. Como otro ejemplo, supongamos que el recurso tiene una respuesta adversa a una ejecución de práctica y provoca que una alarma que ha establecido para supervisar la práctica pase a un estado de `ALARM`. En este escenario, el ARC también interrumpe la sesión de práctica y la finaliza.

Además, hay varios escenarios en los que ARC no inicia una ejecución de práctica programada para un recurso.

En respuesta a las ejecuciones de práctica interrumpidas o bloqueadas de un recurso, ARC hace lo siguiente:

- Si una sesión de práctica para un recurso se interrumpe mientras está en curso, ARC considera que la sesión de práctica semanal ha terminado y programa una nueva sesión de práctica para el recurso para la semana siguiente. El resultado de la práctica semanal es `INTERRUPTED` en esta situación, no `FAILED`. El resultado de la ejecución de práctica se establece `FAILED` solo cuando la alarma de resultado que supervisa la ejecución de práctica pasa a un estado de `ALARM` durante la ejecución de práctica.
- Si hay una restricción que bloquea el inicio de una sesión de práctica para un recurso, ARC no inicia la sesión de práctica. ARC continúa con la supervisión periódica para determinar si aún existen una o más restricciones de bloqueo. Cuando no hay ninguna restricción de bloqueo, ARC inicia la ejecución de práctica del recurso.

Los siguientes son ejemplos de restricciones de bloqueo que impiden que ARC inicie o continúe una ejecución de práctica para un recurso:

- ARC no inicia ni continúa las sesiones de práctica cuando hay un AWS Fault Injection Service experimento en curso. Si un AWS FIS evento está activo cuando ARC ha programado el inicio de una carrera de práctica, ARC no la iniciará. El ARC monitorea durante las sesiones de práctica las restricciones de bloqueo, incluido un AWS FIS evento. Si un AWS FIS evento comienza mientras hay una sesión de práctica activa, ARC finaliza la sesión de práctica y no intenta iniciar otra hasta la siguiente sesión de práctica programada regularmente para el recurso.
- Si hay un AWS evento actual en una región, ARC no inicia las sesiones de práctica para obtener recursos y finaliza las sesiones de práctica activas en la región.

Cuando la sesión de práctica termine sin ser interrumpida, el ARC programa la siguiente sesión de práctica en una semana, como de costumbre. Si una sesión de práctica no se inicia debido a una restricción de bloqueo, como un AWS FIS experimento o un intervalo de tiempo bloqueado que hayas especificado, ARC seguirá intentando iniciar una sesión de práctica hasta que se pueda iniciar la sesión de práctica.

Comprobaciones de capacidad para las carreras de práctica

Cuando comienza una sesión de práctica, para alejar temporalmente el tráfico de una zona de disponibilidad, ARC comprueba si hay suficiente capacidad en otras zonas de disponibilidad para alejar el tráfico de la zona de disponibilidad de forma segura. Si no hay suficiente capacidad disponible, el cambio de tráfico de la sesión de práctica no se inicia y la sesión de práctica finaliza.

Además, el ARC comprueba la capacidad de los recursos del balanceador de carga cuando se completa un cambio automático zonal, antes de que el ARC finalice el cambio de tráfico iniciado por el cambio automático. Si la comprobación de capacidad falla cuando finaliza el cambio automático, el tráfico no se desplaza de nuevo a la zona de disponibilidad de la que se alejó.

Las comprobaciones de capacidad balanceada solo se completan para los balanceadores de carga y los grupos de Auto Scaling.

En el caso de un recurso de equilibrador de carga, las comprobaciones de capacidad validan que los hosts en buen estado asociados al equilibrador de carga estén distribuidos entre las zonas de disponibilidad. En concreto, las comprobaciones de capacidad garantizan que el número de hosts en buen estado en todas las zonas de disponibilidad en las que está registrado el recurso esté equilibrado. En el caso de las comprobaciones de capacidad, equilibrado significa que la capacidad

en buen estado de cada zona de disponibilidad es igual a la de las demás zonas, dentro de una pequeña variación.

Tenga en cuenta que las comprobaciones de capacidad no se aplican a los balanceadores de carga con grupos objetivo de tipo Lambda ni a los balanceadores de carga de aplicaciones, ya que esos objetivos no están configurados por zonas.

También se realizan comprobaciones de capacidad para los grupos de Auto Scaling. Para un grupo de Auto Scaling, las comprobaciones de capacidad validan que la capacidad zonal total en buen estado de un grupo de Auto Scaling (es decir, la cantidad total de hosts en buen estado en todas las zonas de disponibilidad) cumpla con el conjunto de capacidad deseado para ese grupo de Auto Scaling.

Cuando se produce un error en una comprobación de capacidad

Cuando una comprobación de capacidad descubre que la capacidad disponible no está equilibrada para un recurso, el resultado de la práctica sí lo está`CAPACITY_CHECK_FAILED`. Para obtener más información sobre los motivos por los que se ha producido un error en una comprobación de capacidad, consulte el campo de comentarios del`ZonalShiftSummary`. Para encontrar el campo de comentarios para el turno zonal de su sesión de práctica, haga lo siguiente:

1. Utilice el AWS CLI, enumere los cambios zonales del recurso que especificó en la ejecución de práctica mediante la operación de ListZonalShiftsAPI.

   FOr Por ejemplo, para devolver los cambios zonales, puedes ejecutar un comando similar al siguiente:

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

2. Revise la matriz de `ZonalShiftSummary` objetos devueltos para encontrar el cambio zonal de la sesión de práctica que falló debido a las comprobaciones de capacidad.
3. Para conocer el cambio zonal aplicable, revise la información del `Comment` campo.

Notificación para las carreras de práctica y los cambios automáticos

Puedes elegir que se te notifique sobre las prácticas y los cambios automáticos de tu recurso configurando EventBridge las notificaciones de Amazon. Puedes configurar EventBridge las

notificaciones incluso cuando no hayas activado el cambio automático zonal para ningún recurso, lo que se conoce como notificación de cambio automático al observador. Con la notificación al observador de cambios automáticos, recibirá una notificación sobre todos los cambios automáticos que inicie el ARC cuando una zona de disponibilidad esté potencialmente dañada. Tenga en cuenta que debe configurar esta opción en cada una de las Región de AWS que desee recibir notificaciones.

Para ver los pasos para activar la notificación de cambio automático al observador, consulteActivar o desactivar la notificación de cambio automático al observador. Para obtener más información sobre las opciones de notificación y cómo configurarlas EventBridge, consulteUso del cambio automático zonal con Amazon EventBridge.

Prioridad de los cambios zonales

No se puede aplicar más de un cambio zonal a la vez. Es decir, solo una práctica consiste en ejecutar un cambio zonal, un cambio zonal iniciado por el cliente, un cambio automático o un experimento con el recurso. AWS FIS Cuando se inicia un segundo cambio zonal, el ARC sigue una prioridad para determinar qué tipo de cambio zonal está en vigor para un recurso.

El principio general de prioridad es que los cambios zonales que inicie como cliente tienen prioridad sobre otros tipos de turnos. Sin embargo, tenga en cuenta que una sesión de práctica AWS iniciada actualmente le impide iniciar una sesión de práctica bajo demanda.

Para ilustrar la prioridad en ARC, a continuación se explica cómo funciona la prioridad, por ejemplo, en algunos escenarios:

Tipo de cambio zonal aplicado	Tipo de cambio zonal iniciado	Resultado
AWS FIS experimento	Practica, corre	La sesión de práctica no podrá comenzar, ya que el AWS FIS experimento tiene prioridad.
AWS FIS experimento	Cambio zonal manual	El AWS FIS experimento se cancelará y se aplicará el cambio zonal manual.
AWS FIS experimento	Cambio automático de zona	El AWS FIS experimento se cancelará y se aplicará el cambio automático zonal.

Tipo de cambio zonal aplicado	Tipo de cambio zonal iniciado	Resultado
AWS FIS experimento	AWS FIS experimento	El AWS FIS experimento iniciado no podrá iniciarse porque hay un experimento en ejecución que activó la acción de AWS FIS cambio automático.
Practica y corre	Cambio zonal manual	La sesión de práctica se cancelará y el resultado se establecerá en y se aplicará el cambio zonal. `INTERRUPTED`
Carrera de práctica	AWS FIS experimento	La sesión de práctica se cancelará y el resultado se `INTERRUPTED` establecerá en y se aplicará el AWS FIS experimento.
Carrera de práctica	Cambio automático de zona	La carrera de práctica se cancelará y el resultado se establecerá en y se aplicará el cambio automático zonal. `INTERRUPTED`
Cambio zonal manual	Carrera de práctica	La tanda de práctica no podrá comenzar.
Cambio zonal manual	AWS FIS experimento	El AWS FIS experimento no podrá iniciarse o fallará si ya está en curso.
Cambio zonal manual	Cambio automático de zona	El cambio automático zonal estará presente, `ACTIVE` pero no `APPLIED` en el recurso. El cambio zonal manual tiene prioridad.

Tipo de cambio zonal aplicado	Tipo de cambio zonal iniciado	Resultado
Cambio automático de zona	AWS FIS experimento	El AWS FIS experimento no podrá iniciarse o fallará si está en curso.
Cambio automático de zona	Cambio zonal manual	El cambio automático zonal estará presente, `ACTIVE` pero no `APPLIED` en el recurso. El cambio zonal manual tiene prioridad.
Cambio automático de zona	Practica y corre	La carrera de práctica no podrá comenzar, ya que prevalecerá el cambio automático zonal.

El cambio de tráfico que está actualmente en vigor para el recurso tiene un estado de cambio de zona aplicado establecido en `APPLIED`. Solo se establece un cambio en `APPLIED` en cualquier momento. Los demás cambios que están en curso están configurados en el estado`NOT_APPLIED`, pero permanecen en él. `ACTIVE`

Detener un cambio automático activo o una ejecución de práctica de un recurso

Para detener un cambio automático en curso para un recurso, debes cancelar el cambio zonal.

Se siguen realizando ejecuciones de práctica habituales para el recurso, con la misma programación. Si desea detener las ejecuciones de práctica además de deshabilitar los cambios automáticos, debe eliminar la configuración de la ejecución de práctica asociada al recurso.

Al eliminar una configuración de ejecución de práctica, AWS deja de realizar ejecuciones de práctica que desvían el tráfico del recurso fuera de una zona de disponibilidad cada semana. Además, dado que el cambio automático zonal requiere ejecuciones de práctica, al eliminar una configuración de ejecución de práctica mediante la consola ARC, esta acción también deshabilita el cambio automático zonal para el recurso. Sin embargo, tenga en cuenta que si utiliza la API de cambio automático de zona para eliminar una ejecución de práctica, primero, debe deshabilitar el cambio automático de zona para el recurso.

Para obtener más información, consulte Cancelación de un cambio automático zonal y Habilitar el cambio automático zonal y trabajar con él.

Cómo se desvía el tráfico

Para los turnos automáticos y para los turnos zonales de práctica, el tráfico se desplaza fuera de una zona de disponibilidad mediante el mismo mecanismo que utiliza ARC para los cambios zonales iniciados por el cliente. Una comprobación de estado defectuosa provoca que Amazon Route 53 retire del DNS las direcciones IP correspondientes al recurso, de modo que el tráfico se redirija desde la zona de disponibilidad. En su lugar, las nuevas conexiones ahora se enrutan a otras zonas de Región de AWS disponibilidad.

Con un cambio automático, cuando una zona de disponibilidad se recupera y AWS decide finalizar el cambio automático, ARC invierte el proceso de comprobación de estado y solicita que se reviertan las comprobaciones de estado de Route 53. A continuación, se restauran las direcciones IP zonales originales y, si las comprobaciones de estado siguen funcionando correctamente, se vuelve a incluir la zona de disponibilidad en el enrutamiento de la aplicación.

Es importante tener en cuenta que los cambios automáticos no se basan en comprobaciones de estado que supervisen el estado subyacente de los equilibradores de carga ni de las aplicaciones. ARC utiliza las comprobaciones de estado para alejar el tráfico de las zonas de disponibilidad, solicitando que las comprobaciones de estado estén en mal estado y, a continuación, restablece las comprobaciones de estado a la normalidad cuando finaliza un cambio zonal o automático.

Alarmas para las ejecuciones de práctica

Puede especificar dos CloudWatch alarmas para las sesiones de práctica en el cambio automático zonal. Es obligatoria la primera alarma, la alarma de resultado. Debe configurar la alarma de resultado para supervisar el estado de la aplicación cuando el tráfico se desvíe de una zona de disponibilidad durante cada ejecución de práctica de 30 minutos.

Para que una ejecución de práctica sea eficaz, especifique como alarma de resultado una CloudWatch alarma que supervise las métricas del recurso o de la aplicación y que responda con un `ALARM` estado en el que la aplicación se vea afectada negativamente por la pérdida de una zona de disponibilidad. Para obtener más información, consulte la sección Alarmas que especifique para las ejecuciones de práctica en Mejores prácticas a la hora de configurar el cambio automático zonal.

La alarma de resultados también proporciona información sobre el resultado de la ejecución de práctica que ARC informa para cada ejecución de práctica. Si la alarma entra en un estado de

ALARM, la ejecución de práctica finaliza y el resultado de la ejecución de práctica se devuelve como FAILED. Si la ejecución de práctica completa el periodo de prueba programado de 30 minutos y la alarma de resultado no entra en el estado de ALARM, el resultado se devuelve como SUCCEEDED. En la sección Resultados de ejecuciones de práctica se proporciona una lista de todos los valores de resultados, junto con descripciones.

Si lo desea, puede especificar una segunda alarma, la alarma de bloqueo. La alarma de bloqueo no permite iniciar ejecuciones de práctica, ni continuar con ellas, cuando se encuentra en un estado de ALARM. Esta alarma bloquea el inicio de los cambios de tráfico de ejecución de práctica, y detiene cualquier ejecución de práctica en curso, cuando la alarma se encuentra en un estado de ALARM.

Por ejemplo, en una arquitectura grande con varios microservicios, cuando un microservicio tiene un problema, lo normal es detener todos los demás cambios en el entorno de la aplicación, lo que incluye bloquear las ejecuciones de práctica.

Fechas y periodos bloqueados (UTC)

Tienes la opción de bloquear las carreras de práctica para fechas específicas del calendario o para intervalos de tiempo específicos, es decir, días y horas, en UTC.

Por ejemplo, si tiene una actualización de la aplicación programada para el 1 de mayo de 2024 y no quiere que las ejecuciones de práctica desvíen el tráfico en ese momento, puede establecer una fecha bloqueada para el 2024-05-01.

O supongamos que se ejecutan resúmenes de informes empresariales tres días a la semana. En esta situación, puede establecer los siguientes días y horas periódicos como periodos de tiempo bloqueados, por ejemplo, en UTC: MON-20:30-21:30 WED-20:30-21:30 FRI-20:30-21:30.

Región de AWS disponibilidad para el cambio automático zonal

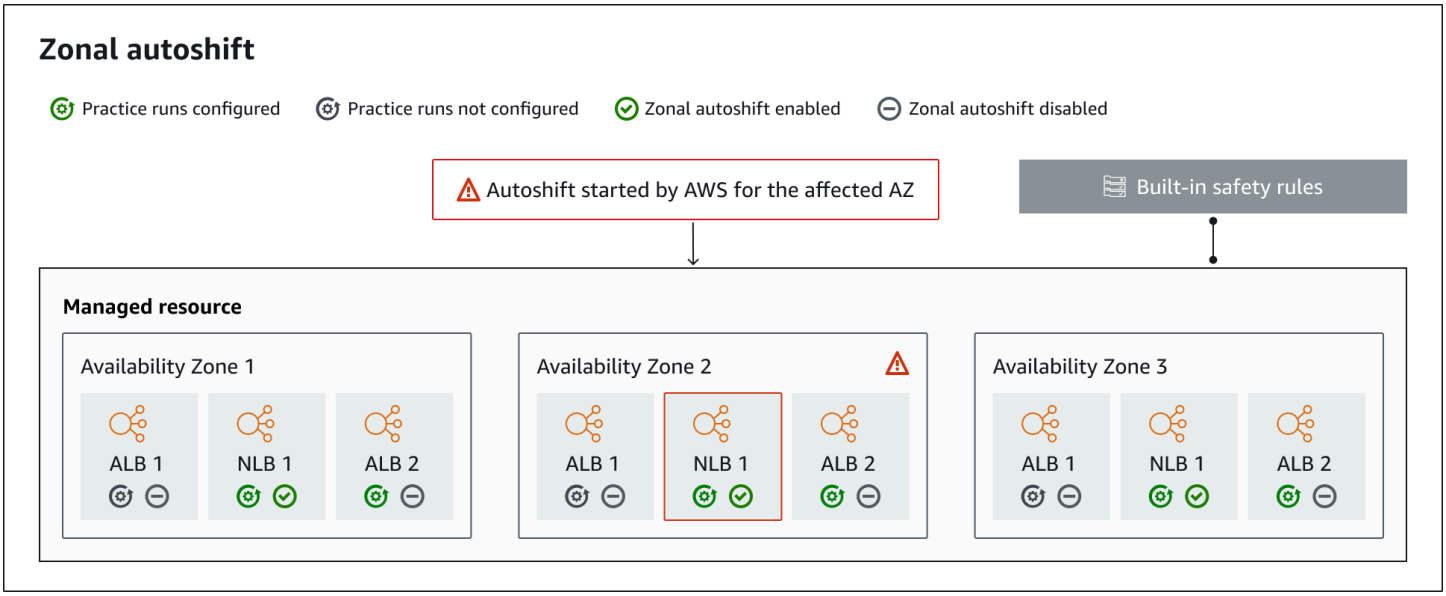
El cambio zonal y el cambio automático zonal están disponibles actualmente en las regiones comerciales Regiones de AWS, así como en las de China, es decir, en la región de China (Beijing) y en la región de China (Ningxia).

Los recursos que utilizan Amazon Application Recovery Controller (ARC) pueden incluir consideraciones adicionales. Para obtener más información, consulte Recursos admitidos.

Para obtener una lista de regiones e información detallada sobre los puntos de enlace de soporte y servicio regionales para ARC, consulte los puntos de enlace y las cuotas de Amazon Application Recovery Controller (ARC) en la Referencia general de Amazon Web Services.

Componentes del cambio automático de zona

El siguiente diagrama ilustra un ejemplo de un cambio automático que desvía el tráfico de una zona de disponibilidad. AWS inicia un cambio automático cuando la telemetría interna indica que hay una alteración en la zona de disponibilidad que podría afectar a los clientes.



Los siguientes son componentes de las capacidades de cambio automático zonal de ARC.

Cambio automático de zona

El cambio automático de zona desvía el tráfico para un recurso, sin que tenga que realizar ninguna acción. El cambio automático zonal es una función de ARC que permite AWS iniciar un cambio automático cuando la telemetría interna indica que existe una alteración en la zona de disponibilidad que podría afectar a los clientes. Tenga en cuenta que, en algunos casos, es posible que se desvíen recursos que no se vean afectados.

Ejecuciones de práctica

Al habilitar el cambio automático zonal para un recurso, también debe configurar las ejecuciones de práctica de cambio automático zonal para el recurso. AWS realiza un cambio zonal para las sesiones de práctica aproximadamente una vez por semana, durante unos 30 minutos. También puedes programar sesiones de práctica a pedido.

Las ejecuciones de práctica garantizan que la aplicación pueda ejecutarse con normalidad sin una zona de disponibilidad. En una ejecución de práctica, AWS desplaza el tráfico de un recurso fuera de una zona de disponibilidad con un cambio zonal y, a continuación, desplaza el tráfico hacia atrás cuando finaliza la ejecución de práctica.

Configuración de una ejecución de práctica

Una configuración de ejecución de práctica define las fechas y ventanas bloqueadas, si las hay, y las CloudWatch alarmas que se especifican para una ejecución de AWS práctica de un recurso en el cambio automático zonal. Puede editar la configuración de una sesión de práctica en cualquier momento para añadir o cambiar las fechas o ventanas bloqueadas, o para actualizar las alarmas de la ejecución de práctica.

Para activar el cambio automático zonal, debe disponer de una configuración de ejecución de práctica para un recurso. También puede eliminar una carrera de práctica. Para eliminar la configuración de una ejecución de práctica de un recurso, debe deshabilitarse el cambio automático de zona.

Alarma de una ejecución de práctica

Al configurar las ejecuciones de práctica, se especifican CloudWatch las alarmas que se crean en CloudWatch función de los requisitos de recursos y aplicaciones. Las alarmas que se especifiquen pueden impedir que se inicie una ejecución de práctica o pueden detener una ejecución de práctica en curso si la aplicación se ve afectada negativamente por esta.

Si una alarma que especifique pasa a un `ALARM` estado, ARC finaliza el cambio zonal durante la práctica, de modo que el tráfico del recurso ya no se desvíe de la zona de disponibilidad.

Hay dos tipos de alarmas que se especifican para las ejecuciones de práctica: una alarma de resultado para supervisar el estado del recurso y la aplicación durante la ejecución de práctica, y una alarma de bloqueo, que se puede configurar para impedir que se inicien las ejecuciones de práctica o para detener una ejecución de práctica en curso. La alarma de resultado es obligatoria; la alarma de bloqueo es opcional.

Resultado de una ejecución de práctica

ARC informa de un resultado para cada sesión de práctica. A continuación se muestran los posibles resultados de las ejecuciones de práctica:

- PENDIENTE: el cambio de zona para la ejecución de práctica está activo (en curso). Aún no hay ningún resultado que mostrar.
- CORRECTO: la alarma de resultado no entró en ningún estado de `ALARM` durante la ejecución de práctica, y la ejecución de práctica llevó a cabo el periodo de prueba completo de 30 minutos.
- INTERRUMPIDA: la ejecución de práctica finalizó por un motivo distinto al de la alarma de resultado al entrar en un estado de `ALARM`. Una ejecución de práctica puede interrumpirse por

varios motivos. Por ejemplo, una ejecución de práctica que finaliza porque la alarma de bloqueo especificada para ella ha entrado en un estado de `ALARM` tiene un resultado de `INTERRUPTED`. Para obtener más información sobre un resultado de `INTERRUPTED`, consulte Resultados de las ejecuciones de práctica.

- ERROR: la alarma de resultado entró en un estado de `ALARM` durante la ejecución de práctica.
- CAPACITY_CHECK_FAILED: No se pudo comprobar la capacidad equilibrada entre las zonas de disponibilidad para los recursos del grupo de equilibrio de carga y Auto Scaling.

Reglas de seguridad integradas

Las normas de seguridad integradas en el ARC impiden que se produzca más de un cambio de tráfico para un recurso a la vez. Es decir, solo un cambio zonal iniciado por el cliente, un cambio zonal de práctica (iniciado por AWS o por un cliente) o un cambio automático para el recurso pueden desviar activamente el tráfico de una zona de disponibilidad. Por ejemplo, si inicia un cambio de zona para un recurso cuando se ha desviado en ese momento con el cambio automático, el cambio de zona tendrá prioridad. Para obtener más información, consulte Prioridad de los cambios zonales.

Identificador de recursos

El identificador de un recurso para el que se habilita el cambio automático zonal, que es el nombre de recurso de Amazon (ARN) del recurso. Solo puede habilitar el cambio automático zonal para los recursos de su cuenta que estén en un AWS servicio compatible con ARC.

Administrar recursos

Los balanceadores de carga de aplicaciones registran los recursos automáticamente con ARC para el cambio automático zonal. Debe habilitar manualmente otros recursos para el cambio automático zonal.

Nombre del recurso

El nombre de un recurso gestionado en ARC.

Estado aplicado

Un estado aplicado indica si un cambio de tráfico está en vigor para un recurso. Al configurar el cambio automático de zona, un recurso puede tener más de un cambio de tráfico activo, es decir, un cambio de zona de ejecución de práctica, un cambio de zona iniciado por el cliente o un cambio automático. Sin embargo, solo se aplica uno, es decir, está en vigor para el recurso a la vez. El cambio que tiene el estado `APPLIED` determina la zona de disponibilidad a la que se ha desviado el tráfico de la aplicación para un recurso y cuándo finaliza ese cambio de tráfico.

Tipo de turno

Define el tipo de cambio zonal. Los cambios zonales pueden tener uno de los siguientes tipos:

- ZONAL_SHIFT
- ZONAL_AUTOSHIFT
- PRACTICE_RUN
- FIS_EXPERIMENT

Planos de datos y control para el cambio automático zonal

Al planificar la conmutación por error y la recuperación ante desastres, tenga en cuenta la resistencia de sus mecanismos de conmutación por error. Le recomendamos que se asegure de que los mecanismos de los que depende durante la conmutación por error estén altamente disponibles, de modo que pueda utilizarlos cuando los necesite en caso de desastre. Por lo general, debería utilizar funciones de plano de datos para sus mecanismos siempre que pueda, a fin de obtener la máxima fiabilidad y tolerancia a los fallos. Teniendo esto en cuenta, es importante entender cómo se divide la funcionalidad de un servicio entre planos de control y planos de datos, y cuándo se puede confiar en una fiabilidad extrema con el plano de datos de un servicio.

En general, un plano de control permite realizar funciones de administración básicas, como crear, actualizar y eliminar recursos del servicio. Un plano de datos proporciona la funcionalidad principal de un servicio.

Para obtener más información sobre los planos de datos, los planos de control y cómo AWS se crean servicios para cumplir los objetivos de alta disponibilidad, consulte el artículo Static stability using Availability Zones en Amazon Builders' Library.

Precios del cambio automático zonal en ARC

En el caso del cambio automático zonal, AWS desplaza el tráfico de una zona de disponibilidad en su nombre para destinarlo a los recursos compatibles cuando AWS determine que existe un posible problema que pueda afectar negativamente a las aplicaciones de los clientes. No se aplican cargos adicionales por habilitar el cambio automático de zona.

Para obtener información detallada sobre los precios de ARC y ejemplos de precios, consulte los precios de ARC.

Mejores prácticas a la hora de configurar el cambio automático zonal

Tenga en cuenta las siguientes prácticas recomendadas y consideraciones al habilitar el cambio automático zonal en Amazon Application Recovery Controller (ARC).

El cambio automático zonal incluye dos tipos de cambios de tráfico: los cambios automáticos y los turnos zonales de práctica.

- Con el cambio automático, AWS ayuda a reducir el tiempo de recuperación al desviar el tráfico de recursos de las aplicaciones desde una zona de disponibilidad durante los eventos, en su nombre.
- En el caso de las sesiones de práctica, ARC inicia un turno zonal en su nombre o usted inicia una sesión de práctica en un turno zonal. En la AWS práctica, el cambio zonal desvía el tráfico de una zona de disponibilidad para dirigirse a un recurso y viceversa, siguiendo una cadencia semanal. Las ejecuciones de práctica le ayudan a asegurarse de que ha escalado verticalmente la capacidad suficiente para las zonas de disponibilidad de una región como para que su aplicación tolere la pérdida de una zona de disponibilidad.

Hay varias prácticas recomendadas y consideraciones que se deben tener en cuenta con los turnos automáticos y las sesiones de práctica. Revise los siguientes temas antes de habilitar un cambio automático de zona o configurar ejecuciones de práctica para un recurso.

Temas

- Limite el tiempo que los clientes permanecen conectados a sus terminales
- Redimensiona la capacidad de tus recursos y prueba los cambios de tráfico
- Tenga en cuenta los tipos y las restricciones de los recursos
- Especifique las alarmas para las sesiones de práctica
- Evalúe los resultados de las sesiones de práctica

Limite el tiempo que los clientes permanecen conectados a sus terminales

Cuando Amazon Application Recovery Controller (ARC) desvía el tráfico de una zona afectada, por ejemplo, mediante el cambio zonal o el cambio automático zonal, el mecanismo que utiliza ARC para mover el tráfico de las aplicaciones es una actualización del DNS. Una actualización del DNS provoca que todas las conexiones nuevas se dirijan lejos de la ubicación dañada. Sin embargo, los clientes con conexiones abiertas preexistentes pueden seguir realizando solicitudes a la ubicación dañada hasta que los clientes se vuelvan a conectar. Para garantizar

una recuperación rápida, le recomendamos que limite el tiempo que los clientes permanecen conectados a sus terminales.

Si usa un Application Load Balancer, puede usar la `keepalive` opción para configurar la duración de las conexiones. Le sugerimos que reduzca el `keepalive` valor para ajustarlo al objetivo de tiempo de recuperación de su aplicación, por ejemplo, 300 segundos. Al elegir una `keepalive` hora, tenga en cuenta que este valor es una compensación entre volver a conectarse con más frecuencia, en general, lo que puede afectar a la latencia, y alejar más rápidamente a todos los clientes de una zona de disponibilidad o región con problemas.

Para obtener más información sobre cómo configurar la `keepalive` opción para Application Load Balancer, consulte la duración del mantenimiento del cliente HTTP en la Guía del usuario del Application Load Balancer.

Redimensiona la capacidad de tus recursos y prueba los cambios de tráfico

Cuando se AWS desplaza el tráfico de una zona de disponibilidad a un cambio zonal o automático, es importante que las zonas de disponibilidad restantes puedan atender las crecientes tasas de solicitud de su recurso. Este patrón se conoce como estabilidad estática. Para obtener más información, consulte el documento técnico Estabilidad estática con zonas de disponibilidad en la Amazon Builder's Library.

Por ejemplo, si la aplicación necesita 30 instancias para atender a sus clientes, debe aprovisionar 15 instancias en tres zonas de disponibilidad, para un total de 45 instancias. De este modo, cuando el tráfico se AWS desplaza fuera de una zona de disponibilidad (con un cambio automático o durante una sesión de práctica),AWS podrá seguir atendiendo a los clientes de su aplicación con el total restante de 30 instancias, distribuidas en dos zonas de disponibilidad.

La función de cambio automático zonal de ARC le ayuda a recuperarse rápidamente de AWS los eventos ocurridos en una zona de disponibilidad cuando tiene una aplicación con recursos que están preescalados para funcionar con normalidad ante la pérdida de una zona de disponibilidad. Antes de habilitar el cambio automático de zona para un recurso, escale la capacidad del recurso en todas las zonas de disponibilidad configuradas de una Región de AWS. A continuación, inicie los cambios de zona del recurso para comprobar que la aplicación sigue funcionando con normalidad cuando el tráfico se desvíe de una zona de disponibilidad.

Después de realizar la prueba con cambios de zona, habilite el cambio automático de zona y configure las ejecuciones de práctica para los recursos de la aplicación. Realice sus propias simulaciones de práctica bajo demanda para asegurarse de que la configuración se escale correctamente. Las ejecuciones de práctica periódicas con cambio automático de zona le ayudan

a asegurarse, de forma continua, de que su capacidad sigue escalándose de forma adecuada. Con suficiente capacidad en todas las zonas de disponibilidad, la aplicación puede seguir atendiendo a los clientes, sin interrupciones, durante un cambio automático.

Para obtener más información sobre cómo iniciar un cambio de zona de un recurso, consulte Cambio zonal en ARC.

Tenga en cuenta los tipos y las restricciones de los recursos

El cambio automático de zona permite desviar el tráfico de una zona de disponibilidad de todos los recursos compatibles con el cambio de zona. En algunas situaciones específicas de recursos, el cambio automático de zona no desvía el tráfico de una zona de disponibilidad para un cambio automático.

Por ejemplo, si los grupos de destino del equilibrador de carga de las zonas de disponibilidad no tienen ninguna instancia o si todas las instancias tienen un estado incorrecto, el equilibrador de carga se encuentra en un estado de apertura por error. Si se AWS inicia un cambio automático para un balanceador de cargas en este escenario, el cambio automático no cambia las zonas de disponibilidad que usa el balanceador de cargas porque el balanceador de cargas ya está en un estado de apertura por error. Este es el comportamiento esperado. El cambio automático no puede provocar que una zona de disponibilidad esté en mal estado y desviar el tráfico a las demás zonas de disponibilidad Región de AWS si todas las zonas de disponibilidad se abren por error (en mal estado).

Para obtener más información sobre los recursos compatibles, incluidos todos los requisitos y excepciones que debe tener en cuenta, consulte Recursos admitidos.

Especifique las alarmas para las sesiones de práctica

Se configura al menos una alarma (la alarma de resultado) para las sesiones de práctica con cambio automático zonal. Opcionalmente, también puedes configurar una segunda alarma (la alarma de bloqueo).

Al considerar las CloudWatch alarmas que configura para las ejecuciones de práctica de su recurso, tenga en cuenta lo siguiente:

- Para la alarma de resultado, que es obligatoria, le recomendamos que configure una CloudWatch alarma para que pase a un `ALARM` estado en el que las métricas del recurso o de la aplicación indiquen que desplazar el tráfico fuera de la zona de disponibilidad afecta negativamente al rendimiento. Por ejemplo, puede determinar un umbral para las tasas de solicitud de un recurso y, a continuación, configurar una alarma para que pase a un estado de

ALARM cuando se supere dicho umbral. Es responsable de configurar una alarma adecuada que origine que AWS finalice la ejecución de práctica y devuelva un resultado de FAILED.

- Le recomendamos que siga el AWS Well Architected Framework, que recomienda implementar indicadores clave de rendimiento (KPIs) como CloudWatch alarmas. Si lo hace, puede usar estas alarmas para crear una alarma compuesta que sirva como desencadenador de seguridad y evitar que se inicien ejecuciones de práctica en el caso de que pudieran impedir que la aplicación no cumpliera con un KPI. Cuando la alarma deja de estar activaALARM, ARC inicia las sesiones de práctica la próxima vez que se programe una sesión de práctica para el recurso.
- Para la alarma de bloqueo de la práctica, si decide configurarla, puede optar por realizar un seguimiento de una métrica específica que utilice para indicar que no desea que comience una ejecución de AWS práctica.
- Para practicar la ejecución de alarmas, debe especificar el nombre de recurso de Amazon (ARN) para cada alarma, que primero debe configurar en Amazon. CloudWatch Las CloudWatch alarmas que especifique pueden ser alarmas compuestas, lo que le permitirá incluir varias métricas y comprobaciones para su aplicación y recurso que puedan activar la alarma para que pase a un ALARM estado. Para obtener más información, consulta Combinación de alarmas en la Guía del CloudWatch usuario de Amazon.
- Asegúrese de que las CloudWatch alarmas que especifique para las ejecuciones de práctica estén en la misma región que el recurso para el que está configurando una ejecución de práctica.

Evalúa los resultados de las sesiones de práctica

El ARC informa un resultado para cada sesión de práctica. Después de una sesión de práctica, evalúa el resultado y determina si necesitas tomar medidas. Por ejemplo, es posible que necesite ampliar la capacidad o ajustar la configuración de una alarma.

A continuación se muestran los posibles resultados de las ejecuciones de práctica:

- CORRECTO: la alarma de resultado no entró en ningún estado de ALARM durante la ejecución de práctica, y la ejecución de práctica llevó a cabo el periodo de prueba completo de 30 minutos.
- ERROR: la alarma de resultado entró en un estado de ALARM durante la ejecución de práctica.
- INTERRUMPIDA: la ejecución de práctica finalizó por un motivo distinto al de la alarma de resultado al entrar en un estado de ALARM. Una ejecución de práctica puede interrumpirse por varios motivos. Entre ellos, se incluyen los siguientes:

  - La práctica finalizó porque se AWS inició un cambio automático en la región Región de AWS o se produjo una situación de alarma en la región.
  - La ejecución de práctica finalizó porque se eliminó la configuración de la ejecución de práctica del recurso.
  - La ejecución de práctica finalizó porque se inició un cambio de zona iniciado por el cliente para el recurso en la zona de disponibilidad desde la que estaba desviando el tráfico el cambio de zona de ejecución de práctica.
  - La ejecución de práctica finalizó porque ya no se puede acceder a una CloudWatch alarma especificada para la configuración de la ejecución de práctica.
  - La ejecución de práctica finalizó porque la alarma de bloqueo especificada para la ejecución de práctica entró en un estado de `ALARM`.
  - La ejecución de práctica finalizó por un motivo desconocido.
  - La sesión de práctica finalizó porque se inició un cambio automático zonal con prioridad. Consulte Prioridad para ver los cambios zonales.
- CAPACITY_CHECK_FAILED: No se pudo comprobar la capacidad equilibrada entre las zonas de disponibilidad para los recursos del grupo de equilibrio de carga y Auto Scaling.
- PENDIENTE: la ejecución de práctica está activa (en curso). Aún no hay ningún resultado que mostrar.

Operaciones de la API de cambio automático de zona

En la siguiente tabla, se enumeran las operaciones de la API ARC que puede utilizar con el cambio automático zonal. Para ver ejemplos del uso de las operaciones de la API de cambio automático zonal con el, consulte. AWS CLI

Para ver ejemplos de cómo utilizar las operaciones habituales de la API de cambio automático de zona con la AWS Command Line Interface, consulte Ejemplos de uso del cambio AWS CLI automático zonal.

Acción	Uso de la consola ARC	Uso de la API ARC
Creación de una configuración de ejecución de práctica	Consulte Habilitar o deshabilitar el cambio automático de zona	Consulte CreatePracticeRunConfiguration.

Acción	Uso de la consola ARC	Uso de la API ARC
Eliminación de una configuración de ejecución de práctica	Consulte Configuración, modificación o eliminación de una configuración de ejecución de práctica	Consulte DeletePracticeRunConfiguration.
Enumeración de cambios automáticos	Consulte Cambio automático zonal en ARC	Consulte ListAutoshifts.
Enumeración de los recursos para el cambio automático de zona	Consulte Recursos admitidos	Consulte ListManagedResources.
Obtención de los recursos para el cambio automático de zona	Consulte Recursos admitidos	Consulte GetManagedResource.
Modificación de una configuración de ejecución de práctica	Consulte Configuración, modificación o eliminación de una configuración de ejecución de práctica	Consulte UpdatePracticeRunConfiguration.
Habilitar o deshabilitar el cambio automático de zona	Consulte Habilitar o deshabilitar el cambio automático de zona	Consulte UpdateZonalAutoshiftConfiguration.
Habilite o deshabilite la notificación de cambio automático al observador	Consulte Habilitar el cambio automático zonal y trabajar con él	Consulte UpdateAutoshiftObserverNotificationStatus.
Comienza una carrera de práctica	Consulte Al iniciar una sesión de práctica, realice un cambio zonal	Consulte StartPracticeRun.
Cancela una carrera de práctica	Consulte Cancelación de un cambio de zona de ejecución de práctica	Consulte CancelPracticeRun.

Ejemplos de uso del cambio AWS CLI automático zonal

En esta sección, se describen ejemplos de aplicaciones sencillas sobre cómo trabajar con el cambio automático zonal y cómo AWS Command Line Interface trabajar con la capacidad de cambio automático zonal de Amazon Application Recovery Controller (ARC) mediante operaciones de API. Los ejemplos están pensados para ayudarle a desarrollar una comprensión básica de cómo trabajar con el cambio automático zonal mediante la CLI.

El cambio automático zonal es una capacidad de ARC. Con el cambio automático zonal, usted autoriza AWS a desviar el tráfico de recursos de aplicaciones compatibles de una zona de disponibilidad durante los eventos, en su nombre, para reducir el tiempo de recuperación. Para obtener más información sobre los recursos que puede utilizar con el cambio automático zonal, consulte. Recursos admitidos

El cambio automático zonal incluye recorridos de práctica, que también alejan el tráfico de las zonas de disponibilidad, para ayudar a comprobar que los cambios automáticos son seguros para su aplicación.

Para obtener una lista de las acciones de la API de cambio automático de zona y enlaces a más información, consulte Operaciones de la API de cambio automático de zona. Para obtener más información sobre el uso del AWS CLI, consulte la AWS CLI Referencia de comandos.

Contenido

- Creación de una configuración de ejecución de práctica
- Habilitar o deshabilitar los cambios automáticos
- Inicie una sesión de práctica bajo demanda
- Cancelación de una ejecución de práctica en curso
- Cancelación de un cambio automático en curso
- Modificación de una configuración de ejecución de práctica
- Eliminación de una configuración de ejecución de práctica

Creación de una configuración de ejecución de práctica

Antes de habilitar el cambio automático de zona para un recurso, debe crear una configuración de ejecución de práctica para el recurso con el fin de elegir las opciones para las ejecuciones de práctica requeridas. Para crear una configuración de ejecución de práctica para un recurso con la CLI, utilice el comando `create-practice-run-configuration`.

Tenga en cuenta lo siguiente al crear una configuración de ejecución de práctica para un recurso:

- En este momento, el único tipo de alarma admitido es `CLOUDWATCH`.
- Debe utilizar alarmas que estén en el mismo lugar en el Región de AWS que está desplegado el recurso.
- Es necesario especificar una alarma de resultado. La especificación de una alarma de bloqueo es opcional.
- La especificación de fechas o ventanas bloqueadas es opcional.

Para crear una configuración de ejecución de práctica con la CLI, utilice el comando `create-practice-run-configuration`.

Por ejemplo, para crear una configuración de ejecución de práctica para un recurso, utilice un comando como el siguiente:

```
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"
        ]
}
```

Habilitar o deshabilitar los cambios automáticos

Para habilitar o deshabilitar los cambios automáticos de un recurso, actualice el estado del cambio automático de zona con la CLI. Para cambiar el estado del cambio automático de zona, utilice el comando `update-zonal-autoshift-configuration`.

Por ejemplo, para habilitar los cambios automáticos de un recurso, utilice un comando como el siguiente:

```
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"
}
```

Inicie una sesión de práctica bajo demanda

Puede iniciar un turno zonal de ejecución de práctica bajo demanda con la CLI mediante el `start-practice-run` comando.

Por ejemplo, para iniciar una ejecución de práctica de un recurso, utilice un comando como el siguiente:

```
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.",
}
```

Cancelación de una ejecución de práctica en curso

Puede cancelar una ejecución de práctica en curso con la CLI mediante el `cancel-practice-run` comando.

Por ejemplo, para cancelar una ejecución de práctica para un recurso, utilice un comando como el siguiente:

```
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"
}
```

Cancelación de un cambio automático en curso

Puede cancelar un cambio automático en curso con la CLI cancelando el cambio automático zonal del recurso. Para cancelar un cambio automático zonal, utilice el. `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"
}
```

Modificación de una configuración de ejecución de práctica

Puede editar la configuración de una ejecución de práctica de un recurso con la CLI para actualizar diferentes opciones de configuración, como cambiar las alarmas de las ejecuciones de práctica o actualizar las fechas o ventanas bloqueadas, cuando ARC no inicie las ejecuciones de práctica. Para modificar la configuración de una ejecución de práctica, utilice el comando `update-practice-run-configuration`.

Tenga en cuenta lo siguiente al modificar una configuración de ejecución de práctica para un recurso:

- En este momento, el único tipo de alarma admitido es `CLOUDWATCH`.
- Debe usar alarmas que estén en la misma ubicación en la Región de AWS que está desplegado el recurso.
- Es necesario especificar una alarma de resultado. La especificación de una alarma de bloqueo es opcional.
- La especificación de fechas o ventanas bloqueadas es opcional.
- Las fechas o ventanas bloqueadas que especifique sustituyen a los valores existentes.

Por ejemplo, para modificar una configuración de ejecución de práctica para un recurso con el fin de especificar una nueva fecha bloqueada, utilice un comando como el siguiente:

```
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"
       ]
}
```

Eliminación de una configuración de ejecución de práctica

Puede eliminar una configuración de ejecución de práctica para un recuso, pero, primero, debe deshabilitar el cambio automático de zona de dicho recurso. Se necesita un recurso para tener una configuración de ejecución de práctica para habilitar el cambio automático de zona. Las ejecuciones de práctica habituales le ayudan a asegurarse de que la aplicación puede ejecutarse con normalidad sin una zona de disponibilidad.

Para eliminar una configuración de ejecución de práctica mediante la CLI, primero, deshabilite el cambio automático de zona, si es necesario, mediante el comando `update-zonal-autoshift`. A continuación, para eliminar la configuración de ejecución de práctica, utilice el comando `delete-practice-run-configuration`.

En primer lugar, deshabilite el cambio automático de zona para el recurso mediante un comando como el siguiente:

```
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"
}
```

A continuación, elimine la configuración de ejecución de práctica con un comando como el siguiente:

```
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"
}
```

Habilitar el cambio automático zonal y trabajar con él

En esta sección se proporcionan los procedimientos para trabajar con cambios automáticos zonales en Amazon Application Recovery Controller (ARC). Después de activar el cambio automático zonal, puede realizar cambios en las configuraciones de las carreras de práctica, iniciar una carrera de práctica bajo demanda, cancelar un turno en curso, incluidas las carreras de práctica, o activar las notificaciones del observador de cambios automáticos.

Habilitar o deshabilitar el cambio automático de zona

En estos pasos se explica cómo activar o desactivar el cambio automático zonal en la consola Amazon Application Recovery Controller (ARC). Para trabajar con el cambio automático de zona de forma programática, consulte la Guía de referencia de la API del cambio de zona y del cambio automático de zona.

Cuando el cambio automático zonal está activado, usted autoriza AWS a desviar el tráfico de recursos de la aplicación desde una zona de disponibilidad durante los eventos, en su nombre, para reducir el tiempo de recuperación.

Para habilitar o deshabilitar el cambio automático de zona

1. Abra la consola ARC en. https://console.aws.amazon.com/route53recovery/home#/dashboard
2. En Multi-AZ, elija Cambio automático de zona.
3. En Configuraciones de cambio automático de zona de recursos, elija un recurso.
4. En el menú Acciones, selecciona Activar el cambio automático zonal y, a continuación, sigue los pasos para completar la actualización.

Si el recurso no tiene una configuración de ejecución de práctica, la opción Habilitar el cambio automático de zona no está disponible. Para configurar una configuración de ejecución de práctica y habilitar el cambio automático de zona, elija Configurar el cambio automático de zona.

Contenido

- Configuración, modificación o eliminación de una configuración de ejecución de práctica
- Cancelación de un cambio automático zonal
- Al iniciar una sesión de práctica, realice un cambio zonal
- Cancelación de un cambio de zona de ejecución de práctica
- Activar o desactivar la notificación de cambio automático al observador

Configuración, modificación o eliminación de una configuración de ejecución de práctica

En los pasos de esta sección se explica cómo editar o eliminar una configuración de ejecución de práctica en la consola Amazon Application Recovery Controller (ARC). Para trabajar con el cambio automático de zona de forma programática, incluidos los cambios en las configuraciones de ejecuciones de práctica, consulte la Guía de referencia de la API del cambio de zona y del cambio automático de zona.

Si elimina una configuración de ejecución de práctica de la consola, se deshabilitará el cambio automático de zona. Antes de eliminar una configuración de ejecución de práctica con una operación de la API, debe deshabilitar el cambio automático de zona. Puede configurar una ejecución de

práctica sin habilitar el cambio automático de zona. Sin embargo, para que el cambio automático de zona esté habilitado para un recurso, es necesario tener una ejecución de práctica configurada para el recurso.

Para configurar una ejecución de práctica

1. Abra la consola ARC enhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. En Multi-AZ, elija Cambio automático de zona.
3. Seleccione Configurar el cambio automático de zona.
4. Elija un recurso para configurar el cambio automático de zona.
5. Seleccione desactivar el cambio automático zonal si no quiere AWS iniciar un cambio automático para un recurso cuando se produce un evento. AWS Si lo desea, puede continuar con el asistente para configurar una configuración de ejecución de práctica sin habilitar los cambios automáticos.
6. Elija las opciones para las ejecuciones de práctica del recurso. En el caso de las alarmas, puede hacer lo siguiente:

   - (Obligatorio) Especifique una alarma de resultado para supervisar las ejecuciones de práctica de este recurso.
   - (Opcional) Especifique una alarma de bloqueo para las ejecuciones de práctica de este recurso.

   Para obtener más información, consulte la sección Alarmas que especifique para las ejecuciones de práctica en Mejores prácticas a la hora de configurar el cambio automático zonal.
7. También puede especificar fechas o periodos de tiempo bloqueados. Elige fechas o ventanas (días y horas) para impedir que ARC inicie las sesiones de práctica de este recurso. Todas las fechas y horas se indican en UTC.
8. Seleccione la casilla de verificación para confirmar que haya leído la nota de confirmación.
9. Seleccione Crear.

Para editar una configuración de ejecución de práctica

1. Abra la consola ARC enhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. En Multi-AZ, elija Cambio automático de zona.
3. En Configuraciones de cambio automático de zona de recursos, elija un recurso.

4. En el menú Acciones, seleccione Modificar la configuración de la ejecución de práctica.
5. Realice cambios en la configuración de la ejecución de la práctica para realizar una o varias de las siguientes acciones:

   - En el caso de las alarmas, puede hacer lo siguiente:
     - En la alarma de bloqueo, puede añadir una alarma, eliminarla o especificar otra alarma de bloqueo.
     - En el caso de la alarma de resultado que monitorea las sesiones de práctica, puede especificar una CloudWatch alarma diferente para utilizarla. Las alarmas de resultado son obligatorias, por lo que no puede eliminarlas.
   - En el caso de las fechas y los periodos de tiempo bloqueados, puede añadir nuevas fechas o días y horas, o puede eliminar o actualizar las fechas o días y horas existentes. Todas las fechas y horas se indican en UTC.
6. Seleccione Save.

Para eliminar una configuración de ejecución de práctica

1. Abra la consola ARC enhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. En Multi-AZ, elija Cambio automático de zona.
3. En Configuraciones de cambio automático de zona de recursos, elija un recurso.
4. En el menú Acciones, seleccione Eliminar la configuración de la ejecución de práctica.
5. En el cuadro de diálogo modal de confirmación, escriba `Delete` y elija Eliminar.

   Tenga en cuenta que al eliminar una configuración de ejecución de práctica en la consola también se deshabilitará el cambio automático de zona del recurso. El cambio automático de zona requiere que se configure una ejecución de práctica para el recurso.

Cancelación de un cambio automático zonal

Para detener un cambio automático zonal en curso para un recurso, debes cancelar el cambio automático zonal.

Para detener un cambio automático zonal en curso

1. Abra la consola ARC en. https://console.aws.amazon.com/route53recovery/home#/dashboard
2. En Multi-AZ, elija Cambio de zona.

3. Seleccione el cambio automático zonal que desee cancelar y, a continuación, elija Cancelar cambio zonal.
4. En el cuadro de diálogo de confirmación de modo, elija Confirmar.

Al iniciar una sesión de práctica, realice un cambio zonal

En los pasos de esta sección se explica cómo iniciar un cambio zonal de práctica bajo demanda en la consola ARC. Para trabajar con el cambio de zona y el cambio automático de zona de forma programática, consulte la Guía de referencia de la API del cambio de zona y del cambio automático de zona.

Puede iniciar un turno zonal de ensayo después de configurar el cambio automático zonal y crear una configuración de ensayo.

Para iniciar una práctica, ejecute un cambio zonal

1. Abra la consola ARC enhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. En Multi-AZ, elija Cambio automático de zona.
3. En Recursos de cambio automático zonal, busque un recurso individual que tenga configurado el cambio automático zonal.
4. En la página de descripción general de los recursos, elija Iniciar una carrera de práctica.
5. Seleccione una zona de disponibilidad y, a continuación, introduzca un comentario para la sesión de práctica. La sesión de práctica desviará el tráfico de la zona de disponibilidad que haya seleccionado.
6. Elija Iniciar.

Cancelación de un cambio de zona de ejecución de práctica

Los pasos de esta sección explican cómo cancelar un cambio zonal en la consola ARC. Para trabajar con el cambio de zona y el cambio automático de zona de forma programática, consulte la Guía de referencia de la API del cambio de zona y del cambio automático de zona.

Puedes cancelar los turnos zonales o las carreras de práctica que inicies tú mismo. También puedes cancelar los turnos zonales que AWS se inician con un recurso para una sesión de práctica con el cambio automático zonal.

Para cancelar un cambio de zona de ejecución de práctica

1. Abre la consola ARC en. https://console.aws.amazon.com/route53recovery/home#/dashboard
2. En Multi-AZ, elija Cambio de zona.
3. Seleccione el turno zonal de la carrera de práctica que desee cancelar y, a continuación, elija Cancelar cambio zonal o Cancelar carrera de práctica.
4. En el cuadro de diálogo de confirmación de modo, elija Confirmar.

Activar o desactivar la notificación de cambio automático al observador

Puedes configurar el cambio automático zonal para que te notifique, a través de Amazon EventBridge, cada vez que se AWS inicie un cambio automático para desviar el tráfico de una zona de disponibilidad potencialmente afectada. Debe configurar esta opción en cada una de Región de AWS las que desee recibir notificaciones. No es necesario configurar ningún recurso específico con el cambio automático zonal para habilitar estas notificaciones independientes. Para obtener más información, consulte Uso del cambio automático zonal con Amazon EventBridge.

En los pasos de esta sección se explica cómo activar la notificación de cambio automático a los observadores mediante la consola Amazon Application Recovery Controller (ARC). Para trabajar con el cambio automático de zona de forma programática, consulte la Guía de referencia de la API del cambio de zona y del cambio automático de zona.

Para activar o desactivar la notificación de cambio automático al observador

1. Abra la consola ARC enhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. En Primeros pasos, selecciona Activar la notificación al observador de cambios automáticos.
3. En el cuadro de diálogo de confirmación, selecciona Activar la notificación al observador.

Probando el cambio automático zonal con AWS FIS

Puede utilizarlos AWS Fault Injection Service para configurar y ejecutar experimentos que le ayuden a simular las condiciones del mundo real, como el escenario de disponibilidad de la zona de disponibilidad: interrupción del suministro eléctrico, en el que se demostrará lo que ocurre cuando se AWS inicia un cambio automático zonal en los recursos habilitados para el cambio automático durante una posible avería generalizada de la zona.

La acción de iniciar la `aws:arc:start-zonal-autoshift` recuperación le permite demostrar cómo AWS desplaza automáticamente el tráfico, en el caso de los recursos habilitados para el cambio automático zonal, de una zona de disponibilidad potencialmente dañada y lo redirige automáticamente a una zona AZs en buen estado Región de AWS durante la ejecución del escenario de disponibilidad de la zona de disponibilidad de la zona de disponibilidad.

Por ejemplo, puede utilizar la biblioteca de AWS FIS escenarios para simular una avería en la zona de disponibilidad provocada por una interrupción del suministro eléctrico. En este experimento, cinco minutos después de que comience la interrupción del suministro eléctrico en la zona de servicio, la acción de recuperación desvía `aws:arc:start-zonal-autoshift` automáticamente el tráfico de recursos de la zona de servicio especificada. El tráfico se desplaza durante los 25 minutos restantes de la interrupción del suministro eléctrico, a fin de demostrar cómo se activaría el cambio automático en caso de que se produjera un posible deterioro generalizado de la zona azotada. Cuando se complete el experimento, el turno de tráfico finaliza y el tráfico AZs vuelve a fluir hacia todas partes. Este proceso demuestra una recuperación completa tras un incidente de suministro eléctrico que afectó a una zona de servicio.

En qué se diferencian los experimentos de las sesiones de práctica de cambio automático zonal

AWS FIS Los experimentos se diferencian de las prácticas de cambio automático zonal en que, durante las prácticas, el ARC desplaza el tráfico del recurso fuera de una zona de disponibilidad como parte de un proceso normal para garantizar que la aplicación pueda tolerar la pérdida de una zona de disponibilidad. Sin embargo, durante un AWS FIS experimento, AWS FIS demuestra cómo se activarían en su nombre un cambio en la zona Z y un cambio automático para sus recursos habilitados para el cambio automático y, a continuación, cancela el cambio automático una vez resuelto el problema.

No se puede actualizar un cambio zonal iniciado por el AWS FIS mientras está en ejecución. Además, si cancelas un cambio zonal fuera de AWS FIS, el experimento finaliza. AWS FIS

AWS FIS mecanismo de seguridad basado en la caducidad

AWS FIS gestiona el cambio zonal mediante las operaciones StartZonalShiftUpdateZonalShift, y CancelZonalShiftAPI, con el `expiresIn` campo para estas solicitudes configurado en 1 minuto como mecanismo de seguridad. Esto permite AWS FIS revertir rápidamente el cambio zonal si se producen eventos inesperados, como interrupciones de la red o problemas con el sistema. En la consola ARC, aparecerá el campo de fecha de caducidad AWS FIS gestionada y la caducidad real

prevista viene determinada por la duración especificada en la acción de cambio zonal. Para obtener más información sobre las carreras de práctica, consulte Cómo funcionan los cambios automáticos zonales y las carreras de práctica

No se puede aplicar más de un cambio zonal a la vez. Es decir, solo una práctica consiste en ejecutar un cambio zonal, un cambio zonal iniciado por el cliente, un cambio automático o un experimento con el recurso. AWS FIS Cuando se inicia un segundo cambio zonal, el ARC sigue una prioridad para determinar qué tipo de cambio zonal está en vigor para un recurso. Para obtener más información sobre la prioridad de los cambios zonales, consulte. Prioridad de los cambios zonales

Para obtener más información sobre las acciones de AWS FIS recuperación, consulte la acción de AWS FIS recuperación en la Guía del AWS Fault Injection Service usuario.

Registro y supervisión del cambio automático zonal en Amazon Application Recovery Controller (ARC)

Puede usar AWS CloudTrail Amazon EventBridge para monitorear el cambio automático zonal en Amazon Application Recovery Controller (ARC), analizar patrones y ayudar a solucionar problemas.

Temas

- Registro de llamadas a la API de cambio automático zonal mediante AWS CloudTrail
- Uso del cambio automático zonal con Amazon EventBridge

Registro de llamadas a la API de cambio automático zonal mediante AWS CloudTrail

El cambio automático zonal para ARC está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en ARC. CloudTrail captura como eventos todas las llamadas a la API relacionadas con el cambio zonal. Las llamadas capturadas incluyen llamadas desde la consola ARC y llamadas en código a las operaciones de la API ARC para el cambio zonal.

Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos para el cambio zonal. Si no configura una ruta, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos.

Con la información recopilada por CloudTrail, puede determinar la solicitud de cambio zonal que se realizó a ARC, la dirección IP desde la que se realizó la solicitud, quién la hizo, cuándo se hizo y detalles adicionales.

Para obtener más información CloudTrail, consulte la Guía del AWS CloudTrail usuario.

Información sobre el cambio automático zonal en CloudTrail

CloudTrail está activado en tu cuenta Cuenta de AWS al crear la cuenta. Cuando se produce una actividad en ARC para el cambio automático zonal, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Puede ver, buscar y descargar eventos recientes en su. Cuenta de AWS Para obtener más información, consulte Trabajar con el historial de CloudTrail eventos.

Para obtener un registro continuo de los eventos en su entorno Cuenta de AWS, incluidos los eventos relacionados con el cambio automático zonal en ARC, cree un rastro. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las Regiones de AWS. La ruta registra los eventos de todas las regiones de la AWS partición y envía los archivos de registro al bucket de Amazon S3 que especifique. Además, puede configurar otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para más información, consulte los siguientes temas:

- Introducción a la creación de registros de seguimiento
- CloudTrail servicios e integraciones compatibles
- Configuración de las notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de CloudTrail registro de varias regiones y recibir archivos de CloudTrail registro de varias cuentas

Todas las acciones de ARC se registran CloudTrail y se documentan en la Guía de referencia de la API de control de enrutamiento para Amazon Application Recovery Controller. Por ejemplo, las llamadas a las `ListManagedResources` acciones `StartZonalShift` y las acciones generan entradas en los archivos de CloudTrail registro.

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con credenciales de usuario root o AWS Identity and Access Management (IAM).
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro AWS servicio.

Para obtener más información, consulte el elemento userIdentity de CloudTrail .

Visualización de los eventos ARC en el historial de eventos

CloudTrail le permite ver los eventos recientes en el historial de eventos. Para obtener más información, consulte Trabajar con el historial de CloudTrail eventos en la Guía del AWS CloudTrail usuario.

Descripción de las entradas de los archivos de registro de cambios automáticos zonales

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

En el siguiente ejemplo, se muestra una entrada de CloudTrail registro que muestra la `ListManagedResources` acción del cambio automático zonal.


```
{
      "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"
      }
    }
```

Uso del cambio automático zonal con Amazon EventBridge

Con Amazon EventBridge, puedes configurar reglas basadas en eventos que supervisen tus recursos de cambio automático zonales e inicien acciones específicas que usen otros servicios. AWS Por ejemplo, puede establecer una regla para el envío de notificaciones por correo electrónico señalando un tema de Amazon SNS cuando comience una sesión de práctica para el cambio automático zonal.

Puedes crear reglas en Amazon EventBridge para actuar en el cambio automático zonal. Un evento de cambio automático zonal especifica la información de estado de las carreras de práctica o los cambios automáticos, por ejemplo, cuando se inicia una carrera de práctica. Puede configurar el cambio automático zonal para que le notifique los eventos de cambio automático zonal en el caso de los recursos que habilite para el servicio.

También puede optar por activar, además de otras notificaciones o en lugar de ellas, la notificación al observador del cambio automático, que proporciona un evento de notificación cada vez que se AWS inicia un cambio automático en una zona de disponibilidad potencialmente afectada. La notificación al observador de cambios automáticos es independiente de las notificaciones que recibe cuando el tráfico de los recursos que ha activado para el cambio automático zonal se aleja de una zona de disponibilidad. No necesita configurar ningún recurso con el cambio automático zonal para habilitar la notificación al observador del cambio automático. Para obtener más información, consulte [Habilitar el cambio automático zonal y trabajar con él](#).

Para capturar eventos de cambio automático zonal específicos que le interesen, defina patrones específicos de eventos que EventBridge pueda utilizar para detectarlos. Los patrones de eventos de tienen la misma estructura que los eventos con los que coinciden. El patrón cita los campos para los que se desea encontrar coincidencias y proporciona los valores que está buscando.

Los eventos se emiten en la medida de lo posible. Se envían desde ARC a prácticamente en tiempo real, EventBridge en circunstancias operativas normales. Sin embargo, pueden surgir situaciones que retrasen o impidan la entrega de un evento.

Para obtener información sobre cómo funcionan EventBridge las reglas con los patrones de eventos, consulte Eventos y patrones de eventos en EventBridge.

Supervise un recurso de cambio automático zonal con EventBridge

Con él EventBridge, puede crear reglas que definan las acciones que se deben tomar cuando ARC emita eventos para sus recursos. Por ejemplo, puede crear una regla que envíe un mensaje de correo electrónico cuando comience una sesión de práctica para el cambio automático zonal.

Para escribir o copiar y pegar un patrón de eventos en la EventBridge consola, selecciona la opción de usar Introducir mi propia opción en la consola. Para ayudarle a determinar los patrones de eventos que podrían serle útiles, en este tema se incluyen ejemplos de patrones de coincidencia de eventos de cambio automático zonal y eventos de cambio automático zonal que puede utilizar.

Para crear una regla para un evento de recurso, realice lo siguiente:

1. Abre la EventBridge consola de Amazon en https://console.aws.amazon.com/events/.
2. Elige la región en la Región de AWS que quieres crear la regla, es decir, la región desde la que te interesa ver los eventos.
3. Seleccione Creación de regla.
4. Ingrese un Name (Nombre) para la regla y opcionalmente, una descripción.
5. Para Bus de eventos, deje el valor predeterminado, predeterminado.
6. Elija Siguiente.
7. En el paso Crear un patrón de eventos, en Origen del evento, deje el valor predeterminado, Eventos de AWS .
8. En Ejemplo de evento, elija Introducir el mío.
9. Para Ejemplos de eventos, escriba o copie y pegue un patrón de eventos.

Ejemplos de patrones de eventos de cambio automático zonal

Los patrones de eventos tienen la misma estructura que los eventos con los que coinciden. El patrón cita los campos para los que se desea encontrar coincidencias y proporciona los valores que está buscando.

Puede copiar y pegar los patrones de eventos de esta sección EventBridge para crear reglas que pueda usar para supervisar las acciones y los recursos del cambio automático zonal.

Al crear patrones de eventos para eventos de cambio automático de zona, puede especificar cualquiera de las siguientes opciones para el `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`

Cuando se interrumpe una ejecución de práctica, consulte el campo `additionalFailureInfo` para obtener más información sobre lo que ha provocado la interrupción.

Puede elegir monitorizar todos los AWS cambios automáticos activando las notificaciones del observador de cambios automáticos. Tras activar la notificación al observador del cambio automático, para recibir las notificaciones, elija que se le notifique según el tipo de detalle del cambio automático zonal. `Autoshift In Progress` Para ver los pasos para activar la notificación al observador del cambio automático, consulte. Habilitar el cambio automático zonal y trabajar con él

Para ver ejemplos, consulte la sección Ejemplos de eventos de cambio automático zonal.

- Seleccione todos los eventos del cambio automático zonal en los que se haya iniciado un cambio automático.

  Tenga en cuenta lo siguiente:

- Si tiene habilitada la notificación al observador del cambio automático, ARC devuelve todos los eventos del cambio automático.
- Si no tiene habilitada la notificación al observador de cambios automáticos, ARC devuelve los eventos de cambio automático solo cuando un recurso que haya configurado para el cambio automático zonal está incluido en un cambio automático.

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

- Seleccione todos los eventos del cambio automático zonal en los que se haya iniciado una sesión de práctica.

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

- Seleccione todos los eventos del cambio automático zonal en los que se haya fallado una carrera de práctica.

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

Ejemplo de eventos de cambio automático zonal

En esta sección se incluyen ejemplos de eventos de acciones de cambio automático zonal.

El siguiente es un ejemplo de un evento de la `Autoshift In Progress` acción, cuando 1) la notificación al observador del cambio automático está habilitada y 2) no se ha configurado un recurso con el cambio automático zonal que esté incluido en un cambio automático:

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

El siguiente es un ejemplo de un evento de la `Autoshift In Progress` acción, cuando 1) la notificación al observador de cambios automáticos está deshabilitada y 2) se ha configurado un recurso con cambio automático zonal que se incluye en un cambio automático:

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

El siguiente es un ejemplo de evento de la acción: `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"
        }
    }
}
```

El siguiente es un ejemplo de evento de la `FIS Experiment Autoshift In Progress` acción:

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

Especifique un grupo de CloudWatch registros para usarlo como objetivo

Al crear una EventBridge regla, debe especificar el destino al que se envían los eventos que coinciden con la regla. Para obtener una lista de los objetivos disponibles EventBridge, consulte Objetivos disponibles en la EventBridge consola. Uno de los destinos que puedes añadir a una EventBridge regla es un grupo de CloudWatch registros de Amazon. En esta sección se describen los requisitos para añadir grupos de CloudWatch registros como objetivos y se proporciona un procedimiento para añadir un grupo de registros al crear una regla.

Para agregar un grupo de CloudWatch registros como destino, puede realizar una de las siguientes acciones:

- Cree un nuevo grupo de registros
- Elija un grupo de registros existente

Si especifica un nuevo grupo de registros mediante la consola al crear una regla, crea EventBridge automáticamente el grupo de registros. Asegúrese de que el grupo de registros que utilice como destino para la EventBridge regla comience por`/aws/events`. Si desea elegir un grupo de registros existente, tenga en cuenta que solo los grupos de registros que comiencen por `/aws/events` aparecen como opciones en el menú desplegable. Para obtener más información, consulta Crear un nuevo grupo de registros en la Guía del CloudWatch usuario de Amazon.

Si crea o usa un grupo de CloudWatch registros para usarlo como destino mediante CloudWatch operaciones fuera de la consola, asegúrese de configurar los permisos correctamente. Si usa la consola para agregar un grupo de registros a una EventBridge regla, la política basada en recursos del grupo de registros se actualiza automáticamente. Sin embargo, si usa el SDK AWS Command Line Interface o un AWS SDK para especificar un grupo de registros, debe actualizar la política basada en recursos para el grupo de registros. El siguiente ejemplo de política ilustra los permisos que debe definir en una política basada en recursos para el grupo de registros:

```
{
  "Statement": [
    {
      "Action": [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "events.amazonaws.com",
          "delivery.logs.amazonaws.com"
        ]
      },
      "Resource": "arn:aws:logs:region:account:log-group:/aws/events/*:*",
      "Sid": "TrustEventsToStoreLogEvent"
    }
  ],
  "Version": "2012-10-17"
}
```

No puede configurar una política basada en recursos para un grupo de registros mediante la consola. Para añadir los permisos necesarios a una política basada en recursos, utilice la operación de API. CloudWatch PutResourcePolicy A continuación, puede utilizar el comando describe-resource-policiesCLI para comprobar que la política se ha aplicado correctamente.

Para crear una regla para un evento de recurso y especificar un objetivo de grupo de CloudWatch registros

1. Abre la EventBridge consola de Amazon en https://console.aws.amazon.com/events/.
2. Elige en Región de AWS qué quieres crear la regla.

3. Seleccione Crear regla y, a continuación, introduzca cualquier información sobre esa regla, como el patrón de eventos o los detalles de la programación.

   Para obtener más información sobre la creación de EventBridge reglas para ARC, consulte las secciones anteriores de este tema.
4. En la página Seleccionar destino, elija CloudWatchcomo objetivo.
5. Elija un grupo de CloudWatch registros en el menú desplegable.

Identity and Access Management para el cambio automático zonal en ARC

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a los recursos. AWS Los administradores de IAM controlan quién puede autenticarse (iniciar sesión) y quién puede autorizarse (tener permisos) para usar los recursos de ARC. La IAM es una Servicio de AWS opción que puede utilizar sin coste adicional.

Contenido

- Cómo funciona el cambio automático zonal en ARC con IAM
- Ejemplos de políticas basadas en la identidad para el cambio automático zonal en ARC
- Uso de la función vinculada al servicio para el cambio automático zonal en ARC
- AWS políticas gestionadas para el cambio automático zonal en ARC

Cómo funciona el cambio automático zonal en ARC con IAM

Antes de usar IAM para gestionar el acceso al cambio automático zonal en Amazon Application Recovery Controller (ARC), infórmese sobre las funciones de IAM disponibles para su uso con el cambio automático zonal.

Funciones de IAM que puede utilizar con el cambio automático zonal en ARC

Característica de IAM	Soporte de cambio automático zonal
Políticas basadas en identidades	Sí
Políticas basadas en recursos	No
Acciones de políticas	Sí

Característica de IAM	Soporte de cambio automático zonal
Recursos de políticas	Sí
Claves de condición de política	Sí
ACLs	No
ABAC (etiquetas en políticas)	Parcial
Credenciales temporales	Sí
Permisos de entidades principales	Sí
Roles de servicio	No
Roles vinculados al servicio	Sí

Para obtener una visión general y de alto nivel del funcionamiento de AWS los servicios con la mayoría de las funciones de IAM, consulte AWS los servicios que funcionan con IAM en la Guía del usuario de IAM.

Políticas de ARC basadas en la identidad

Compatibilidad con las políticas basadas en identidad: sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está asociada. Para obtener más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de las políticas de JSON de IAM en la Guía del usuario de IAM.

Para ver ejemplos de políticas de ARC basadas en la identidad, consulte. Ejemplos de políticas basadas en identidad en Amazon Application Recovery Controller (ARC)

Políticas basadas en recursos dentro de ARC

Admite políticas basadas en recursos: no

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico.

Acciones políticas para ARC

Compatibilidad con las acciones de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Las acciones políticas suelen tener el mismo nombre que la operación de AWS API asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de acciones de ARC para el cambio automático zonal, consulte Acciones definidas por Amazon Route 53 Zonal Shift en la Referencia de autorización de servicio.

Las acciones políticas de ARC para el cambio automático zonal utilizan los siguientes prefijos antes de la acción:

```
arc-zonal-shift
```

Para especificar varias acciones en una única instrucción, sepárelas con comas. Por ejemplo, los siguientes:

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

```
      "arc-zonal-shift:action2"
         ]
```

Puede utilizar caracteres comodín (*) para especificar varias acciones . Por ejemplo, para especificar todas las acciones que comiencen con la palabra `Describe`, incluya la siguiente acción:

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

Para ver ejemplos de políticas ARC basadas en la identidad para el cambio automático zonal, consulte. Ejemplos de políticas basadas en la identidad para el cambio automático zonal en ARC

Recursos de políticas para el cambio automático zonal en ARC

Compatibilidad con los recursos de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puedes realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puedes hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utiliza un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

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

Para ver una lista de los tipos de recursos y sus acciones ARNs, así como las acciones que puede especificar con el ARN de cada recurso, consulte el tema siguiente en la Referencia de autorización de servicios:

- Acciones definidas por Amazon Route 53 - Zonal Shift

Para ver las acciones y los recursos que puede utilizar con una clave de condición, consulte el siguiente tema en la Referencia de autorización de servicio:

- Claves de condición definidas por Amazon Route 53 - Zonal Shift

Para ver ejemplos de políticas ARC basadas en la identidad para el cambio automático zonal, consulte. Ejemplos de políticas basadas en la identidad para el cambio automático zonal en ARC

Claves de condición de la política para el cambio automático zonal en ARC

Compatibilidad con claves de condición de políticas específicas del servicio: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puedes realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puedes crear expresiones condicionales que utilizan operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación `AND` lógica. Si especifica varios valores para una única clave de condición, AWS evalúa la condición mediante una `OR` operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puedes utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puedes conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para más información, consulta Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

Para ver una lista de las claves de condición ARC para el cambio automático zonal, consulte los siguientes temas en la Referencia de autorización de servicio:

- Claves de condición del cambio de zona de Amazon Route 53

Para ver las acciones y los recursos que puede usar con una clave de condición, consulte los siguientes temas de la Referencia de autorización de servicio:

- Acciones definidas por el cambio de zona de Amazon Route 53

Para ver ejemplos de políticas ARC basadas en la identidad para el cambio automático zonal, consulte. Ejemplos de políticas basadas en la identidad para el cambio automático zonal en ARC

Listas de control de acceso () en ARC ACLs

Soporta ACLs: No

Las listas de control de acceso (ACLs) controlan qué directores (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLs son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Control de acceso basado en atributos (ABAC) con ARC

Compatibilidad con ABAC (etiquetas en las políticas): parcial

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos. En AWS, estos atributos se denominan etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a muchos AWS recursos. El etiquetado de entidades y recursos es el primer paso de ABAC. A continuación, designa las políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso al que se intenta acceder.

ABAC es útil en entornos que crecen con rapidez y ayuda en situaciones en las que la administración de las políticas resulta engorrosa.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte Definición de permisos con la autorización de ABAC en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

El cambio automático zonal de ARC incluye la siguiente compatibilidad parcial con ABAC:

- El cambio automático zonal es compatible con ABAC para los recursos gestionados que están registrados en ARC para el cambio zonal. Para obtener más información sobre los recursos gestionados de ABAC para Equilibrador de carga de red y Equilibrador de carga de aplicación, consulte ABAC con Elastic Load Balancing en la Guía del usuario de Elastic Load Balancing.

Uso de credenciales temporales con ARC

Compatibilidad con credenciales temporales: sí

Algunas Servicios de AWS no funcionan cuando inicias sesión con credenciales temporales. Para obtener información adicional, incluida información sobre cuáles Servicios de AWS funcionan con credenciales temporales, consulta Cómo Servicios de AWS funcionan con IAM en la Guía del usuario de IAM.

Utiliza credenciales temporales si inicia sesión en ellas AWS Management Console mediante cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accedes AWS mediante el enlace de inicio de sesión único (SSO) de tu empresa, ese proceso crea automáticamente credenciales temporales. También crea credenciales temporales de forma automática cuando inicia sesión en la consola como usuario y luego cambia de rol. Para obtener más información sobre el cambio de roles, consulte Cambio de un usuario a un rol de IAM (consola) en la Guía del usuario de IAM.

Puedes crear credenciales temporales manualmente mediante la AWS CLI API o. AWS A continuación, puede utilizar esas credenciales temporales para acceder AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para obtener más información, consulte Credenciales de seguridad temporales en IAM.

Permisos principales entre servicios para ARC

Admite sesiones de acceso directo (FAS): sí

Cuando utiliza una entidad de IAM (usuario o rol) para realizar acciones en ella AWS, se le considera principal. Las políticas conceden permisos a una entidad principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. En este caso, debe tener permisos para realizar ambas acciones.

Para ver si una acción requiere acciones dependientes adicionales en una política, consulte el siguiente tema en la Referencia de autorización de servicios:

- Cambio de zona de Amazon Route 53

Funciones de servicio para ARC

Compatible con roles de servicio: No

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

Funciones vinculadas al servicio para ARC

Admite roles vinculados a servicios: sí

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Para obtener más información sobre la creación o administración de funciones vinculadas al servicio de ARC, consulte. Uso de la función vinculada al servicio para el cambio automático zonal en ARC

Para más información sobre cómo crear o administrar roles vinculados a servicios, consulta Servicios de AWS que funcionan con IAM. Busque un servicio en la tabla que incluya `Yes` en la columna Rol vinculado a un servicio. Seleccione el vínculo Sí para ver la documentación acerca del rol vinculado a servicios para ese servicio.

Ejemplos de políticas basadas en la identidad para el cambio automático zonal en ARC

De forma predeterminada, los usuarios y los roles no tienen permiso para crear o modificar los recursos de ARC. Tampoco pueden realizar tareas mediante la AWS Management Console, AWS Command Line Interface (AWS CLI) o la AWS API. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puedes añadir las políticas de IAM a roles y los usuarios puedes asumirlos.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM (consola) en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos por ARC, incluido el ARNs formato de cada uno de los tipos de recursos, consulte Acciones, recursos y claves de condición de Amazon Application Recovery Controller (ARC) en la Referencia de autorización de servicios.

Temas

- Prácticas recomendadas sobre las políticas
- Ejemplo: acceso zonal a la consola de cambio automático
- Ejemplos: acciones de la API ARC

Prácticas recomendadas sobre las políticas

Las políticas basadas en la identidad determinan si alguien puede crear, eliminar o acceder a los recursos de ARC de su cuenta. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulta las políticas administradas por AWS o las políticas administradas por AWS para funciones de tarea en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulta Políticas y permisos en IAM en la Guía del usuario de IAM.
- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo AWS CloudFormation. Para obtener más información, consulta Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.

- Utiliza el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Validación de políticas con el Analizador de acceso de IAM en la Guía del usuario de IAM.
- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para exigir la MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para más información, consulte Acceso seguro a la API con MFA en la Guía del usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Ejemplo: acceso zonal a la consola de cambio automático

Para acceder a la consola Amazon Application Recovery Controller (ARC), debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre los recursos ARC de su propiedad Cuenta de AWS. Si crea una política basada en identidades que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

No es necesario que concedas permisos mínimos de consola a los usuarios que solo realicen llamadas a la API AWS CLI o a la AWS API. En su lugar, permite el acceso únicamente a las acciones que coincidan con la operación de API que intentan realizar.

Para realizar algunas tareas, los usuarios deben tener permiso para crear el rol vinculado al servicio que está asociado al cambio automático zonal en ARC. Para obtener más información, consulte Uso de la función vinculada al servicio para el cambio automático zonal en ARC.

Para que los usuarios tengan acceso total al uso del cambio automático zonal en el AWS Management Console, adjunte al usuario una política como la siguiente:

```
{
    "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": "*"
        }
    ]
}
```

Ejemplos: acciones de la API ARC

Puede utilizar una política para garantizar que un usuario pueda utilizar las acciones de la API ARC para el cambio automático zonal a fin de configurar el cambio automático zonal de forma que AWS desvíe el tráfico de recursos de las aplicaciones de una zona de disponibilidad, por su parte, a uno AZs en buen estado, a fin de reducir el Región de AWS tiempo de recuperación durante los eventos. Para proporcionar estos permisos, adjunta una política que corresponda a las operaciones de la API con las que el usuario debe trabajar, tal y como se describe a continuación.

Para realizar algunas tareas, los usuarios deben tener permisos para el rol vinculado al servicio asociado a ARC. Los permisos necesarios para crear el rol vinculado al servicio se incluyen en el siguiente ejemplo de política. Para obtener más información, consulte Uso de la función vinculada al servicio para el cambio automático zonal en ARC.

Para trabajar con las operaciones de la API para el cambio automático zonal, adjunte al usuario una política como la siguiente:

```
{
    "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" : "*"
        }
    ]
}
```

Uso de la función vinculada al servicio para el cambio automático zonal en ARC

El cambio automático zonal en Amazon Application Recovery Controller utiliza una función vinculada a un AWS Identity and Access Management servicio (IAM). Un rol vinculado a un servicio es un tipo único de rol de IAM que está vinculado directamente a un servicio, en este caso, ARC. ARC predefine la función vinculada al servicio e incluye todos los permisos que el servicio requiere para llamar a otros AWS servicios en su nombre con fines específicos.

Un rol vinculado a un servicio facilita la configuración de ARC, ya que no es necesario añadir manualmente los permisos necesarios. ARC define los permisos para la función vinculada al servicio y, a menos que se defina lo contrario, solo ARC puede asumir sus funciones. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se pueda asociar a ninguna otra entidad de IAM.

Solo puede eliminar un rol vinculado a servicios después de eliminar sus recursos relacionados. Esto protege sus recursos de cambio automático zonal de ARC porque no puede eliminar inadvertidamente el permiso de acceso a los recursos.

Para obtener información sobre otros servicios que admiten funciones vinculadas a servicios, consulte AWS Servicios que funcionan con IAM y busque los servicios que tengan la palabra Sí en la columna Función vinculada a servicios. Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado a servicios en cuestión.

Permisos de rol vinculados al servicio para AWSService RoleForZonalAutoshiftPracticeRun

ARC usa el rol vinculado al servicio denominado AWSServiceRoleForZonalAutoshiftPracticeRunpara hacer lo siguiente:

- Supervise las CloudWatch alarmas de Amazon y los AWS Health Dashboard eventos de los clientes proporcionados por los clientes para las sesiones de práctica
- Gestionar las ejecuciones de práctica (cambios de zona de práctica)

En esta sección se describen los permisos del rol vinculado al servicio y la información sobre cómo crear, editar y eliminar el rol.

Permisos de rol vinculados al servicio para AWSService RoleForZonalAutoshiftPracticeRun

Este rol vinculado al servicio utiliza la política administrada `AWSZonalAutoshiftPracticeRunSLRPolicy`.

El rol vinculado a servicio de AWSServiceRoleForZonalAutoshiftPracticeRun confía en el siguiente servicio para asumir el rol:

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

Para ver los permisos de esta política, consulte AWSZonalAutoshiftPracticeRunSLRPolicy en la Referencia de la política administrada de AWS .

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Crear el rol AWSServiceRoleForZonalAutoshiftPracticeRunvinculado al servicio para ARC

No necesita crear manualmente el rol vinculado al servicio AWSServiceRoleForZonalAutoshiftPracticeRun. Al crear la configuración de la primera ejecución práctica en el AWS Management Console, el o un AWS SDK AWS CLI, ARC crea automáticamente el rol vinculado al servicio.

Si elimina este rol vinculado a servicios y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Al crear la configuración de la primera ejecución práctica, ARC vuelve a crear el rol vinculado al servicio automáticamente.

Edición del rol vinculado al AWSServiceRoleForZonalAutoshiftPracticeRunservicio para ARC

ARC no permite editar el rol vinculado al AWSServiceRoleForZonalAutoshiftPracticeRunservicio. Después de crear un rol vinculado al servicio, no podrá cambiar el nombre del rol, ya que otras entidades podrían hacer referencia a él. Sin embargo, puede editar la descripción del rol mediante IAM. Para obtener más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM.

Eliminar el rol vinculado al AWSServiceRoleForZonalAutoshiftPracticeRunservicio para ARC

Si ya no necesita usar una característica o servicio que requieran un rol vinculado a un servicio, le recomendamos que elimine dicho rol. Así no tendrá una entidad no utilizada que no se supervise ni mantenga de forma activa. Sin embargo, debe limpiar los recursos de un rol vinculado a un servicio antes de eliminarlo manualmente.

Una vez que haya desactivado el cambio automático, podrá eliminar el rol vinculado al AWSServiceRoleForZonalAutoshiftPracticeRunservicio. Para obtener más información sobre la capacidad de cambio automático, consulte Cambio zonal en ARC.

> **Note**
>
> Si el servicio ARC utiliza la función al intentar eliminar los recursos, es posible que no se pueda eliminar la función de servicio. En tal caso, espere unos minutos e intente eliminar de nuevo el rol.

Para eliminar manualmente el rol vinculado a servicios mediante IAM

Utilice la consola de IAM AWS CLI, la o la AWS API para eliminar la función vinculada al AWSService RoleForZonalAutoshiftPracticeRun servicio. Para obtener más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

Actualizaciones del rol ARC vinculado al servicio para el cambio automático zonal

Para ver las actualizaciones de las políticas AWS administradas para las funciones vinculadas al servicio de ARC, consulte la tabla de actualizaciones de políticas AWS administradas de ARC. También puede suscribirse a las alertas RSS automáticas en la página del historial del documento ARC.

AWS políticas gestionadas para el cambio automático zonal en ARC

Una política AWS administrada es una política independiente creada y administrada por AWS. AWS Las políticas administradas están diseñadas para proporcionar permisos para muchos casos de uso comunes, de modo que pueda empezar a asignar permisos a usuarios, grupos y funciones.

Ten en cuenta que es posible que las políticas AWS administradas no otorguen permisos con privilegios mínimos para tus casos de uso específicos, ya que están disponibles para que los usen todos los AWS clientes. Se recomienda definir políticas administradas por el cliente específicas para sus casos de uso a fin de reducir aún más los permisos.

No puedes cambiar los permisos definidos en AWS las políticas administradas. Si AWS actualiza los permisos definidos en una política AWS administrada, la actualización afecta a todas las identidades principales (usuarios, grupos y roles) a las que está asociada la política. AWS es más probable que actualice una política AWS administrada cuando Servicio de AWS se lance una nueva o cuando estén disponibles nuevas operaciones de API para los servicios existentes.

Para obtener más información, consulte Políticas administradas de AWS en la Guía del usuario de IAM.

AWS política gestionada: AWSZonal AutoshiftPracticeRun SLRPolicy

No puede asociar `AWSZonalAutoshiftPracticeRunSLRPolicy` a sus entidades IAM. Esta política está asociada a un rol vinculado a un servicio que permite a Amazon Application Recovery Controller (ARC) hacer lo siguiente para el cambio automático zonal:

- Supervise las CloudWatch alarmas de Amazon y los AWS Health Dashboard eventos de los clientes proporcionados por los clientes para las sesiones de práctica
- Gestionar las ejecuciones de práctica (cambios de zona de práctica)
- Gestione controles de capacidad equilibrados para las sesiones de práctica y los turnos automáticos

Para obtener más información, consulte Uso de la función vinculada al servicio para el cambio automático zonal en ARC.

Actualizaciones de las políticas AWS gestionadas para el cambio automático zonal

Para obtener más información sobre las actualizaciones de las políticas AWS gestionadas para el cambio automático zonal en ARC desde que este servicio comenzó a realizar el seguimiento de estos cambios, consulte. Actualizaciones de las políticas AWS gestionadas de Amazon Application Recovery Controller (ARC) Para recibir alertas automáticas sobre los cambios en esta página, suscríbase a la fuente RSS de la página del historial de documentos de ARC.

Utilice el control de enrutamiento para recuperar aplicaciones multirregionales en ARC

En esta sección, se explica cómo utilizar la capacidad de control de enrutamiento de Amazon Application Recovery Controller (ARC) para minimizar las interrupciones y ayudar a proporcionar continuidad a los usuarios cuando se implementa una AWS aplicación en varias Regiones de AWS.

También puede obtener información sobre la comprobación de disponibilidad, una función de ARC que puede utilizar para obtener información sobre si sus aplicaciones y recursos están preparados para la recuperación.

Los temas de esta sección describen las capacidades de control de enrutamiento y verificación de disponibilidad, cómo configurarlas y cómo usarlas.

Temas

- Control de enrutamiento en ARC
- Verificación de disponibilidad en ARC
- Conmutador de región en ARC

Control de enrutamiento en ARC

Para conmutar por error el tráfico a réplicas de aplicaciones en varias Regiones de AWS, puede utilizar los controles de enrutamiento de Amazon Application Recovery Controller (ARC) que están integrados con un tipo específico de comprobación de estado en Amazon Route 53. Los controles de enrutamiento son simples conmutadores de encendido/apagado que le permiten cambiar el tráfico de sus clientes de una réplica regional a otra. El redireccionamiento del tráfico se realiza mediante comprobaciones de estado del control de enrutamiento que se configuran con los registros DNS de Amazon Route 53. Por ejemplo, los registros de conmutación por error del DNS, asociados a los nombres de dominio que encabezan las réplicas de las aplicaciones en cada región.

En esta sección se explica cómo funciona el control de enrutamiento, cómo configurar los componentes de control de enrutamiento y cómo usarlos para redirigir el tráfico para la conmutación por error.

Los componentes de control de enrutamiento de ARC son: clústeres, paneles de control, controles de enrutamiento y comprobaciones de estado del control de enrutamiento. Todos los controles

de enrutamiento se agrupan en paneles de control. Puede agruparlos en el panel de control predeterminado que ARC crea para su clúster o crear sus propios paneles de control personalizados. Debe crear un clúster antes de crear un panel de control o un control de enrutamiento. Cada clúster de ARC es un plano de datos compuesto por cinco Regiones de AWS puntos finales.

Después de crear los controles de enrutamiento y las comprobaciones de estado del control de enrutamiento, puede crear reglas de seguridad para el control de enrutamiento a fin de evitar los efectos secundarios involuntarios de la automatización de la recuperación. Puede actualizar los estados del control de enrutamiento para redirigir el tráfico, de forma individual o por lotes, mediante las acciones de la AWS CLI API (recomendadas) o mediante las. AWS Management Console

En esta sección se explica cómo funcionan los controles de enrutamiento y cómo crearlos y usarlos para redirigir el tráfico de su aplicación.

> **Important**
>
> Para obtener información sobre cómo prepararse para usar ARC para redirigir el tráfico como parte de un plan de conmutación por error para su aplicación en caso de desastre, consulte. Mejores prácticas para el control de enrutamiento en ARC

Acerca del control de enrutamiento

El control de enrutamiento redirige el tráfico mediante comprobaciones de estado en Amazon Route 53 que se configuran con registros de DNS asociados al recurso de nivel superior de las celdas del grupo de recuperación, como, por ejemplo, un equilibrador de carga de Elastic Load Balancing. Puede redirigir el tráfico de una celda a otra, por ejemplo, actualizando un estado de control de enrutamiento a `Off` (para detener el flujo de tráfico a una celda) y actualizando otro estado de control de enrutamiento a `On` (para iniciar el flujo de tráfico a otra). El proceso que cambia el flujo de tráfico es la comprobación de estado de Route 53 asociada al control de enrutamiento, después de que ARC lo actualice para configurarlo como correcto o en mal estado, en función del estado de control de enrutamiento correspondiente.

Los controles de enrutamiento admiten la conmutación por error en cualquier AWS servicio que tenga un punto final de DNS. Puede actualizar los estados del control de enrutamiento para conmutar por error el tráfico con fines de recuperación de desastres, o cuando detecte una disminución de la latencia en la aplicación u otros problemas.

También puede configurar reglas de seguridad para el control de enrutamiento, a fin de asegurarse de que el redireccionamiento del tráfico mediante controles de enrutamiento no afecte a la disponibilidad. Para obtener más información, consulte Crear reglas de seguridad para el control de rutas .

Es importante tener en cuenta que los controles de enrutamiento no son en sí mismos comprobaciones de estado que supervisen el estado subyacente de los puntos de conexión. Por ejemplo, a diferencia de una comprobación de estado de Route 53, un control de enrutamiento no supervisa los tiempos de respuesta ni los tiempos de conexión TCP. Un control de enrutamiento es un simple interruptor de encendido o apagado que controla una comprobación de estado. Por lo general, se cambia el estado para redirigir el tráfico, y ese cambio de estado hace que el tráfico se dirija a un determinado punto de conexión para toda una pila de aplicaciones o impide que se dirija a toda la pila de aplicaciones. Por ejemplo, en una situación sencilla, al cambiar un estado de control de enrutamiento de `On` a `Off`, se actualiza una comprobación de estado de Route 53, que haya asociado a un registro de conmutación por error del DNS para desviar el tráfico de un punto de conexión.

¿Cómo utilizar el control de enrutamiento

Para actualizar el estado del control de enrutamiento y poder redirigir el tráfico, debe conectarse a uno de los puntos finales del clúster en ARC. Si el punto de conexión al que intenta conectarse no está disponible, intente cambiar el estado con otro punto de conexión del clúster. El proceso para cambiar los estados de control de enrutamiento debe estar preparado para probar cada punto de conexión de forma rotativa, ya que los puntos de conexión del clúster pasan por los estados disponibles y no disponibles para su mantenimiento y actualización periódicos.

Al crear controles de enrutamiento, puede configurarlos registros de DNS para asociar las comprobaciones de estado del control de enrutamiento a los nombres DNS de Route 53 que aparecen en cada réplica de la aplicación. Por ejemplo, para controlar las conmutaciones por error del tráfico en dos equilibradores de carga, uno en cada una de las dos regiones, debe crear dos comprobaciones de estado del control de enrutamiento y asociarlas a dos registros de DNS, por ejemplo, registros de alias con políticas de enrutamiento de conmutación por error, con los nombres de dominio de los equilibradores de carga respectivos.

También puede configurar escenarios de conmutación por error de tráfico más complejos utilizando el control de enrutamiento ARC junto con las comprobaciones de estado de Route 53 y los conjuntos de registros de DNS, utilizando registros de DNS con políticas de enrutamiento ponderadas. Para ver un ejemplo detallado, consulte la sección sobre la conmutación por error del tráfico de usuarios

en la siguiente entrada del AWS blog: Creación de aplicaciones altamente resilientes con Amazon Application Recovery Controller (ARC), parte 2: pila multirregional

Al iniciar una conmutación por error para Región de AWS utilizar el control de enrutamiento, debido a los pasos relacionados con el flujo de tráfico, es posible que el tráfico no salga de la región inmediatamente. Las conexiones existentes y en curso en la región también pueden tardar poco en completarse, en función del comportamiento del cliente y de la reutilización de las conexiones. Según la configuración de DNS y otros factores, las conexiones existentes pueden completarse en solo unos minutos o pueden tardar más. Para obtener más información, consulte Garantizar que los cambios de tráfico finalicen rápidamente.

Ventajas del control de enrutamiento

Un control de enrutamiento en ARC tiene varias ventajas en comparación con el redireccionamiento del tráfico con las comprobaciones de estado tradicionales. Por ejemplo:

- Un control de enrutamiento permite realizar la conmutación por error de toda una pila de aplicaciones. Esto contrasta con la conmutación por error de los componentes individuales de una pila, como hacen las EC2 instancias de Amazon, en función de las comprobaciones de estado a nivel de recursos.
- Un control de enrutamiento le proporciona una anulación manual, sencilla y segura que puede utilizar para desviar el tráfico con el fin de realizar tareas de mantenimiento o para recuperarse de fallos cuando las supervisiones internas no detectan ningún problema.
- Puede utilizar un control de enrutamiento junto con reglas de seguridad para evitar los efectos secundarios habituales que pueden producirse con la automatización totalmente automatizada basada en comprobaciones de estado, como la conmutación por error a una infraestructura de reserva que no esté preparada para la conmutación por error.

Este es un ejemplo de cómo incorporar controles de enrutamiento a su estrategia de conmutación por error para mejorar la resiliencia y la disponibilidad de sus aplicaciones. AWS

Puede admitir AWS aplicaciones de alta disponibilidad AWS ejecutando varias réplicas redundantes (normalmente tres) en todas las regiones. A continuación, puede utilizar el control de enrutamiento de Amazon Route 53 para dirigir el tráfico a la réplica adecuada.

Por ejemplo, puede configurar una réplica de la aplicación para que esté activa y sirva el tráfico de la aplicación, mientras que otra es una réplica en espera. Cuando se produce un error en la réplica activa, puede redirigir el tráfico de usuarios a ella para restablecer la disponibilidad de la aplicación.

Debe decidir si desea realizar un error desde o hacia una réplica en función de la información de sus sistemas de monitoreo y control de estado.

Si desea permitir recuperaciones más rápidas, otra opción que puede elegir para su arquitectura es una implementación activa-activa. Con este enfoque, las réplicas están activas al mismo tiempo. Esto significa que puede recuperarse de los errores alejando a los usuarios de una réplica de la aplicación dañada simplemente redirigiendo el tráfico a otra réplica activa.

AWS Disponibilidad regional para el control de enrutamiento

Para obtener información detallada sobre el soporte regional y los puntos de enlace de servicio para Amazon Application Recovery Controller (ARC), consulte los puntos de enlace y las cuotas de Amazon Application Recovery Controller (ARC) en la Referencia general de Amazon Web Services.

> **Note**
>
> El control de enrutamiento de Amazon Application Recovery Controller (ARC) es una función global. Sin embargo, debe especificar la región EE.UU. Oeste (Oregón) (especifique el parámetro`--region us-west-2`) en los AWS CLI comandos ARC regionales. Es decir, cuando crea recursos como clústeres, paneles de control o controles de enrutamiento.

Un control de enrutamiento ARC es un on/off conmutador que cambia el estado de una comprobación de estado del ARC y, a continuación, se puede asociar a un registro DNS que redirige el tráfico, por ejemplo, de una réplica de despliegue principal a una réplica de despliegue en espera.

Si se produce un error en la aplicación o un problema de latencia, puede actualizar los estados del control de enrutamiento para transferir el tráfico de la réplica principal a, por ejemplo, una réplica en espera. Al utilizar las operaciones de API del plano de datos ARC, altamente fiables, para realizar consultas de control de enrutamiento y actualizar el estado del control de enrutamiento, puede confiar en ARC para la conmutación por error en situaciones de recuperación ante desastres. Para obtener más información, consulte Obtener y actualizar los estados de control de enrutamiento mediante la API ARC (recomendado).

ARC mantiene los estados de control de enrutamiento en un clúster, que es un conjunto de cinco puntos finales regionales redundantes. ARC propaga los cambios de estado del control de enrutamiento en todo el clúster, que se encuentra en una EC2 flota de Amazon, para obtener quórum en cinco AWS regiones. Tras la propagación, al consultar a ARC el estado del control de enrutamiento mediante la API y el plano de datos de alta fiabilidad, devuelve la vista de consenso.

Puede interactuar con cualquiera de los cinco puntos finales del clúster para actualizar el estado de un control de enrutamiento desde, por ejemplo, hasta. `Off` `On` A continuación, ARC propaga la actualización entre las cinco regiones del clúster.

La coherencia de los datos en los cinco puntos finales del clúster se logra en 5 segundos en promedio y después de no más de 15 segundos como máximo.

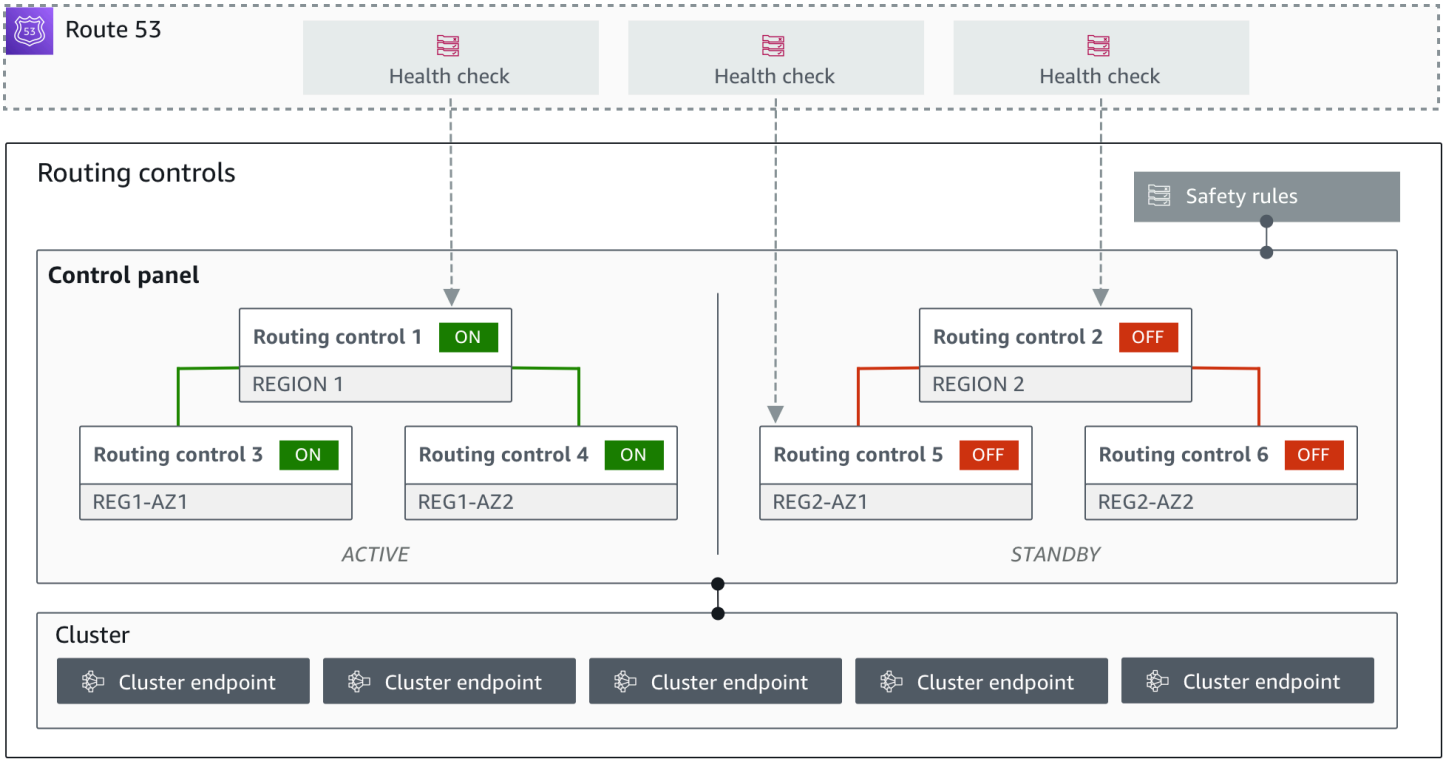
ARC ofrece una confiabilidad extrema con su plano de datos para que pueda realizar una conmutación manual por error de la aplicación entre celdas. ARC garantiza que siempre pueda acceder al menos a tres de los cinco puntos finales del clúster para realizar cambios de estado en el control de enrutamiento. Tenga en cuenta que cada clúster ARC es de un solo inquilino, para garantizar que no le afecten los «vecinos ruidosos» que podrían ralentizar sus patrones de acceso.

Al realizar cambios en los estados del control de enrutamiento, se basa en los tres criterios siguientes, que es muy poco probable que no den resultado:

- Al menos tres de sus cinco puntos finales están disponibles y participan en el quórum.
- Tiene credenciales de IAM que funcionan y puede autenticarse en un punto final de un clúster regional que funcione.
- El plano de datos de Route 53 está en buen estado (este plano de datos está diseñado para cumplir un SLA de disponibilidad del 100%).

Componentes de control de enrutamiento

El siguiente diagrama ilustra un ejemplo de componentes que admiten la función de control de enrutamiento de ARC. Los controles de enrutamiento que se muestran aquí (agrupados en un panel de control) le permiten administrar el tráfico a dos zonas de disponibilidad en cada una de las dos regiones. Al actualizar los estados de control de enrutamiento, ARC cambia las comprobaciones de estado en Amazon Route 53, que redirigen el tráfico de DNS a diferentes celdas. Las reglas de seguridad que se configuran para los controles de enrutamiento ayudan a evitar situaciones de apertura por error y otras consecuencias no intencionadas.



Los siguientes son componentes de la función de control de enrutamiento de ARC.

Clúster

Un clúster es un conjunto de cinco puntos finales regionales redundantes desde los que se inician llamadas a la API para actualizar u obtener los estados del control de enrutamiento. Un clúster incluye un panel de control predeterminado y puede alojar varios paneles de control y controles de enrutamiento en un clúster.

Control de enrutamiento

Un control de enrutamiento es un on/off conmutador simple, alojado en un clúster, que se utiliza para controlar el enrutamiento del tráfico de clientes que entra y sale de las celdas. Al crear un control de enrutamiento, se agrega una verificación de estado del ARC en Route 53. Esto le permite redirigir el tráfico (mediante las comprobaciones de estado, configuradas con registros de DNS para sus aplicaciones) al actualizar el estado del control de enrutamiento en ARC.

Verificación del estado del control de enrutamiento

Los controles de enrutamiento están integrados con las comprobaciones de estado de Route 53. Las comprobaciones de estado están asociadas a los registros de DNS que se encuentran junto a cada réplica de la aplicación, por ejemplo, los registros de conmutación por error. Al cambiar los estados del control de enrutamiento, ARC actualiza las comprobaciones de estado

correspondientes, que redirigen el tráfico, por ejemplo, para que se conmute por error a la réplica en espera.

Plano de control

Un panel de control agrupa un conjunto de controles de enrutamiento relacionados. Puede asociar varios controles de enrutamiento a un panel de control y, a continuación, crear reglas de seguridad para el panel de control a fin de garantizar que las actualizaciones de redireccionamiento del tráfico que realice sean seguras. Por ejemplo, puede configurar un control de enrutamiento para cada uno de los balanceadores de carga de cada zona de disponibilidad y, a continuación, agruparlos en el mismo panel de control. A continuación, puedes añadir una regla de seguridad (una «regla de afirmación») que garantice que al menos una zona (representada por un control de enrutamiento) esté activa en cualquier momento, a fin de evitar situaciones de «apertura por error» imprevistas.

Panel de control predeterminado

Al crear un clúster, ARC crea un panel de control predeterminado. De forma predeterminada, todos los controles de enrutamiento que cree en el clúster se agregan al panel de control predeterminado. O bien, puede crear sus propios paneles de control para agrupar los controles de enrutamiento relacionados.

Regla de seguridad

Las reglas de seguridad son reglas que se añaden al control de enrutamiento para garantizar que las acciones de recuperación no afecten accidentalmente a la disponibilidad de la aplicación. Por ejemplo, es posible que cree una regla de seguridad que cree un control de enrutamiento que actúa como un interruptor general de «encendido/apagado» para que pueda habilitar o deshabilitar un conjunto de otros controles de enrutamiento.

Punto final (punto final del clúster)

Cada clúster de ARC tiene cinco puntos finales regionales que puede utilizar para configurar y recuperar los estados del control de enrutamiento. El proceso de acceso a los puntos finales debe suponer que ARC los activa y desactiva periódicamente para realizar tareas de mantenimiento, por lo que debe probar cada punto final sucesivamente hasta que se conecte a uno de ellos. Puede acceder a los puntos finales para ver el estado actual de los controles de enrutamiento (activados o desactivados) y activar las conmutaciones por error de sus aplicaciones cambiando los estados de los controles de enrutamiento.

Planos de datos y control para el control del enrutamiento

Al planificar la conmutación por error y la recuperación ante desastres, tenga en cuenta la resistencia de sus mecanismos de conmutación por error. Le recomendamos que se asegure de que los mecanismos de los que depende durante la conmutación por error estén altamente disponibles, de modo que pueda utilizarlos cuando los necesite en caso de desastre. Por lo general, debe utilizar funciones de plano de datos para sus mecanismos siempre que pueda, a fin de obtener la máxima fiabilidad y tolerancia a los fallos. Teniendo esto en cuenta, es importante entender cómo se divide la funcionalidad de un servicio entre planos de control y planos de datos, y cuándo se puede confiar en una fiabilidad extrema con el plano de datos de un servicio.

Como ocurre con la mayoría de AWS los servicios, los planos de control y los planos de datos admiten la funcionalidad de la capacidad de control de enrutamiento. Si bien ambos están diseñados para ser fiables, un plano de control está optimizado para garantizar la coherencia de los datos, mientras que un plano de datos está optimizado para garantizar la disponibilidad. Un plano de datos está diseñado para ser resistente, de modo que puede mantener la disponibilidad incluso durante eventos disruptivos, cuando un plano de control podría no estar disponible.

En general, un plano de control permite realizar funciones de administración básicas, como crear, actualizar y eliminar recursos del servicio. Un plano de datos proporciona la funcionalidad principal de un servicio. Por ello, le recomendamos que utilice las operaciones del plano de datos cuando la disponibilidad sea importante, por ejemplo, cuando necesite redirigir el tráfico a una réplica en espera durante una interrupción.

Para el control de enrutamiento, los planos de control y los planos de datos se dividen de la siguiente manera:

- La API del plano de control para el control de enrutamiento es la API de configuración de control de recuperación, compatible con la región EE.UU. Oeste (Oregón) (us-west-2). Utiliza estas operaciones de la API o las AWS Management Console para crear o eliminar clústeres, paneles de control y controles de enrutamiento, a fin de prepararte para un evento de recuperación ante desastres cuando necesites redirigir el tráfico de tu aplicación. El plano de control de la configuración del control de enrutamiento no tiene una alta disponibilidad.
- El plano de datos de control de enrutamiento es un clúster dedicado a cinco regiones aisladas AWS geográficamente. Cada cliente crea uno o más clústeres mediante el plano de control de enrutamiento. El clúster aloja paneles de control y controles de enrutamiento. A continuación, utilice la API de control de enrutamiento (clúster de recuperación) para obtener, enumerar y

actualizar los estados de control de enrutamiento cuando desee redirigir el tráfico de su aplicación. El plano de datos de control de enrutamiento tiene una alta disponibilidad.

Como el plano de datos de control de enrutamiento tiene una alta disponibilidad, le recomendamos que planee usarlo para hacer que las llamadas AWS Command Line Interface a la API funcionen con los estados de control de enrutamiento cuando desee realizar una conmutación por error para recuperarse de un evento. Para obtener más información sobre las consideraciones clave a la hora de preparar y completar una operación de recuperación con el control de enrutamiento, consulteMejores prácticas para el control de enrutamiento en ARC.

Para obtener más información sobre los planos de datos, los planos de control y cómo AWS se crean servicios para cumplir los objetivos de alta disponibilidad, consulte el artículo Static stability using Availability Zones en Amazon Builders' Library.

Etiquetado para el control de enrutamiento en Amazon Application Recovery Controller (ARC)

Las etiquetas son palabras o frases (metadatos) que se utilizan para identificar y organizar AWS los recursos. Puede añadir varias etiquetas a cada recurso, y cada etiqueta incluye una clave y un valor que usted define. Por ejemplo, la clave puede ser el entorno y el valor puede ser la producción. Puede buscar y filtrar sus recursos en función de las etiquetas que añada.

Puede etiquetar los siguientes recursos en el control de enrutamiento en ARC:

- Clústeres
- Paneles de control
- Normas de seguridad

El etiquetado en ARC solo está disponible a través de la API, por ejemplo, mediante el AWS CLI.

Los siguientes son ejemplos de etiquetado en el control de enrutamiento mediante el. 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
```

Para obtener más información, consulte la Guía TagResourcede referencia de la API de configuración de control de recuperación para Amazon Application Recovery Controller (ARC).

Precios del control de enrutamiento en ARC

Para el control de enrutamiento en ARC, usted paga un costo por hora por cada clúster que cree. Cada clúster puede alojar varios controles de enrutamiento, que se utilizan para activar las conmutaciones por error de las aplicaciones.

Para ayudar a administrar los costos y mejorar la eficiencia, puede configurar el uso compartido entre cuentas para un clúster, a fin de compartir un clúster con varias AWS cuentas. Para obtener más información, consulte Support multicuenta para clústeres en ARC.

Para obtener información detallada sobre los precios de ARC y ejemplos de precios, consulta los precios de ARC.

Introducción a la recuperación multirregional en Amazon Application Recovery Controller (ARC)

Para realizar la conmutación por error de sus aplicaciones mediante el control de enrutamiento de Amazon Application Recovery Controller (ARC), debe tener AWS aplicaciones que estén en varios Regiones de AWS. Para empezar, primero asegúrese de que sus aplicaciones estén configuradas en réplicas aisladas en cada región, de modo que pueda realizar la conmutación por error de una a otra durante un evento. A continuación, puede crear controles de enrutamiento para redirigir el tráfico de la aplicación y realizar la conmutación por error de una aplicación principal a una secundaria, manteniendo así la continuidad para los usuarios.

> **Note**
>
> Si tiene una aplicación aislada por zonas de disponibilidad, considere la posibilidad de utilizar el cambio zonal o el cambio automático zonal para la recuperación de la conmutación por error. No es necesario realizar ninguna configuración para utilizar el cambio zonal o el cambio automático zonal a fin de recuperar de forma fiable las aplicaciones en caso de averías en las zonas de disponibilidad. Para obtener más información, consulte Utilice el cambio zonal y el cambio automático zonal para recuperar aplicaciones en ARC.

Para poder utilizar el control de enrutamiento ARC para recuperar aplicaciones durante un evento, le recomendamos que configure al menos dos aplicaciones que sean réplicas una de la otra. Cada réplica, o celda, representa una Región de AWS. Una vez que haya configurado los recursos de la aplicación para que se ajusten a los de Regions, asegúrese de que la aplicación esté configurada para que se recupere correctamente. Para ello, siga estos pasos.

Consejo: Para ayudar a simplificar la configuración, ofrecemos plantillas de HashiCorp Terraform AWS CloudFormation y Terraform que crean una aplicación con réplicas redundantes que fallan independientemente unas de otras. Para obtener más información y descargar las plantillas, consulte. Cómo configurar una aplicación de ejemplo

Para prepararse para usar el control de enrutamiento, asegúrese de que su aplicación esté configurada para ser resistente haciendo lo siguiente:

1. Cree copias independientes de su pila de aplicaciones (capa de red y de cómputo) que sean réplicas unas de otras en cada región, de modo que pueda conmutar por error el tráfico de una a otra cuando se produzca un evento. Asegúrese de no tener dependencias entre regiones en el código de la aplicación que puedan provocar que el fallo de una réplica afecte a la otra. Para que la conmutación por error entre ellas se realice correctamente Regiones de AWS, los límites de tu pila deben estar dentro de una región.
2. Duplique todos los datos de estado necesarios para su aplicación en las réplicas. Puede usar los servicios AWS de bases de datos para ayudar a replicar sus datos.

Comience con el control de enrutamiento para la conmutación por error de tráfico

El control de enrutamiento de Amazon Application Recovery Controller (ARC) le permite activar la conmutación por error para que el tráfico conmute por error entre copias de aplicaciones redundantes, o réplicas, que se ejecutan por separado. Regiones de AWS La conmutación por error se realiza con DNS, utilizando el plano de datos de Amazon Route 53.

Después de configurar las réplicas en cada región, como se describe en la siguiente sección, puede asociar cada una de ellas a un control de enrutamiento. En primer lugar, asocie los controles de enrutamiento a los nombres de dominio de nivel superior de sus réplicas en cada región. A continuación, añada una comprobación del estado del control de enrutamiento al control de enrutamiento para que pueda activar y desactivar el flujo de tráfico. Esto le permite controlar el enrutamiento del tráfico entre las réplicas de su aplicación.

Puede actualizar los estados de control de enrutamiento en el AWS Management Console tráfico de conmutación por error, pero le recomendamos que, en su lugar, utilice las acciones ARC, mediante la API o AWS CLI, para cambiarlas. Las acciones de la API no dependen de la consola, por lo que son más flexibles.

Por ejemplo, para realizar la conmutación por error entre regiones, de us-west-1 a us-east-1, puedes `update-routing-control-state` usar la acción de la API para establecer el estado de to y to. `us-west-1` `Off` `us-east-1` `On`

Antes de crear componentes de control de enrutamiento para configurar la conmutación por error para su aplicación, asegúrese de que la aplicación esté dividida en silos en réplicas regionales, de modo que pueda realizar la conmutación por error de una a otra. Para obtener más información y empezar a aislar una nueva aplicación o a crear una pila de ejemplos, consulte las siguientes secciones.

Cómo configurar una aplicación de ejemplo

Para ayudarle a entender cómo funciona el control de enrutamiento, le ofrecemos una aplicación de ejemplo llamada`TicTacToe`. En el ejemplo se utilizan AWS CloudFormation plantillas para simplificar el proceso, así como una AWS CloudFormation plantilla descargable para que pueda explorar rápidamente la configuración y el uso de ARC por su cuenta.

Tras implementar la aplicación de ejemplo, puede utilizar las plantillas para crear componentes ARC y, a continuación, explorar el uso de los controles de enrutamiento para gestionar el flujo de tráfico que llega a la aplicación. Puede adaptar la plantilla y el proceso a sus propios escenarios y aplicaciones.

Para empezar con un ejemplo de aplicación y AWS CloudFormation plantillas, consulta las instrucciones del archivo README en el repositorio de ARC GitHub. Para obtener más información sobre el uso de AWS CloudFormation plantillas, lee los AWS CloudFormation conceptos de la Guía del AWS CloudFormation usuario.

Mejores prácticas para el control de enrutamiento en ARC

Recomendamos las siguientes prácticas recomendadas para la preparación de la recuperación y la conmutación por error para el control del enrutamiento en ARC.

Temas

- Mantenga seguras y siempre accesibles las AWS credenciales diseñadas específicamente y de larga duración
- Elija valores TTL más bajos para los registros de DNS involucrados en la conmutación por error
- Limite el tiempo que los clientes permanecen conectados a sus puntos finales
- Marque o codifique de forma rígida los cinco puntos finales y el control de enrutamiento del clúster regional ARNs
- Elija uno de sus puntos finales al azar para actualizar los estados de control de enrutamiento
- Utilice la API del plano de datos, extremadamente fiable, para enumerar y actualizar los estados de control de enrutamiento, no la consola

Mantenga seguras y siempre accesibles las AWS credenciales diseñadas específicamente y de larga duración

En un escenario de recuperación ante desastres (DR), reduzca al mínimo las dependencias del sistema mediante un enfoque sencillo para acceder a las tareas de recuperación AWS y realizarlas. Cree credenciales de IAM de larga duración específicas para las tareas de DR y guárdelas de forma segura en una caja fuerte física en las instalaciones o en un almacén virtual para acceder a ellas cuando sea necesario. Con IAM, puede gestionar de forma centralizada las credenciales de seguridad, como las claves de acceso y los permisos de acceso a AWS los recursos. En el caso de tareas no relacionadas con DR, le recomendamos que siga utilizando el acceso federado mediante los servicios de AWS , como, por ejemplo, AWS Single Sign-On.

Para realizar tareas de conmutación por error en ARC con la API del plano de datos del clúster de recuperación, puede adjuntar una política de IAM de ARC a su usuario. Para obtener más información, consulte Ejemplos de políticas basadas en identidad en Amazon Application Recovery Controller (ARC).

Elija valores TTL más bajos para los registros de DNS involucrados en la conmutación por error

En el caso de los registros de DNS que pueda necesitar cambiar como parte del mecanismo de conmutación por error, especialmente los registros cuyo estado se haya comprobado, se recomienda utilizar valores de TTL más bajos. Configurar un TTL de 60 o 120 segundos es una opción común para esta situación.

La configuración TTL (tiempo de vida) de DNS indica a los solucionadores de DNS cuánto tiempo deben almacenar en caché un registro antes de solicitar uno nuevo. Cuando selecciona un TTL, inicia un compromiso entre latencia y fiabilidad y la capacidad de respuesta a los cambios. Con

TTL más cortos en un registro, los solucionadores de DNS detectan las actualizaciones del registro más rápido, ya que deben realizar consultas con más frecuencia.

Para obtener más información, consulte Elija valores de TTL para los registros de DNS en Prácticas recomendadas para registros de DNS de Amazon Route 53.

Limite el tiempo que los clientes permanecen conectados a sus puntos finales

Cuando utilizas controles de enrutamiento para cambiar de uno Región de AWS a otro, el mecanismo que Amazon Application Recovery Controller (ARC) utiliza para mover el tráfico de tus aplicaciones es una actualización de DNS. Esta actualización hace que todas las conexiones nuevas se dirijan lejos de la ubicación dañada.

Sin embargo, los clientes con conexiones abiertas preexistentes pueden seguir realizando solicitudes a la ubicación dañada hasta que los clientes se vuelvan a conectar. Para garantizar una recuperación rápida, le recomendamos que limite el tiempo que los clientes permanecen conectados a sus terminales.

Si usa un Application Load Balancer, puede usar la `keepalive` opción para configurar la duración de las conexiones. Para obtener más información, consulte la duración de keepalive del cliente HTTP en la Guía del usuario de Application Load Balancer.

De forma predeterminada, los balanceadores de carga de aplicaciones establecen el valor de duración de keepalive del cliente HTTP en 3600 segundos o 1 hora. Le sugerimos que reduzca el valor para ajustarlo al objetivo de tiempo de recuperación de su aplicación, por ejemplo, 300 segundos. Al elegir el tiempo de permanencia activo de un cliente HTTP, tenga en cuenta que este valor es una compensación entre volver a conectarse con más frecuencia, en general, lo que puede afectar a la latencia, y alejar más rápidamente a todos los clientes de una zona de disponibilidad o región con problemas.

Marque o codifique de forma rígida los cinco puntos finales del clúster regional y el control de enrutamiento ARNs

Le recomendamos que guarde una copia local de los puntos de enlace del clúster regional de ARC en marcadores o guardada en un código de automatización que utilice para volver a probar los puntos de enlace. Si se produce un error, es posible que no pueda acceder a algunas operaciones de la API, incluidas las operaciones de la API de ARC que no están alojadas en un clúster de plano de datos extremadamente fiable. Puede enumerar los puntos finales de sus clústeres de ARC mediante la operación de DescribeClusterAPI.

Elija uno de sus puntos finales al azar para actualizar los estados de control de enrutamiento

Los controles de enrutamiento proporcionan cinco puntos finales regionales para garantizar una alta disponibilidad, incluso en caso de averías. Para lograr su total resiliencia, es importante contar con una lógica de reintento que pueda utilizar los cinco puntos finales según sea necesario. Para obtener información sobre el uso de ejemplos de código con el AWS SDK, incluidos ejemplos para probar puntos de enlace de clústeres, consulte. Ejemplos de código para Application Recovery Controller mediante AWS SDKs

Utilice la API del plano de datos, extremadamente fiable, para enumerar y actualizar los estados de control de enrutamiento, no la consola

Con la API del plano de datos ARC, consulte los controles y estados de enrutamiento con la ListRoutingControlsoperación y actualice los estados del control de enrutamiento para redirigir el tráfico y realizar la conmutación por error con la UpdateRoutingControlStateoperación. Puede usar el código AWS CLI (como en estos ejemplos) o el código que escriba con uno de los AWS SDKs. ARC ofrece una confiabilidad extrema con la API en el plano de datos para conmutar el tráfico por error. Recomendamos usar la API en lugar de cambiar los estados de control de enrutamiento en la AWS Management Console.

Conéctese a uno de los puntos finales de su clúster regional para que ARC utilice la API del plano de datos. Si el punto de conexión no está disponible, puede intentar conectarse a otro punto de conexión del clúster.

Si una regla de seguridad bloquea una actualización del estado del control de enrutamiento, puede omitirla para realizar la actualización y conmutar por error el tráfico. Para obtener más información, consulte Anulación de las reglas de seguridad para redirigir el tráfico.

Pruebe la conmutación por error con ARC

Pruebe la conmutación por error con regularidad con el control de enrutamiento ARC, para realizar la conmutación por error de su pila de aplicaciones principal a una pila de aplicaciones secundaria. Es importante asegurarse de que las estructuras ARC que ha agregado estén alineadas con los recursos correctos de su pila y de que todo funcione como se espera. Debe probarlo después de configurar ARC para su entorno y seguir realizando pruebas periódicamente para que su entorno de conmutación por error esté preparado antes de que se produzca una situación de fallo en la que necesite que el sistema secundario esté listo y funcionando rápidamente para evitar que los usuarios sufran tiempos de inactividad.

Operaciones de la API de control de enrutamiento

En esta sección se incluyen tablas con listas de operaciones de API que puede utilizar para configurar y utilizar el control de enrutamiento en Amazon Application Recovery Controller (ARC), con enlaces a la documentación pertinente.

Para ver ejemplos de cómo utilizar las operaciones comunes de la API de configuración del control de enrutamiento con el AWS Command Line Interface, consulte Ejemplos del uso de las operaciones de la API de control de enrutamiento ARC con AWS CLI.

En la siguiente tabla se enumeran las operaciones de la API ARC que puede utilizar para la configuración del control de enrutamiento, con enlaces a la documentación pertinente.

Acción	Uso de la consola ARC	Uso de la API ARC
Creación de un clúster	Consulte Creación de componentes de control de enrutamiento en ARC	Consulte CreateCluster.
Describir un clúster	Consulte Creación de componentes de control de enrutamiento en ARC	Consulte DescribeCluster.
Eliminar un clúster	Consulte Creación de componentes de control de enrutamiento en ARC	Consulte DeleteCluster.
Listar los clústeres de una cuenta	Consulte Creación de componentes de control de enrutamiento en ARC	Consulte ListClusters.
Creación de un control de enrutamiento	Consulte Creación de componentes de control de enrutamiento en ARC	Consulte CreateRoutingControl.
Describa un control de enrutamiento	Consulte Creación de componentes de control de enrutamiento en ARC	Consulte DescribeRoutingControl.

Acción	Uso de la consola ARC	Uso de la API ARC
Actualización de control de enrutamiento	Consulte Creación de componentes de control de enrutamiento en ARC	Consulte UpdateRoutingControl.
Eliminación de un control de enrutamiento	Consulte Creación de componentes de control de enrutamiento en ARC	Consulte DeleteRoutingControl.
Listar los controles de enrutamiento	Consulte Creación de componentes de control de enrutamiento en ARC	Consulte ListRoutingControls.
Creación de un panel de control	Consulte Creación de componentes de control de enrutamiento en ARC	Consulte CreateControlPanel.
Describa un panel de control	Consulte Creación de componentes de control de enrutamiento en ARC	Consulte DescribeControlPanel.
Actualización de un panel de control	Consulte Creación de componentes de control de enrutamiento en ARC	Consulte UpdateControlPanel.
Eliminación de un panel de control	Consulte Creación de componentes de control de enrutamiento en ARC	Consulte DeleteControlPanel.
Descripción de paneles de control	Consulte Creación de componentes de control de enrutamiento en ARC	Consulte ListControlPanels.
Creación de una regla de seguridad	Consulte Crear reglas de seguridad para el control de rutas	Consulte CreateSafetyRule.

Acción	Uso de la consola ARC	Uso de la API ARC
Describa una regla de seguridad	Consulte Crear reglas de seguridad para el control de rutas	Consulte DescribeSafetyRule.
Actualice una regla de seguridad	Consulte Crear reglas de seguridad para el control de rutas	Consulte UpdateSafetyRule.
Eliminación de una regla de seguridad	Consulte Crear reglas de seguridad para el control de rutas	Consulte DeleteSafetyRule.
Enumere las reglas de seguridad	Consulte Crear reglas de seguridad para el control de rutas	Consulte ListSafetyRules.
Enumere comprobaciones de estado asociadas de Route 53	Consulte Crear una verificación de estado del control de enrutamiento en ARC	Consulte ListAssociatedRoute53 HealthChecks
Enumere las políticas AWS RAM de recursos para compartir clústeres	Consulte Support multicuenta para clústeres en ARC	Consulte GetResourcePolicy

En la siguiente tabla se enumeran las operaciones comunes de la API ARC que puede utilizar para gestionar la conmutación por error del tráfico con el plano de datos del control de enrutamiento, con enlaces a la documentación pertinente.

Acción	Uso de la consola ARC	Uso de la API ARC
Obtener el estado de un control de enrutamiento	Consulte Obtener y actualizar los estados de control de enrutamiento en el AWS Management Console	Consulte GetRoutingControlState.

Acción	Uso de la consola ARC	Uso de la API ARC
Listar los controles de enrutamiento	N/A	Consulte ListRoutingControls
Actualizar el estado de un control de enrutamiento	Consulte Obtener y actualizar los estados de control de enrutamiento en el AWS Management Console	Consulte UpdateRoutingControlState.
Actualice varios estados de control de enrutamiento	Consulte Obtener y actualizar los estados de control de enrutamiento en el AWS Management Console	Consulte UpdateRoutingControlStates.

Uso de este servicio con un AWS SDK

AWS Los kits de desarrollo de software (SDKs) están disponibles para muchos lenguajes de programación populares. Cada SDK proporciona una API, ejemplos de código y documentación que facilitan a los desarrolladores la creación de aplicaciones en su lenguaje preferido.

Documentación de SDK	Ejemplos de código
AWS SDK para C++	AWS SDK para C++ ejemplos de código
AWS CLI	AWS CLI ejemplos de código
AWS SDK para Go	AWS SDK para Go ejemplos de código
AWS SDK para Java	AWS SDK para Java ejemplos de código
AWS SDK para JavaScript	AWS SDK para JavaScript ejemplos de código
AWS SDK para Kotlin	AWS SDK para Kotlin ejemplos de código
AWS SDK para .NET	AWS SDK para .NET ejemplos de código
AWS SDK para PHP	AWS SDK para PHP ejemplos de código

Documentación de SDK	Ejemplos de código
Herramientas de AWS para PowerShell	Herramientas de AWS para PowerShell ejemplos de código
AWS SDK para Python (Boto3)	AWS SDK para Python (Boto3) ejemplos de código
AWS SDK para Ruby	AWS SDK para Ruby ejemplos de código
AWS SDK para Rust	AWS SDK para Rust ejemplos de código
AWS SDK para SAP ABAP	AWS SDK para SAP ABAP ejemplos de código
AWS SDK para Swift	AWS SDK para Swift ejemplos de código

Para obtener ejemplos específicos de este servicio, consulte Ejemplos de código para Application Recovery Controller mediante AWS SDKs.

Ejemplo de disponibilidad

¿No encuentra lo que necesita? Solicite un ejemplo de código a través del enlace de Enviar comentarios que se encuentra al final de esta página.

Ejemplos del uso de las operaciones de la API de control de enrutamiento ARC con AWS CLI

En esta sección, se describen ejemplos de aplicaciones sencillas sobre cómo trabajar con el control de enrutamiento y cómo AWS Command Line Interface trabajar con la capacidad de control de enrutamiento de Amazon Application Recovery Controller (ARC) mediante operaciones de API. Los ejemplos están pensados para ayudarlo a desarrollar una comprensión básica de cómo trabajar con el control de enrutamiento mediante la CLI.

Con el control de enrutamiento de Amazon Application Recovery Controller (ARC), puede activar conmutaciones por error de tráfico entre copias de aplicaciones redundantes, o réplicas, que se ejecutan en zonas de disponibilidad Regiones de AWS o independientes.

Los controles de enrutamiento se organizan en grupos denominados paneles de control que se aprovisionan en un clúster. Un clúster ARC es un conjunto regional de puntos finales que se implementa a nivel mundial. Los puntos de conexión del clúster proporcionan una API de alta disponibilidad que puede utilizar para establecer y recuperar los estados de control de enrutamiento. Para obtener más información acerca de los componentes de la característica de control de enrutamiento, consulte Componentes de control de enrutamiento .

> **Note**
>
> ARC es un servicio global que admite varios puntos finales. Regiones de AWS Sin embargo, debe especificar la región EE.UU. Oeste (Oregón), es decir, especificar el parámetro `--region us-west-2`, en la mayoría de los comandos de ARC CLI. Por ejemplo, utilice el `region` parámetro cuando cree grupos de recuperación, paneles de control y clústeres. Al crear un clúster, ARC le proporciona un conjunto de puntos finales regionales. Para obtener o actualizar los estados del control de enrutamiento, debe especificar el punto final regional (el punto final Región de AWS y la URL del punto final) en su comando CLI.

Para obtener más información sobre el uso de AWS CLI, consulte la Referencia de AWS CLI comandos. Para obtener una lista de las acciones de la API de control de enrutamiento, consulte Operaciones de la API de control de enrutamiento y Operaciones de la API de control de enrutamiento.

Empezaremos por crear los componentes que necesita para gestionar la conmutación por error mediante controles de enrutamiento, empezando por la creación de un clúster.

Configure los componentes de control de enrutamiento

El primer paso es crear un clúster. Un clúster ARC es un conjunto de cinco puntos finales, uno en cada uno de los cinco diferentes Regiones de AWS. La infraestructura ARC permite que estos puntos finales funcionen de forma coordinada, de modo que garanticen la alta disponibilidad y la coherencia secuencial de las operaciones de conmutación por error.

1. Creación de un clúster

1a. Cree un clúster. `network-type`Es opcional y puede ser o. `IPV4` `DUALSTACK` El valor predeterminado es `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"
}
```

Cuando se crea un recurso ARC por primera vez, su estado es `PENDING` mientras se crea el clúster. Llame a `describe-cluster` para comprobar su progreso.

1b. Describir un clúster

```
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"
}
```

Cuando el estado es DESPLEGADO, ARC ha creado correctamente el clúster con el conjunto de puntos finales con los que puede interactuar. Llame a `list-clusters` para hacer una lista de todos los clústeres.

1c. Enumere los clústeres.

```
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. Actualice el tipo de red de sus clústeres. Las opciones son `IPV4` y `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. Creación de un panel de control

Un panel de control es una agrupación lógica para organizar los controles de enrutamiento ARC. Al crear un clúster, ARC le proporciona automáticamente un panel de control denominado`DefaultControlPanel`. Puede utilizar este panel de control de forma inmediata.

Un panel de control solo puede existir en un clúster. Si desea mover un panel de control a otro clúster, debe eliminarlo y, a continuación, crearlo en el segundo clúster. Llame a `list-control-panels` para ver todos los paneles de control de la cuenta. Para ver solo los paneles de control de un determinado clúster, añada el campo `--cluster-arn`.

2a. Enumere los paneles de control.

```
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"
        }
    ]
}
```

Si lo desea, llame a `create-control-panel` para crear su propio panel de control.

2b. Creación de un panel de control

```
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"
    }
}
```

Cuando crea un recurso ARC por primera vez, su estado es `PENDING` mientras se está creando. Llame a `describe-control-panel` para comprobar su progreso.

2c. Describa un panel de control.

```
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. Obtener un control de enrutamiento

Ahora que ha configurado el clúster y ha examinado los paneles de control, puede empezar a crear controles de enrutamiento. Al crear un control de enrutamiento, debe especificar como mínimo el nombre de recurso de Amazon (ARN) del clúster en el que desea que esté el control de enrutamiento. También puede especificar el ARN de un panel de control para el control de enrutamiento. También tendrá que especificar el clúster en el que se encuentra el panel de control.

Si no especifica ningún panel de control, el control de enrutamiento se añadirá al panel de control creado automáticamente, `DefaultControlPanel`.

Llame a `create-routing-control` para crear un control de enrutamiento.

3a. Obtener un control de enrutamiento.

```
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"
    }
}
```

Los controles de enrutamiento siguen el mismo patrón de creación que otros recursos ARC, por lo que puede realizar un seguimiento de su progreso mediante una operación de descripción.

3b. Describa un control de enrutamiento.

```
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"
    }
}
```

Llame a `list-routing-controls` para enumerar los controles de enrutamiento de un panel de control. Se necesita el ARN del panel de control.

3c. Listar los controles de enrutamiento

```
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"
        }
    ]
}
```

En el siguiente ejemplo, en el que trabajamos con los estados de control de enrutamiento, supongamos que tenemos los dos controles de enrutamiento que aparecen en la lista en esta sección (Rc1 y Rc2). En este ejemplo, cada control de enrutamiento representa una zona de disponibilidad en la que se implementa la aplicación.

4. Creación de reglas de seguridad

Al trabajar con varios controles de enrutamiento al mismo tiempo, es posible que desee adoptar algunas medidas de seguridad al habilitarlos y deshabilitarlos, con el fin de evitar consecuencias no intencionadas, como desactivar ambos controles de enrutamiento y detener todo el flujo de tráfico. Para crear estas salvaguardas, debe crear reglas de seguridad para el control de enrutamiento.

Hay dos tipos de reglas de seguridad: reglas de aserción y reglas de regulación. Para obtener más información sobre las reglas de seguridad, consulte Crear reglas de seguridad para el control de rutas .

En la siguiente llamada se proporciona un ejemplo de cómo crear una regla de aserción que garantice que al menos uno de los dos controles de enrutamiento esté configurado en 0n en un momento dado. Para crear la regla, ejecute `create-safety-rule` con el parámetro `assertion-rule`.

Para obtener información detallada sobre el funcionamiento de la API de reglas de aserción, consulte AssertionRulela Guía de referencia de la API de control de enrutamiento para Amazon Application Recovery Controller.

4a. Cree una regla de aserción.

```
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
        }
    }
}
```

En la siguiente llamada se proporciona un ejemplo de cómo crear una regla de regulación que proporciona un conmutador general de “encendido/apagado” o “regulación” para un conjunto de controles de enrutamiento de destino de un panel de control. Esto le permite impedir la actualización de los controles de enrutamiento de destino para que, por ejemplo, la automatización no pueda realizar actualizaciones no autorizadas. En este ejemplo, el conmutador de regulación es un control de enrutamiento especificado por el parámetro `GatingControls` y los dos controles de enrutamiento que están controlados o “regulados” los especifica el parámetro `TargetControls`.

> **Note**
>
> Antes de crear la regla de regulación, debe crear el control de enrutamiento de regulación, que no incluye los registros de conmutación por error de DNS ni los controles de enrutamiento de destino, que sí debe configurar con los registros de conmutación por error de DNS.

Para crear la regla, ejecute `create-safety-rule` con el parámetro `gating-rule`.

Para obtener información detallada sobre el funcionamiento de la API de reglas de aserción, consulte GatingRulela Guía de referencia de la API de control de enrutamiento para Amazon Application Recovery Controller.

4b. Cree una regla de regulación.

```
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
        }
    }
}
```

Al igual que con otros recursos de control de enrutamiento, puede describir, enumerar o eliminar las reglas de seguridad una vez que se propaguen al plano de datos.

Después de configurar una o varias reglas de seguridad, puede seguir interactuando con el clúster para establecer o recuperar el estado de los controles de enrutamiento. Si una operación de `set-routing-control-state` infringe una regla que haya creado, recibirá una excepción similar a la siguiente:

```
Cannot modify control state for [0123456bbbbbbb0123456bbbbbb01234560123
abcdefg1234567] due to failed rule evaluation
0123456bbbbbbb0123456bbbbbb0123456333333444444
```

El primer identificador es el ARN del panel de control concatenado con el ARN del control de enrutamiento. El segundo identificador es el ARN del panel de control concatenado con el ARN del control de seguridad.

5. Creación de una comprobación de estado

Para utilizar los controles de enrutamiento para conmutar el tráfico por error, debe crear comprobaciones de estado en Amazon Route 53 y, a continuación, asociar las comprobaciones de estado a sus registros de DNS. Para conmutar el tráfico por error, un control de enrutamiento ARC configura la comprobación de estado como incorrecta, de modo que Route 53 redireccione el tráfico. (La comprobación de estado no valida el estado de la aplicación; simplemente se utiliza como método para redirigir el tráfico).

Como ejemplo, supongamos que tiene dos celdas (regiones o zonas de disponibilidad). Configura una como celda principal de la aplicación y la otra como secundaria a la que realizar la conmutación por error.

Para configurar las comprobaciones de estado para la conmutación por error, puede hacer lo siguiente, por ejemplo:

1. Utilice la CLI de ARC para crear un control de enrutamiento para cada celda.
2. Utilice la CLI de Route 53 para crear una verificación de estado de ARC en Route 53 para cada control de enrutamiento.
3. Utilice la CLI de Route 53 para crear dos registros de DNS de conmutación por error en Route 53 y asociar una comprobación de estado a cada uno de ellos.

5a. Cree un control de enrutamiento para cada celda.

```
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
```

5b. Cree una comprobación de estado para cada control de enrutamiento.

> **Note**
>
> Las comprobaciones de estado de ARC se crean mediante la CLI de 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. Cree dos registros de DNS de conmutación por error y asocie una comprobación de estado a cada uno de ellos.

Los registros de DNS de conmutación por error en Route 53 se crean mediante la CLI de Route 53. Para crear los registros, siga las instrucciones de la referencia de AWS CLI comandos de Amazon Route 53 para el change-resource-record-setscomando. En los registros, especifique el valor de DNS de cada celda junto con el valor `HealthCheckID` correspondiente que Route 53 creó para la comprobación de estado (consulte la sección 6b).

Para la celda principal:

```
{
    "Name": "myapp.yourdomain.com",
    "Type": "CNAME",
    "SetIdentifier": "primary",
    "Failover": "PRIMARY",
    "TTL": 0,
    "ResourceRecords": [
        {
            "Value": "cell1.yourdomain.com"
        }
    ],
    "HealthCheckId": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
}
```

Para la celda secundaria:

```
{
```

```
    "Name": "myapp.yourdomain.com",
    "Type": "CNAME",
    "SetIdentifier": "secondary",
    "Failover": "SECONDARY",
    "TTL": 0,
    "ResourceRecords": [
        {
            "Value": "cell2.yourdomain.com"
        }
    ],
    "HealthCheckId": "yyyyyy-yyyy-yyyy-yyyy-yyyyyyyyyyyy"
}
```

Ahora, para realizar la conmutación por error de la celda principal a la celda secundaria, puede seguir el ejemplo de la CLI del paso 4b para actualizar el estado de `RoutingControlCell1` a `OFF` y de `RoutingControlCell2` a `ON`.

Enumere y actualice los controles y estados de enrutamiento con AWS CLI

Después de crear los recursos de Amazon Application Recovery Controller (ARC), como el clúster, los controles de enrutamiento y los paneles de control, puede interactuar con el clúster para enumerar y actualizar los estados de control de enrutamiento para la conmutación por error.

Para cada clúster que cree, ARC le proporciona un conjunto de puntos finales del clúster, uno de cada cinco. Regiones de AWS Debe especificar uno de estos puntos de enlace regionales (el Región de AWS y la URL del punto de enlace) al realizar llamadas al clúster para recuperar o establecer los estados de control de enrutamiento en o. `On` `Off` Cuando utilice el AWS CLI, para obtener o actualizar los estados del control de enrutamiento, además del punto final regional, también debe especificar el `--region` del punto final regional, como se muestra en los ejemplos de esta sección.

Puede utilizar cualquiera de los puntos de conexión regionales del clúster. Recomendamos que sus sistemas roten por los puntos de enlace regionales y que estén preparados para volver a intentarlo con cada uno de los puntos de enlace disponibles. Para ver ejemplos de código que ilustran cómo probar los puntos de conexión de un clúster de forma secuencial, consulte Acciones para Application Recovery Controller mediante AWS SDKs .

Para obtener más información sobre el uso del AWS CLI, consulte la AWS CLI Referencia de comandos. Para obtener una lista de las acciones de la API de configuración del enrutamiento y enlaces a más información, consulte Operaciones de la API de control de enrutamiento.

> **Important**
>
> Si bien puede actualizar un estado de control de enrutamiento en la consola de Amazon Route 53, le recomendamos que actualice los estados del control de enrutamiento mediante el AWS CLI uso de un AWS SDK. ARC ofrece una confiabilidad extrema con el plano de datos de control de enrutamiento ARC para redireccionar el tráfico y conmutar por error entre celdas. Para obtener más recomendaciones sobre el uso de ARC para la conmutación por error, consulte. Mejores prácticas para el control de enrutamiento en ARC

Al crear un control de enrutamiento, el estado se establece en `Off`. Esto significa que el tráfico no se enruta a la celda de destino para ese control de enrutamiento. Puede verificar el estado del control de enrutamiento mediante la ejecución del comando `get-routing-control-state`.

Para determinar la región y el punto final que se van a especificar, ejecute el `describe-clusters` comando para ver el `ClusterEndpoints`. Cada uno `ClusterEndpoint` incluye una región y el punto final correspondiente que puede usar para obtener o actualizar los estados del control de enrutamiento. DescribeClusteres una operación de API de configuración de control de recuperación. Le recomendamos que guarde una copia local de los puntos de conexión del clúster regional de ARC, en marcadores o codificada en el código de automatización que utilice para volver a probar los puntos de conexión.

1. Listar los controles de enrutamiento

Puede ver los controles de enrutamiento y los estados de control de enrutamiento utilizando los puntos de enlace del plano de datos ARC, altamente confiables.

1. Enumere los controles de enrutamiento de un determinado panel de control. Si no especifica un panel de control, `list-routing-controls` devuelve todos los controles de enrutamiento del clúster.

```
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. Obtenga controles de enrutamiento

2. Obtener el estado de un control de enrutamiento.

```
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. Actualice los controles de enrutamiento

Para dirigir el tráfico al punto de conexión de destino controlado por el control de enrutamiento, actualice el estado del control de enrutamiento a 0n. Ejecute el comando `update-routing-control-state` para actualizar el estado de control de enrutamiento (si la solicitud se realiza correctamente, la respuesta estará vacía).

2a. Actualizar el estado de un control de enrutamiento.

```
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
```

```
{}
```

Puede actualizar varios controles de enrutamiento al mismo tiempo con una llamada a la API: `update-routing-control-states`. (si la solicitud se realiza correctamente, la respuesta estará vacía).

2b. Actualice varios estados de control de enrutamiento a la vez (actualizaciones por lotes).

```
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
```

```
{}
```

Trabajar con componentes de control de enrutamiento en ARC

Temas

- Creación de componentes de control de enrutamiento en ARC
- Visualización y actualización de los estados de control de enrutamiento en ARC
- Crear reglas de seguridad para el control de rutas
- Support multicuenta para clústeres en ARC

Creación de componentes de control de enrutamiento en ARC

En esta sección se explica cómo crear un clúster, controles de enrutamiento, comprobaciones de estado y paneles de control para trabajar con el control de enrutamiento en Amazon Application Recovery Controller (ARC).

Comience por crear un clúster para alojar los controles de enrutamiento y los paneles de control que utiliza para agruparlos. A continuación, cree controles de enrutamiento y comprobaciones de estado para redirigir el tráfico para la conmutación por error de una celda a otra, de modo que el tráfico vaya a la réplica de copia de seguridad, por ejemplo.

Tenga en cuenta que se le cobra por hora por cada clúster que cree. Por lo general, solo se necesita un clúster para alojar los controles de enrutamiento y los paneles de control para la administración del control de recuperación de una aplicación. Además, puede configurar el uso AWS Resource Access Manager compartido de recursos de forma que un clúster pueda alojar los controles de enrutamiento y otros recursos de ARC que sean propiedad de varios Cuentas de AWS. Para obtener información sobre el uso compartido de recursos en ARC, Support multicuenta para clústeres en ARC. Para obtener información sobre precios, consulte los precios de Amazon Application Recovery Controller (ARC) y desplácese hacia abajo hasta Amazon Route 53.

Para utilizar los controles de enrutamiento para conmutar el tráfico por error, debe crear comprobaciones de estado de control de enrutamiento que asocie con los registros de DNS de Amazon Route 53 para los recurso de la aplicación. Por ejemplo, supongamos que tiene dos celdas, una que ha configurado como celda principal para la aplicación y la otra que ha configurado como secundaria para realizar la conmutación por error.

Para configurar las comprobaciones de estado para la conmutación por error, haga lo siguiente:

1. Cree un control de enrutamiento para cada celda.

2. Cree una comprobación de estado para cada control de enrutamiento.
3. Cree dos registros de DNS, por ejemplo, dos registros de conmutación por error de DNS y asocie una comprobación de estado a cada uno de ellos.

Otra situación en la que se puede crear un control de enrutamiento es cuando se crea una regla de seguridad que sea una regla de regulación. En este caso, no asocie las comprobaciones de estado ni los registros de DNS al control de enrutamiento porque las usará como un control de enrutamiento de regulación. Para obtener más información, consulte Crear reglas de seguridad para el control de rutas .

Los pasos para crear los componentes para el control de enrutamiento en la consola ARC se incluyen en estas secciones. Para obtener información sobre el uso de las operaciones de la API de configuración del control de recuperación con ARC, consulte la Operaciones de la API de control de enrutamiento.

Crear un clúster en ARC

Debe crear un clúster para alojar los controles de enrutamiento y los paneles de control en ARC.

Un clúster es un conjunto de puntos de conexión regionales redundantes desde los que puede ejecutar llamadas a la API para actualizar u obtener el estado de uno o varios controles de enrutamiento. Un solo clúster puede alojar varios controles de enrutamiento.

> **Important**
>
> Tenga en cuenta que se le cobra por hora por cada clúster que cree. Un clúster puede alojar una serie de controles de enrutamiento y paneles de control para la administración del control de recuperación de una aplicación, que suele ser suficiente para una aplicación.

Para crear un clúster

1. Abra la consola ARC enhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Seleccione Clusters (Clústeres).
3. Elija Crear e introduzca un nombre para su clúster.
4. Elija Create cluster.

Creación de un control de enrutamiento en ARC

Cree un control de enrutamiento para cada celda a la que desea dirigir el tráfico. Por ejemplo, si tiene una aplicación con recursos que ha almacenado en silos para poder recuperarlos, puede tener una celda para cada una y celdas anidadas para cada Región de AWS zona de disponibilidad dentro de cada región. En esta situación, debería crear un control de enrutamiento para cada celda y cada celda anidada.

Al crear controles de enrutamiento, tenga en cuenta que los nombres de los controles de enrutamiento deben ser únicos en cada panel de control.

Después de crear los controles de enrutamiento para redireccionar el tráfico, asocie cada uno de ellos a una comprobación de estado, lo que le permitirá dirigir el tráfico a las celdas, en función de los registros de DNS que haya asociado a cada una de ellas. Si va a configurar una regla de regulación como regla de seguridad y a crear un control de enrutamiento de regulación, no añada ninguna comprobación de estado al control de enrutamiento.

Para crear un control de enrutamiento

1. Abra la consola ARC en. https://console.aws.amazon.com/route53recovery/home#/dashboard
2. Elija el control de enrutamiento.
3. En la página Control de enrutamiento, elija Crear y, a continuación, un control de enrutamiento.
4. Introduzca un nombre para el control de enrutamiento, elija el clúster al que desee añadir el control y seleccione añadirlo a un panel de control existente, incluido el uso del panel de control predeterminado. O cree un panel de control nuevo.
5. Si opta por crear un panel de control nuevo, elija un clúster en el que crear el panel de control y, a continuación, introduzca un nombre para el panel.
6. Seleccione Crear control de enrutamiento.
7. Siga los pasos para asignar un nombre al control de enrutamiento y crearlo.

Crear una verificación de estado del control de enrutamiento en ARC

Debe asociar una comprobación de estado del control de enrutamiento a cada control de enrutamiento que desee utilizar para redireccionar el tráfico. A continuación, configure cada comprobación de estado con un registro de DNS de Amazon Route 53, por ejemplo, un registro de DNS de conmutación por error. A continuación, puede redirigir el tráfico en Amazon Application

Recovery Controller (ARC) simplemente actualizando el estado del control de enrutamiento asociado para configurarlo en o. `On` `Off`

> **Note**
>
> No puede editar ninguna comprobación de estado de control de enrutamiento existente para asociarla a un control de enrutamiento diferente.

Para crear una comprobación de estado de control de enrutamiento

1. Abra la consola ARC en. https://console.aws.amazon.com/route53recovery/home#/dashboard
2. Elija el control de enrutamiento.
3. En la página Control de enrutamiento, elija un control de enrutamiento.
4. En la página de detalles del control de enrutamiento, seleccione Crear comprobación de estado.
5. Introduzca un nombre para la comprobación de estado y luego elija Crear.

A continuación, cree los registros de DNS de Route 53 y asocie las comprobaciones de estado de control de enrutamiento a cada uno de ellos. Por ejemplo, supongamos que desea utilizar dos registros de conmutación por error de DNS a los que asociar las comprobaciones de estado de control de enrutamiento. Para que ARC conmute correctamente el tráfico por error mediante controles de enrutamiento, comience por crear los dos registros de conmutación por error en Route 53: uno principal y otro secundario. Para obtener más información sobre la configuración de los registros de conmutación por error de DNS, consulte Conceptos de comprobación de estado.

Al crear el registro de conmutación por error principal, los valores deberían ser similares a los siguientes:

```
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
```

Los valores del registro de conmutación por error secundario deberían parecerse a los que se indican a continuación:

```
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
```

Ahora, supongamos que quiere redirigir el tráfico porque se ha producido un error. Para ello, debe actualizar los estados de control de enrutamiento asociados para cambiar el estado de control de enrutamiento principal a `OFF` y el estado de control de enrutamiento secundario a `ON`. Al hacerlo, las comprobaciones de estado asociadas impiden que el tráfico vaya a la réplica principal y, en su lugar, lo dirigen a la réplica secundaria. Para obtener más información sobre la conmutación por error del tráfico con controles de enrutamiento, consulte Obtener y actualizar los estados de control de enrutamiento mediante la API ARC (recomendado).

Para ver ejemplos de los AWS CLI comandos para crear controles de enrutamiento y las comprobaciones de estado asociadas mediante las operaciones de la API ARC, consulte Ejemplos del uso de las operaciones de la API de control de enrutamiento ARC con AWS CLI.

Creación de un panel de control en ARC

Un panel de control en Amazon Application Recovery Controller (ARC) le permite agrupar los controles de enrutamiento relacionados. Un panel de control puede tener controles de enrutamiento que representen un microservicio de una aplicación, una aplicación completa en sí misma o un grupo de aplicaciones, en función del alcance de la conmutación por error. Una ventaja de agrupar los controles de enrutamiento en un panel de control es que puede utilizar las reglas de seguridad con un panel de control para proteger los cambios en el direccionamiento del tráfico.

Al crear un clúster, ARC crea un panel de control predeterminado. Puede usar el panel de control predeterminado para los controles de enrutamiento, o puede crear uno o varios paneles de control para agrupar los controles de enrutamiento. Tenga en cuenta que solo se admiten caracteres ASCII para los nombres de los paneles de control.

Los pasos para crear un panel de control en la consola ARC se incluyen en esta sección. Para obtener información sobre el uso de las operaciones de la API de configuración del control de recuperación con ARC, consulte la Operaciones de la API de control de enrutamiento.

Creación de un panel de control

1. Abra la consola ARC enhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Elija el control de enrutamiento.
3. En la página Control de enrutamiento, elija Crear y, a continuación, un control de panel.
4. Elija un clúster en el que crear el panel de control y, a continuación, introduzca un nombre para el panel.
5. Seleccione Crear panel de control.

Visualización y actualización de los estados de control de enrutamiento en ARC

En esta sección se describe cómo ver y actualizar los estados del control de enrutamiento en Amazon Application Recovery Controller (ARC). Los controles de enrutamiento son simples conmutadores de encendido y apagado que administran el flujo de tráfico a las celdas de su grupo de recuperación. Las celdas suelen ser zonas de disponibilidad Regiones de AWS, o algunas veces, que incluyen sus recursos. Si el estado de un control de enrutamiento es 0n, el tráfico fluye hacia la celda que está controlada por dicho control de enrutamiento.

Los controles de enrutamiento se agrupan en paneles de control, que son agrupaciones lógicas de conmutación por error. Al abrir un panel de control en la consola, por ejemplo, puede ver todos los controles de enrutamiento de una agrupación a la vez para ver por dónde fluye el tráfico.

Puede actualizar el estado del control de enrutamiento en la consola ARC o mediante la API ARC. Le recomendamos que actualice los estados del control de enrutamiento mediante la API. En primer lugar, ARC ofrece una fiabilidad extrema con la API en el plano de datos para realizar estas acciones. Esto es importante cuando se cambian estos estados, ya que los cambios de estado de enrutamiento conmutan por error entre las celdas al redirigir el tráfico de las aplicaciones. Además, al usar la API, puede intentar conectarse a diferentes puntos de conexión del clúster de forma rotativa, según sea necesario, si un punto de conexión del clúster al que intenta conectarse no está disponible.

Puede actualizar un estado de control de enrutamiento o puede actualizar varios estados de control de enrutamiento a la vez. Por ejemplo, es posible que desee establecer un estado de control

de enrutamiento en `Off` para impedir que el tráfico fluya hacia una celda, como una zona de disponibilidad en la que una aplicación experimenta un aumento de la latencia. Al mismo tiempo, es posible que desee establecer otro estado de control de enrutamiento en `On` para iniciar el flujo de tráfico a otra celda o zona de disponibilidad. En esta situación, puede actualizar ambos estados de control de enrutamiento a la vez para que el tráfico siga fluyendo.

Temas

- Obtener y actualizar los estados de control de enrutamiento mediante la API ARC (recomendado)
- Obtener y actualizar los estados de control de enrutamiento en el AWS Management Console

Obtener y actualizar los estados de control de enrutamiento mediante la API ARC (recomendado)

Le recomendamos que utilice las operaciones de la API de Amazon Application Recovery Controller (ARC) para obtener o actualizar los estados del control de enrutamiento mediante un AWS CLI comando o un código que haya desarrollado para utilizar las operaciones de la API ARC con una de las AWS SDKs. Recomendamos utilizar las operaciones de la API, con la CLI o en código, para trabajar con los estados de control de enrutamiento, en lugar de utilizar la AWS Management Console.

ARC ofrece una fiabilidad extrema para la conmutación por error entre celdas (Regiones de AWS) al actualizar los estados de control de enrutamiento mediante la API, ya que los controles de enrutamiento se almacenan en un clúster de alta disponibilidad. ARC garantiza que siempre pueda acceder al menos a tres de los cinco puntos finales del clúster regional para realizar cambios en el estado del control de enrutamiento. Para obtener o cambiar un estado de control de enrutamiento mediante la API, debe conectarse a uno de los puntos de conexión regionales del clúster. Si el punto de conexión no está disponible, puede intentar conectarse a otro de los puntos de conexión del clúster.

Puede ver la lista de puntos finales del clúster regionales de su clúster en la consola de Route 53 o mediante una acción de la API. DescribeCluster El proceso para obtener y cambiar los estados de control de enrutamiento debe estar preparado para probar cada punto de conexión de forma rotativa, según sea necesario, ya que los puntos de conexión del clúster pasan por los estados disponibles y no disponibles para su mantenimiento y actualización periódicos.

Proporcionamos información detallada y ejemplos de código para usar las operaciones de la API de ARC para obtener y actualizar los estados del control de enrutamiento y trabajar con los puntos de enlace de los clústeres regionales. Para obtener más información, consulte los siguientes temas:

- Para ver ejemplos de código que explican cómo rotar los puntos finales de un clúster regional para obtener y establecer los estados de control de enrutamiento, consulte Acciones para Application Recovery Controller mediante AWS SDKs .
- Para obtener información sobre el uso de AWS CLI para obtener y actualizar los estados de control de enrutamiento, consulte Enumere y actualice los controles y estados de enrutamiento con AWS CLI.

Obtener y actualizar los estados de control de enrutamiento en el AWS Management Console

Puede obtener y actualizar los estados de control de enrutamiento en la AWS Management Console. Sin embargo, tenga en cuenta que no puede elegir diferentes puntos de conexión regionales del clúster en la consola. Es decir, no existe un proceso para elegir y rotar los puntos de enlace del clúster en la consola, como se puede hacer con la API Amazon Application Recovery Controller (ARC). Además, la consola no tiene una alta disponibilidad, mientras que el plano de datos ARC ofrece una fiabilidad extrema. Por estos motivos, le recomendamos que utilice la API ARC para obtener y actualizar los estados de control de enrutamiento para las operaciones de producción.

Para obtener más recomendaciones sobre el uso de ARC para la conmutación por error, consulteMejores prácticas para el control de enrutamiento en ARC.

Para ver y actualizar los controles de enrutamiento en la consola, siga los pasos de los siguientes procedimientos.

Obtener el estado de un control de enrutamiento

1. Abra la consola ARC enhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Elija el control de enrutamiento.
3. En la lista, elija un panel de control y vea los controles de enrutamiento.

Para actualizar uno o varios estados de control de enrutamiento

1. Abre la consola Amazon Route 53 en https://console.aws.amazon.com/route53/casa.
2. En Application Recovery Controller, seleccione Control de enrutamiento .
3. Elija Acción y, a continuación, Cambiar enrutamiento de tráfico.
4. Actualice los estados de uno o varios controles de enrutamiento para que estén `Off` u `On`, según dónde desee que fluya o deje de fluir el tráfico para la aplicación.
5. Escriba `confirm` en el cuadro de texto.

6. Seleccione Actualizar enrutamiento de tráfico.

Crear reglas de seguridad para el control de rutas

Cuando trabaja con varios controles de enrutamiento al mismo tiempo, puede decidir que desea establecer medidas de seguridad para evitar consecuencias imprevistas. Por ejemplo, es posible que desee evitar que se desactiven por error todos los controles de enrutamiento de una aplicación, lo que provocaría un fallo de apertura. O tal vez desee implementar un conmutador principal de encendido o apagado para deshabilitar un conjunto de controles de enrutamiento, tal vez para evitar que la automatización desvíe el tráfico. Para establecer medidas de seguridad como estas para el control de enrutamiento en ARC, debe crear reglas de seguridad.

Las reglas de seguridad para el control de enrutamiento se configuran con una combinación de controles de enrutamiento, reglas y otras opciones que especifique. Cada regla de seguridad está asociada a un único panel de control, pero un panel de control puede tener más de una regla de seguridad. Al crear reglas de seguridad, tenga en cuenta que los nombres de las reglas de seguridad deben ser únicos en cada panel de control.

Temas

- Tipos de reglas de seguridad
- Creación de una regla de seguridad en la consola
- Modificación o eliminación de una regla de seguridad en la consola
- Anulación de las reglas de seguridad para redirigir el tráfico

Tipos de reglas de seguridad

Existen dos tipos de reglas de seguridad, las reglas de aserción y las reglas de regulación, que se pueden utilizar para proteger la conmutación por error de diferentes maneras.

Regla de aserción

Con una regla de aserción, cuando cambias uno o un conjunto de estados de control de enrutamiento, ARC exige que se cumplan los criterios que estableciste al configurar la regla o, de lo contrario, no cambiarán los estados del control de enrutamiento.

Por ejemplo, esto es útil para evitar una apertura por error, como una situación en la que se detiene el tráfico que va a una celda pero no se inicia el flujo de tráfico a otra celda. Para evitar esto, una regla de aserción garantiza que al menos un control de enrutamiento de un conjunto

de controles de enrutamiento en un panel de control esté establecido en On en un momento dado. Esto garantiza que el tráfico fluya al menos a una región o zona de disponibilidad de una aplicación.

Para ver un ejemplo de AWS CLI comando que crea una regla de aserción para hacer cumplir este criterio, consulte Crear reglas de seguridad en. Ejemplos del uso de las operaciones de la API de control de enrutamiento ARC con AWS CLI

Para obtener información detallada sobre las propiedades de operación de la API de reglas de aserción, consulte AssertionRulela Guía de referencia de la API de control de enrutamiento para Amazon Application Recovery Controller.

Regla de regulación

Con una regla de regulación, puede aplicar un conmutador general de encendido o apagado en un conjunto de controles de enrutamiento, de modo que se aplique si esos estados de control de enrutamiento se pueden cambiar en función de un conjunto de criterios que especifique en la regla. El criterio más simple es si un único control de enrutamiento que especifique como conmutador está configurado en `ON` o `OFF`.

Para implementar esto, debe crear un control de enrutamiento de regulación, que se utilizará como conmutador general, y controles de enrutamiento de destino para controlar el flujo de tráfico a diferentes regiones o zonas de disponibilidad. A continuación, para evitar que se actualicen de forma manual o automática los controles de enrutamiento de destino que haya configurado para la regla de bloqueo, defina el estado del control de enrutamiento en `Off`. Para permitir las actualizaciones, debe establecerse en On.

Para ver un ejemplo de AWS CLI comando que crea una regla de control que implementa este tipo de cambio general, consulte Crear reglas de seguridad en Ejemplos del uso de las operaciones de la API de control de enrutamiento ARC con AWS CLI.

Para obtener información detallada sobre las propiedades de operación de la API de reglas de bloqueo, consulte GatingRulela Guía de referencia de la API de control de enrutamiento para Amazon Application Recovery Controller.

Creación de una regla de seguridad en la consola

En los pasos de esta sección se explica cómo crear una regla de seguridad en la consola ARC. Los pasos son similares tanto si se crea una regla de aserción como si se crea una regla de regulación. Las diferencias se indican en el procedimiento.

Para obtener información sobre el uso de las operaciones de la API de control de enrutamiento y recuperación con Amazon Application Recovery Controller (ARC), consulte Operaciones de la API de control de enrutamiento.

Creación de una regla de seguridad

1. Abra la consola ARC enhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Elija el control de enrutamiento.
3. En la página Control de enrutamiento, elija un panel de control.
4. En la página de detalles del panel de control, seleccione Acción y, a continuación, Añadir regla de seguridad.
5. Elija el tipo de regla que desee añadir: Regla de aserción o Regla de regulación.
6. Elija un nombre y, si lo desea, cambie el periodo de espera.
7. Especifique las opciones de configuración de la regla de seguridad.

   - En el caso una regla de aserción, especifique los controles de enrutamiento certificados.
   - En el caso de una regla de regulación, especifique el control de enrutamiento de regulación y los controles de enrutamiento de destino.

   Para ambas reglas, especifique la configuración de la regla eligiendo el tipo y el umbral, y si la regla se invierte.

   > **Note**
   >
   > Para obtener más información sobre cómo especificar una regla de aserción, consulte la información sobre el AssertionRulefuncionamiento en la Guía de referencia de la API de control de enrutamiento para Amazon Application Recovery Controller. Para obtener más información sobre cómo especificar una regla de bloqueo, consulte la información proporcionada sobre la GatingRuleoperación en la Guía de referencia de la API de control de enrutamiento para Amazon Application Recovery Controller.

8. Seleccione Crear.

Modificación o eliminación de una regla de seguridad en la consola

Los pasos de esta sección explican cómo editar o eliminar una regla de seguridad en la consola ARC. Solo puede realizar modificaciones limitadas en una regla de seguridad, cambiar el nombre o actualizar el periodo de espera. Para realizar otros cambios, elimine y vuelva a crear la regla de seguridad.

Para obtener información sobre el uso de las operaciones de API con Amazon Application Recovery Controller (ARC), consulte la Operaciones de la API de control de enrutamiento.

Eliminación de una regla de seguridad

1. Abra la consola ARC enhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Elija el control de enrutamiento.
3. En la página Control de enrutamiento, elija un panel de control.
4. En la página de detalles del panel de control, elija una regla de seguridad y, a continuación, Eliminar o Editar.

Anulación de las reglas de seguridad para redirigir el tráfico

Hay situaciones en las que es posible que desee omitir las medidas de control de enrutamiento que se aplican con las reglas de seguridad que ha configurado. Por ejemplo, es posible que quiera realizar rápidamente una conmutación por error para recuperarse de un desastre, y una o más reglas de seguridad podrían impedir inesperadamente la actualización del estado del control de enrutamiento para redirigir el tráfico. En una situación “de emergencia” como esta, puede anular una o varias reglas de seguridad para cambiar el estado del control de enrutamiento y realizar una conmutación por error de la aplicación.

Puede omitir las reglas de seguridad al actualizar un estado de control de enrutamiento (o varios estados de control de enrutamiento) mediante el `update-routing-control-states` AWS CLI comando `update-routing-control-state` o con el `safety-rules-to-override` parámetro. Especifique el parámetro con el nombre de recurso de Amazon (ARN) de la regla de seguridad que desee anular o especifique una lista separada por comas ARNs para anular dos o más reglas de seguridad.

Cuando una regla de seguridad bloquea una actualización del estado del control de enrutamiento, el mensaje de error incluirá el ARN de la regla que bloqueó la actualización. De este modo, puede anotar el ARN y, a continuación, especificarlo en un comando de la CLI del estado de control de enrutamiento con el parámetro de anulación de la regla de seguridad.

> **Note**
>
> Dado que es posible que haya más de una regla de seguridad para los controles de enrutamiento que está actualizando, puede ejecutar el comando de la CLI para actualizar el estado del control de enrutamiento mediante la anulación de una regla de seguridad, pero recibirá un error que indicará que otra regla de seguridad bloquea la actualización. Siga añadiendo la regla de seguridad ARNs a la lista de reglas que desee anular en el comando de actualización, separadas por comas, hasta que el comando de actualización se complete correctamente.

Para obtener más información sobre el uso de la `SafetyRulesToOverride` propiedad con la API SDKs, consulte. UpdateRoutingControlState

A continuación se muestran dos ejemplos de comandos de la CLI para anular las reglas de seguridad y actualizar los estados de control de enrutamiento.

Anulación de una regla de seguridad

```
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
```

Anulación de dos reglas de seguridad

```
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
```

Support multicuenta para clústeres en ARC

Amazon Application Recovery Controller (ARC) se integra AWS Resource Access Manager para permitir el uso compartido de recursos. AWS RAM es un servicio que le permite compartir recursos con otros Cuentas de AWS o a través de ellos AWS Organizations. Para el control de enrutamiento ARC, puede compartir el recurso del clúster.

Con AWS RAM, puede compartir los recursos de su propiedad mediante la creación de un recurso compartido. Un uso compartido de recursos especifica los recursos que compartir y los consumidores con quienes compartirlos. Los participantes pueden incluir:

- Cuentas de AWS Específico dentro o fuera de la organización del propietario en AWS Organizations
- Una unidad organizativa dentro de su organización en AWS Organizations
- Toda su organización en AWS Organizations

Para obtener más información al respecto AWS RAM, consulte la Guía AWS RAM del usuario.

Si se utiliza AWS Resource Access Manager para compartir los recursos del clúster entre las cuentas de ARC, puede utilizar un clúster para alojar los paneles de control y los controles de enrutamiento propiedad de varias personas Cuentas de AWS. Si opta por compartir un clúster, las demás personas Cuentas de AWS que especifique pueden utilizar el clúster para alojar sus propios paneles de control y controles de enrutamiento, lo que permite un mayor control y flexibilidad sobre las capacidades de enrutamiento entre los diferentes equipos.

AWS RAM es un servicio que ayuda a AWS los clientes a compartir recursos de forma segura entre ellos Cuentas de AWS. Con AWS RAMél, puede compartir recursos dentro de una organización o unidades organizativas (OUs) mediante funciones y usuarios de IAM. AWS Organizations AWS RAM es una forma centralizada y controlada de compartir un clúster.

Al compartir un clúster, puede reducir la cantidad total de clústeres que necesita su organización. Con un clúster compartido, puede asignar el costo total del funcionamiento del clúster a diferentes equipos para maximizar los beneficios del ARC con un menor costo. (la creación de recursos

alojados en un clúster no implica costos adicionales, ni para el propietario ni para los participantes). Compartir clústeres entre cuentas también puede facilitar el proceso de incorporación de varias aplicaciones a ARC, especialmente si tiene una gran cantidad de aplicaciones distribuidas en varias cuentas y equipos de operaciones.

Para empezar a compartir recursos entre cuentas en ARC, debe crear un recurso compartido en. AWS RAM El recurso compartido especifica los participantes que están autorizados a compartir el clúster que pertenece a su cuenta. A continuación, los participantes pueden crear recursos, como paneles de control y controles de enrutamiento, en el clúster mediante AWS Management Console o ejecutando operaciones de la API de ARC mediante AWS Command Line Interface o AWS SDKs.

En este tema se explica cómo compartir los recursos que le pertenecen y cómo utilizar los recursos que se comparten con usted.

Contenido

- Requisitos previos para compartir clústeres
- Uso compartido de un clúster
- Dejar de compartir un clúster compartido
- Identificación de un clúster compartido
- Responsabilidades y permisos de clústeres compartidos
- Costes de facturación
- Cuotas

Requisitos previos para compartir clústeres

- Para compartir un clúster, debes tenerlo en tu Cuenta de AWS. Esto significa que el recurso debe asignarse o suministrarse en su cuenta. No puede compartir un clúster que se ha compartido con usted.
- Para compartir un clúster con su organización o con una unidad organizativa en AWS Organizations, debe habilitar el uso compartido con AWS Organizations. Para obtener más información, consulte Habilitar el uso compartido con AWS Organizations en la Guía del usuario de AWS RAM .

Uso compartido de un clúster

Cuando compartes un clúster de tu propiedad, los participantes que especifiques para compartir el clúster pueden crear y alojar sus propios recursos de ARC en el clúster.

Para compartir un clúster, debe añadirlo al recurso compartido. Un uso compartido de recursos es un recurso de AWS RAM que le permite compartir los recursos a través de Cuentas de AWS. Un uso compartido de recursos especifica los recursos que compartir y los participantes con los que compartirlos. Para compartir un clúster, puede crear un nuevo uso compartido de recursos o añadir el recurso a un uso compartido existente. Para crear un nuevo recurso compartido, puedes usar la AWS RAM consola o usar las operaciones de la AWS RAM API con la tecla AWS Command Line Interface o AWS SDKs.

Si forma parte de una organización AWS Organizations y está habilitado el uso compartido dentro de su organización, los participantes de su organización tienen acceso automático al clúster compartido. De lo contrario, los participantes reciben una invitación para unirse al uso compartido de recursos y se les concede acceso al clúster compartido después de aceptar la invitación.

Puedes compartir un clúster de tu propiedad mediante la AWS RAM consola o mediante las operaciones de la AWS RAM API con AWS CLI o SDKs.

Para compartir un clúster de tu propiedad mediante la AWS RAM consola

Consulte Creación de un uso compartido de recursos en la Guía del usuario de AWS RAM .

Para compartir un clúster de tu propiedad mediante el AWS CLI

Utilice el comando create-resource-share.

Otorgar permisos para compartir clústeres

Para compartir clústeres entre cuentas se requieren permisos para el principal de IAM mediante AWS RAM el cual se comparte el clúster.

Te recomendamos que utilices la política de IAM `AmazonRoute53RecoveryControlConfigFullAccess` gestionada para garantizar que tus directores de IAM dispongan de los permisos necesarios para compartir y utilizar clústeres compartidos.

Compartir un clúster mediante una política de IAM personalizada requiere `route53-recovery-control-config:PutResourcePolicy` y `route53-recovery-control-config:DeleteResourcePolicy` permisos para `route53-recovery-control-`

`config:GetResourcePolicy` ese clúster. `PutResourcePolicy`y `DeleteResourcePolicy` son acciones de IAM que solo requieren permisos. Si se intenta compartir un clúster AWS RAM sin disponer de estos permisos, se producirá un error.

Para obtener más información sobre la forma en que se AWS Resource Access Manager usa IAM, consulte Cómo se AWS Resource Access Manager usa IAM en la Guía del AWS RAM usuario.

Dejar de compartir un clúster compartido

Al dejar de compartir un clúster, se aplica lo siguiente a los participantes y propietarios:

- Los recursos existentes de los participantes siguen existiendo en el clúster que se ha dejado de compartir.
- Los participantes pueden seguir actualizando los estados de control de enrutamiento en el clúster no compartido para administrar el enrutamiento y la conmutación por error de las aplicaciones.
- Los participantes ya no pueden crear nuevos recursos en el clúster que se ha dejado de compartir.
- Si los participantes siguen teniendo recursos en un clúster que se ha dejado de compartir, el propietario no puede eliminar el clúster compartido.

Para dejar de compartir un clúster compartido de su propiedad, debe eliminarlo del uso compartido de recursos. Puede hacerlo mediante la AWS RAM consola o mediante operaciones de AWS RAM API con la AWS CLI tecla o. SDKs

Para dejar de compartir un clúster compartido de tu propiedad mediante la consola AWS RAM

Consulte Actualización de un recurso compartido en la Guía del usuario de AWS RAM .

Para dejar de compartir un clúster compartido de tu propiedad mediante el AWS CLI

Utilice el comando disassociate-resource-share.

Identificación de un clúster compartido

Los propietarios y los participantes deben consultar la información en AWS RAM para identificar los clústeres compartidos. También pueden obtener información sobre los recursos compartidos mediante la consola ARC y AWS CLI.

En general, para obtener más información sobre los recursos que ha compartido o que se han compartido con usted, consulte la información en la Guía del AWS Resource Access Manager usuario:

- Como propietario, puede ver todos los recursos que comparte con otros usuarios mediante AWS RAM. Para obtener más información, consulte Visualización de los recursos compartidos en AWS RAM.
- Como participante, puede ver todos los recursos que se han compartido con usted utilizando AWS RAM. Para obtener más información, consulte Visualización de los recursos compartidos en AWS RAM.

Como propietario, puede determinar si está compartiendo un clúster consultando la información de las operaciones de la API ARC AWS Management Console o utilizándolas AWS Command Line Interface con ellas.

Para identificar si un clúster de su propiedad se comparte mediante la consola

En la AWS Management Console página de detalles de un clúster, consulta el estado de uso compartido del clúster.

Para identificar si un clúster de tu propiedad está compartido mediante el AWS CLI

Utilice el get-resource-policycomando. Si un clúster tiene una política de recursos, el comando devuelve información sobre la política.

Como participante, cuando un clúster se comparte con usted, por lo general, debe aceptarlo. Además, el campo Propietario del clúster incluye la cuenta del propietario del clúster.

Responsabilidades y permisos de clústeres compartidos

Permisos de los propietarios

Cuando compartes un clúster que te pertenece con otros Cuentas de AWS, los participantes a los que se les permite usar el clúster pueden crear paneles de control, controles de enrutamiento y otros recursos en el clúster.

Como propietario de un clúster, es responsable de crear, administrar y eliminar los clústeres. No puede modificar ni eliminar los recursos creados por los participantes, tales como controles de rutas y reglas de seguridad. Por ejemplo, no puede actualizar un control de enrutamiento creado por un participante para cambiar su estado.

Sin embargo, puede ver los detalles de los controles de enrutamiento creados por los participantes de un clúster que sea de su propiedad. Por ejemplo, puede ver los estados del control de

enrutamiento llamando a una operación de la API de control de enrutamiento de ARC mediante la AWS Command Line Interface tecla o AWS SDKs.

Si necesita modificar los recursos creados por los participantes, estos pueden configurar un rol en IAM con permiso para acceder a los recursos y añadir su cuenta al rol.

Permisos para los participantes

En general, los participantes pueden crear y usar paneles de control, controles de rutas, reglas de seguridad y comprobaciones de estado que creen en un clúster compartido con ellos. Solo pueden ver, modificar o eliminar los recursos del clúster compartido si son los propietarios de los recursos. Por ejemplo, los participantes pueden crear y eliminar reglas de seguridad para los paneles de control que hayan creado.

Las siguientes restricciones se aplican a los participantes:

- Los participantes no pueden ver, modificar ni eliminar los paneles de control creados por otras cuentas que utilicen un clúster compartido.
- Los participantes no pueden ver, crear ni modificar los controles de enrutamiento, incluidos los estados de control de enrutamiento, para los recursos creados en un clúster compartido por otras cuentas.
- Los participantes no pueden crear, modificar ni ver las reglas de seguridad creadas por otras cuentas de un clúster compartido.
- Los participantes no pueden añadir recursos en el panel de control predeterminado de un clúster compartido porque pertenece al propietario del clúster.

Tal y como se ha indicado, los participantes no pueden crear controles de enrutamiento en el panel de control predeterminado para un clúster compartido, ya que el propietario del clúster es el propietario del panel de control predeterminado. Sin embargo, el propietario del clúster puede crear un rol de IAM entre cuentas que proporcione permiso para acceder al panel de control predeterminado del clúster. A continuación, el propietario puede conceder a un participante permisos para que asuma el rol, de modo que este pueda acceder al panel de control predeterminado y usarlo de la forma que el propietario haya especificado mediante los permisos del rol.

Costes de facturación

Al propietario de un clúster en ARC se le facturan los costes asociados al clúster. La creación de recursos alojados en un clúster no conlleva costos adicionales para los propietarios ni para los participantes.

Para obtener información detallada sobre precios y ejemplos, consulte los precios de Amazon Application Recovery Controller (ARC) y desplácese hacia abajo hasta Amazon Application Recovery Controller (ARC).

Cuotas

Todos los recursos creados en un clúster compartido, incluidos los recursos creados por todos los participantes con acceso al clúster compartido, se incluyen en las cuotas vigentes para el clúster y otros recursos, como, por ejemplo, los controles de enrutamiento. Si las cuentas que comparten el recurso del clúster tienen una cuota superior a las cuotas del propietario del clúster, las cuotas del propietario del clúster tienen prioridad sobre las cuotas de las cuentas que comparten.

Para entender mejor cómo funciona esto, consulta los siguientes ejemplos. Para ilustrar cómo funcionan las cuotas al compartir recursos, en estos ejemplos, supongamos que el propietario del clúster es el propietario y la cuenta con la que se ha compartido el clúster es Participant.

Cuota de los paneles de control

Se imponen cuotas para el total de paneles de control del propietario por clúster.

Por ejemplo, supongamos que el propietario tiene una cuota de 50 paneles de control por clúster y tiene 13 paneles de control en el clúster. Ahora, supongamos que el Participante tiene la cuota establecida en 150. En este escenario, Participant solo puede crear hasta 37 paneles de control (es decir, entre 50 y 13) en el clúster compartido.

Además, si otras cuentas que comparten el clúster también crean paneles de control, todas esas cuentas también se tienen en cuenta para la cuota total del clúster de 50 paneles de control.

Cuotas de control de enrutamiento

Los controles de enrutamiento tienen varias cuotas: una cuota por panel de control, una cuota por clúster y una cuota por regla de seguridad. Las cuotas de propietario tienen prioridad en todas estas cuotas.

Por ejemplo, supongamos que el propietario tiene una cuota de 300 controles de enrutamiento por clúster y ya tiene 300 controles de enrutamiento en el clúster. Ahora, supongamos que Participant tiene esta cuota establecida en 500. En este escenario, Participant no puede crear ningún control de enrutamiento nuevo en el clúster compartido.

Normas de seguridad, cuotas

Se aplican cuotas según las normas de seguridad del propietario por cuota del panel de control.

Por ejemplo, supongamos que el propietario tiene una cuota de 20 para el número de normas de seguridad por panel de control y el participante tiene establecida esta cuota en 80. En este escenario, dado que el límite inferior del propietario tiene prioridad, el Participante solo puede crear hasta 20 reglas de seguridad en un panel de control del clúster compartido.

Para obtener una lista de las cuotas de control de enrutamiento, consulteCuotas para el control de enrutamiento.

Registro y supervisión para el control de enrutamiento en Amazon Application Recovery Controller (ARC)

Puede usarlo AWS CloudTrail para monitorear el control de enrutamiento en Amazon Application Recovery Controller (ARC), para analizar patrones y ayudar a solucionar problemas.

Temas

- Registro de llamadas a la API ARC mediante AWS CloudTrail

Registro de llamadas a la API ARC mediante AWS CloudTrail

está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en ARC. CloudTrail captura todas las llamadas a la API de ARC como eventos. Las llamadas capturadas incluyen llamadas desde la consola ARC y llamadas en código a las operaciones de la API ARC.

Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos de ARC. Si no configura una ruta, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos.

Con la información recopilada por CloudTrail, puede determinar la solicitud que se realizó a ARC, la dirección IP desde la que se realizó la solicitud, quién la hizo, cuándo se realizó y detalles adicionales.

Para obtener más información CloudTrail, consulte la Guía AWS CloudTrail del usuario.

Información sobre ARC en CloudTrail

CloudTrail está habilitada en tu cuenta Cuenta de AWS al crear la cuenta. Cuando se produce una actividad en ARC, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS

servicio en el historial de eventos. Puede ver, buscar y descargar eventos recientes en su Cuenta de AWS. Para obtener más información, consulte Trabajar con el historial de CloudTrail eventos.

Para tener un registro continuo de tus eventos Cuenta de AWS, incluidos los eventos de ARC, crea una ruta. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las Regiones de AWS. La ruta registra los eventos de todas las regiones de la AWS partición y envía los archivos de registro al bucket de Amazon S3 que especifique. Además, puede configurar otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para más información, consulte los siguientes temas:

- Introducción a la creación de registros de seguimiento
- CloudTrail servicios e integraciones compatibles
- Configuración de las notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de CloudTrail registro de varias regiones y recibir archivos de CloudTrail registro de varias cuentas

Todas las acciones de ARC se registran CloudTrail y documentan en la Guía de referencia de la API de preparación de recuperación para Amazon Application Recovery Controller, la Guía de referencia de la API de configuración de control de recuperación para Amazon Application Recovery Controller y la Guía de referencia de la API de control de enrutamiento para Amazon Application Recovery Controller. Por ejemplo, las llamadas a `UpdateRoutingControlState` y `CreateRecoveryGroup` las acciones generan entradas en los archivos de CloudTrail registro. `CreateCluster`

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con credenciales de usuario root o AWS Identity and Access Management (IAM).
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro AWS servicio.

Para obtener más información, consulte el elemento userIdentity de CloudTrail .

Visualización de eventos ARC en el historial de eventos

CloudTrail le permite ver los eventos recientes en el historial de eventos. Para ver los eventos de las solicitudes de la API ARC, debe seleccionar EE.UU. Oeste (Oregón) en el selector de regiones situado en la parte superior de la consola. Para obtener más información, consulte Cómo trabajar con el historial de CloudTrail eventos en la Guía del AWS CloudTrail usuario.

Descripción de las entradas de los archivos de registro ARC

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

El siguiente ejemplo muestra una entrada de CloudTrail registro que demuestra la `CreateCluster` acción para configurar el control de enrutamiento.


```
{
  "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"
}
```

El siguiente ejemplo muestra una entrada de CloudTrail registro que demuestra la `UpdateRoutingControlState` acción del control de enrutamiento.

```
{
  "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 para el control de enrutamiento en

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a los AWS recursos. Los administradores de IAM controlan quién puede autenticarse (iniciar sesión) y quién puede autorizarse (tener permisos) para usar los recursos de ARC. La IAM es una Servicio de AWS opción que puede utilizar sin coste adicional.

Contenido

- Cómo funciona el control de enrutamiento de Amazon Application Recovery Controller (ARC) con IAM
- Ejemplos de políticas basadas en la identidad para el control de enrutamiento en ARC
- AWS políticas administradas para el control de enrutamiento en Amazon Application Recovery Controller (ARC)

Cómo funciona el control de enrutamiento de Amazon Application Recovery Controller (ARC) con IAM

Antes de usar IAM para administrar el acceso al control de enrutamiento en Amazon Application Recovery Controller (ARC), conozca qué funciones de IAM están disponibles para usar con el control de enrutamiento.

Funciones de IAM que puede utilizar con el control de enrutamiento en Amazon Application Recovery Controller (ARC)

Característica de IAM	Soporte de control de enrutamiento
Políticas basadas en identidades	Sí
Políticas basadas en recursos	No
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política	Sí
ACLs	No

Característica de IAM	Soporte de control de enrutamiento
ABAC (etiquetas en políticas)	Parcial
Credenciales temporales	Sí
Permisos de entidades principales	Sí
Roles de servicio	No
Roles vinculados al servicio	No

Para obtener una visión general y de alto nivel del funcionamiento de AWS los servicios con la mayoría de las funciones de IAM, consulte AWS los servicios que funcionan con IAM en la Guía del usuario de IAM.

Políticas de ARC basadas en la identidad

Compatibilidad con las políticas basadas en identidad: sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está asociada. Para obtener más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de las políticas de JSON de IAM en la Guía del usuario de IAM.

Para ver ejemplos de políticas ARC basadas en la identidad para el control del enrutamiento, consulte. Ejemplos de políticas basadas en la identidad para el control de enrutamiento en ARC

Políticas basadas en recursos dentro del control de enrutamiento

Admite políticas basadas en recursos: no

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico.

Acciones políticas para el control del enrutamiento

Compatibilidad con las acciones de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Las acciones políticas suelen tener el mismo nombre que la operación de AWS API asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de acciones de ARC para el control de enrutamiento, consulte Acciones definidas por los controles de recuperación de Amazon Route 53 y Acciones definidas por el clúster de recuperación de Amazon Route 53 en la Referencia de autorización de servicio.

Las acciones políticas de ARC para el control del enrutamiento utilizan los siguientes prefijos antes de la acción, en función de la API con la que esté trabajando:

```
route53-recovery-control-config
route53-recovery-cluster
```

Para especificar varias acciones en una única instrucción, sepárelas con comas. Por ejemplo, podría hacer lo siguiente:

```
"Action": [
      "route53-recovery-control-config:action1",
      "route53-recovery-control-config:action2"
         ]
```

Puede utilizar caracteres comodín (*) para especificar varias acciones . Por ejemplo, para especificar todas las acciones que comiencen con la palabra `Describe`, incluya la siguiente acción:

```
"Action": "route53-recovery-control-config:Describe*"
```

Para ver ejemplos de políticas de ARC basadas en la identidad para el control de enrutamiento, consulte. Ejemplos de políticas basadas en la identidad para el control de enrutamiento en ARC

Recursos de políticas para ARC

Compatibilidad con los recursos de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puedes realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puedes hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utiliza un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

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

En la Referencia de autorización de servicios, puede ver la siguiente información relacionada con ARC:

Para ver una lista de los tipos de recursos y sus acciones ARNs, así como las acciones que puede especificar con el ARN de cada recurso, consulte los siguientes temas en la Referencia de autorización de servicios:

- Acciones definidas por Amazon Route 53 Recovery Controls
- Acciones definidas por el clúster de recuperación de Amazon Route 53.

Para ver ejemplos de políticas ARC basadas en la identidad para el control de enrutamiento, consulte. Ejemplos de políticas basadas en la identidad para el control de enrutamiento en ARC

Claves de condición de la política para ARC

Compatibilidad con claves de condición de políticas específicas del servicio: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puedes realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puedes crear expresiones condicionales que utilizan operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación `AND` lógica. Si especifica varios valores para una única clave de condición, AWS evalúa la condición mediante una `OR` operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puedes utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puedes conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para más información, consulta Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

Para ver una lista de las claves de condición ARC para el control de enrutamiento, consulte los siguientes temas en la Referencia de autorización de servicio:

- Claves de condición de Amazon Route 53 Recovery Controls
- Claves de condición de Amazon Route 53 Recovery Cluster

Para ver las acciones y los recursos que puede usar con una clave de condición, consulte los siguientes temas de la Referencia de autorización de servicios:

- Para ver una lista de los tipos de recursos y sus correspondientes ARNs, consulte Acciones definidas por los controles de recuperación de Amazon Route 53 y Acciones definidas por el clúster de recuperación de Amazon Route 53.
- Para ver una lista de las acciones que puede especificar con el ARN de cada recurso, consulte Recursos definidos por los controles de recuperación de Amazon Route 53 y Recursos definidos por el clúster de recuperación de Amazon Route 53.

Para ver ejemplos de políticas ARC basadas en la identidad para el control de enrutamiento, consulte Ejemplos de políticas basadas en la identidad para el control de enrutamiento en ARC

Listas de control de acceso (ACLs) en ARC

Soporta ACLs: No

Las listas de control de acceso (ACLs) controlan qué directores (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLs son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Control de acceso basado en atributos (ABAC) con ARC

Compatibilidad con ABAC (etiquetas en las políticas): parcial

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos. En AWS, estos atributos se denominan etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a muchos AWS recursos. El etiquetado de entidades y recursos es el primer paso de ABAC. A continuación, designa las políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso al que se intenta acceder.

ABAC es útil en entornos que crecen con rapidez y ayuda en situaciones en las que la administración de las políticas resulta engorrosa.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte Definición de permisos con la autorización de ABAC en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

El control de enrutamiento ARC incluye el siguiente soporte para ABAC:

- Recovery Control Config es compatible con ABAC.
- Recovery Cluster no es compatible con ABAC.

Uso de credenciales temporales con ARC

Compatibilidad con credenciales temporales: sí

Algunas Servicios de AWS no funcionan cuando inicias sesión con credenciales temporales. Para obtener información adicional, incluida la información sobre cuáles Servicios de AWS funcionan con credenciales temporales, consulta Cómo Servicios de AWS funcionan con IAM en la Guía del usuario de IAM.

Utiliza credenciales temporales si inicia sesión en ellas AWS Management Console mediante cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accedes AWS mediante el enlace de inicio de sesión único (SSO) de tu empresa, ese proceso crea automáticamente credenciales temporales. También crea credenciales temporales de forma automática cuando inicia sesión en la consola como usuario y luego cambia de rol. Para obtener más información sobre el cambio de roles, consulte Cambio de un usuario a un rol de IAM (consola) en la Guía del usuario de IAM.

Puedes crear credenciales temporales manualmente mediante la AWS CLI API o. AWS A continuación, puede utilizar esas credenciales temporales para acceder AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para obtener más información, consulte Credenciales de seguridad temporales en IAM.

Permisos principales entre servicios para ARC

Admite sesiones de acceso directo (FAS): sí

Cuando utiliza una entidad de IAM (usuario o rol) para realizar acciones en ella AWS, se le considera principal. Las políticas conceden permisos a una entidad principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. En este caso, debe tener permisos para realizar ambas acciones.

Para ver si una acción requiere acciones dependientes adicionales en una política, consulte los siguientes temas en la Referencia de autorizaciones de servicio.

- Amazon Route 53 Recovery Cluster
- Amazon Route 53 Recovery Controls

Funciones de servicio para ARC

Compatible con roles de servicio: No

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

Funciones vinculadas al servicio para ARC

Admite roles vinculados al servicio:

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un servicio. AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en su AWS cuenta y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

El control de enrutamiento no usa roles vinculados al servicio.

Ejemplos de políticas basadas en la identidad para el control de enrutamiento en ARC

De forma predeterminada, los usuarios y los roles no tienen permiso para crear o modificar los recursos de ARC. Tampoco pueden realizar tareas mediante la AWS Management Console, AWS Command Line Interface (AWS CLI) o la AWS API. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puedes añadir las políticas de IAM a roles y los usuarios puedes asumirlos.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM (consola) en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos por ARC, incluido el ARNs formato de cada uno de los tipos de recursos, consulte Acciones, recursos y claves de condición de Amazon Application Recovery Controller (ARC) en la Referencia de autorización de servicios.

Temas

- Prácticas recomendadas sobre las políticas
- Ejemplo: acceso a la consola ARC para el control de enrutamiento
- Ejemplos: acciones de la API ARC para la configuración del control de enrutamiento

Prácticas recomendadas sobre las políticas

Las políticas basadas en la identidad determinan si alguien puede crear, eliminar o acceder a los recursos de ARC de su cuenta. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulta las políticas administradas por AWS o las políticas administradas por AWS para funciones de tarea en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulta Políticas y permisos en IAM en la Guía del usuario de IAM.
- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo AWS CloudFormation. Para obtener más información, consulta Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utiliza el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Validación de políticas con el Analizador de acceso de IAM en la Guía del usuario de IAM.
- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para exigir la MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para más información, consulte Acceso seguro a la API con MFA en la Guía del usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Ejemplo: acceso a la consola ARC para el control de enrutamiento

Para acceder a la consola Amazon Application Recovery Controller (ARC), debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre los recursos ARC de su propiedad Cuenta de AWS. Si crea una política basada en identidades que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

No es necesario que concedas permisos mínimos de consola a los usuarios que solo realicen llamadas a la API AWS CLI o a la AWS API. En su lugar, permite el acceso únicamente a las acciones que coincidan con la operación de API que intentan realizar.

Para garantizar que los usuarios y los roles puedan seguir utilizando la consola ARC cuando solo se permita el acceso a determinadas operaciones de la API, adjunte también a las entidades una política `ReadOnly` AWS gestionada para ARC. Para obtener más información, consulte la página de políticas gestionadas por ARC ARC o Añadir permisos a un usuario en la Guía del usuario de IAM.

Para que los usuarios tengan pleno acceso a las funciones de control de enrutamiento de ARC a través de la consola, adjunte al usuario una política como la siguiente, a fin de otorgarle todos los permisos necesarios para configurar los recursos y las operaciones del control de enrutamiento de ARC:

```
{
    "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": "*"
        }
    ]
}
```

Ejemplos: acciones de la API ARC para la configuración del control de enrutamiento

Para garantizar que un usuario pueda utilizar las acciones de la API de ARC para trabajar con la configuración de control de enrutamiento de ARC, adjunte una política que corresponda a las operaciones de la API con las que el usuario debe trabajar, tal y como se describe a continuación.

Para trabajar con las operaciones de la API para la configuración del control de recuperación, adjunte al usuario una política como la siguiente:

```
{
    "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": "*"
        }
    ]
}
```

Para realizar tareas en el control de enrutamiento de ARC con la API del plano de datos del clúster de recuperación, por ejemplo, actualizar los estados del control de enrutamiento para realizar una conmutación por error durante un desastre, puede adjuntar a su usuario de IAM una política de IAM de ARC como la siguiente.

El booleano `AllowSafetyRuleOverride` permite anular las reglas de seguridad que haya configurado como salvaguardas para los controles de enrutamiento. Este permiso puede ser necesario en situaciones de “rotura de cristales” para eludir las salvaguardias en caso de desastre u otras situaciones de conmutación por error urgente. Por ejemplo, es posible que un operador necesite realizar rápidamente una conmutación por error para recuperarse de un desastre, y una o más normas de seguridad podrían impedir inesperadamente la actualización del estado del control de enrutamiento necesaria para redirigir el tráfico. Este permiso permite al operador especificar las

reglas de seguridad que deben anularse al realizar llamadas a la API para actualizar los estados del control de enrutamiento. Para obtener más información, consulte Anulación de las reglas de seguridad para redirigir el tráfico.

Si quiere permitir que un operador utilice la API del plano de datos del clúster de recuperación pero evitar que se anulen las normas de seguridad, puede adjuntar una política como la siguiente, con `AllowSafetyRuleOverrides` un booleano. `false` Para permitir que el operador anule las reglas de seguridad, defina el booleano en. `AllowSafetyRuleOverrides` `true`

```
{
    "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 políticas administradas para el control de enrutamiento en Amazon Application Recovery Controller (ARC)

Una política AWS administrada es una política independiente creada y administrada por AWS. AWS Las políticas administradas están diseñadas para proporcionar permisos para muchos casos de uso comunes, de modo que pueda empezar a asignar permisos a usuarios, grupos y funciones.

Ten en cuenta que es posible que las políticas AWS administradas no otorguen permisos con privilegios mínimos para tus casos de uso específicos, ya que están disponibles para que los usen todos los AWS clientes. Se recomienda definir políticas administradas por el cliente específicas para sus casos de uso a fin de reducir aún más los permisos.

No puedes cambiar los permisos definidos en AWS las políticas administradas. Si AWS actualiza los permisos definidos en una política AWS administrada, la actualización afecta a todas las identidades principales (usuarios, grupos y roles) a las que está asociada la política. AWS es más probable que actualice una política AWS administrada cuando Servicio de AWS se lance una nueva o cuando estén disponibles nuevas operaciones de API para los servicios existentes.

Para obtener más información, consulte Políticas administradas de AWS en la Guía del usuario de IAM.

AWS política gestionada: AmazonRoute 53 RecoveryControlConfigFullAccess

Puede adjuntar `AmazonRoute53RecoveryControlConfigFullAccess` a sus entidades de IAM. Esta política otorga acceso total a las acciones para trabajar con la configuración del control de recuperación en ARC. Asocie esta política a usuarios IAM y otras entidades principales que necesiten un acceso completo a las acciones de configuración de control de recuperación.

A su entera discreción, puede añadir el acceso a acciones adicionales de Amazon Route 53 para que los usuarios puedan crear comprobaciones de estado para los controles de enrutamiento. Por ejemplo, puede conceder permiso para una o más de las siguientes acciones: `route53:GetHealthCheckroute53:CreateHealthCheck`,`route53:DeleteHealthCheck`, y`route53:ChangeTagsForResource`.

Para ver los permisos de esta política, consulte la sección AmazonRoute53 RecoveryControlConfigFullAccess en la Referencia de políticas AWS administradas.

AWS política gestionada: AmazonRoute 53 RecoveryControlConfigReadOnlyAccess

Puede adjuntar `AmazonRoute53RecoveryControlConfigReadOnlyAccess` a sus entidades de IAM. Es útil para los usuarios que necesitan ver las configuraciones de reglas de seguridad y

control de enrutamiento. Esta política otorga acceso de solo lectura a las acciones para trabajar con la configuración del control de recuperación en ARC. Estos usuarios no pueden crear, actualizar ni eliminar recursos de control de recuperación.

Para ver los permisos de esta política, consulte la sección AmazonRoute53 RecoveryControlConfigReadOnlyAccess en la Referencia de políticas AWS administradas.

AWS política gestionada: AmazonRoute 53 RecoveryClusterFullAccess

Puede adjuntar `AmazonRoute53RecoveryClusterFullAccess` a sus entidades de IAM. Esta política otorga acceso total a las acciones para trabajar con el plano de datos del clúster en ARC. Asocie esta política a usuarios de IAM y otras entidades principales que necesiten un acceso completo para actualizar y recuperar los estados de control de enrutamiento.

Para ver los permisos de esta política, consulte la sección AmazonRoute53 RecoveryClusterFullAccess en la Referencia de políticas AWS administradas.

AWS política gestionada: AmazonRoute 53 RecoveryClusterReadOnlyAccess

Puede adjuntar `AmazonRoute53RecoveryClusterReadOnlyAccess` a sus entidades de IAM. Esta política otorga acceso de solo lectura al plano de datos del clúster en ARC. Estos usuarios pueden recuperar los estados de control de enrutamiento, pero no pueden actualizarlos.

Para ver los permisos de esta política, consulte la sección AmazonRoute53 RecoveryClusterReadOnlyAccess en la Referencia de políticas AWS administradas.

Actualizaciones de las políticas AWS administradas para el control de enrutamiento

Para obtener más información sobre las actualizaciones de las políticas AWS administradas para el control de enrutamiento en ARC desde que este servicio comenzó a rastrear estos cambios, consulteActualizaciones de las políticas AWS gestionadas de Amazon Application Recovery Controller (ARC). Para recibir alertas automáticas sobre los cambios en esta página, suscríbase a la fuente RSS de la página del historial de documentos de ARC.

Cuotas para el control de enrutamiento

El control de enrutamiento de Amazon Application Recovery Controller (ARC) está sujeto a las siguientes cuotas (anteriormente denominadas límites).

Entidad	Cuota

Entidad	Cuota
Número de clústeres por cuenta	2
Número de paneles de control por clúster	50
Número de controles de enrutamiento del panel de control	100
Número total de controles de enrutamiento (en todos los paneles de control) por clúster	300
Número de normas de seguridad por panel de control	20
Número de controles de enrutamiento por llamada UpdateRoutingControlStatesde operación	10
Número de llamadas a la API mutantes a un punto final del clúster, por segundo	3

Verificación de disponibilidad en ARC

Con la verificación de disponibilidad en Amazon Application Recovery Controller (ARC), puede obtener información sobre si sus aplicaciones y recursos están preparados para la recuperación. Tras modelar la AWS aplicación en ARC y crear comprobaciones de disponibilidad, las comprobaciones supervisan continuamente la información sobre la aplicación, como las cuotas de AWS recursos, la capacidad y las políticas de enrutamiento de la red. A continuación, puede optar por recibir notificaciones sobre los cambios que puedan afectar a su capacidad de realizar la conmutación por error a una réplica de la aplicación o de recuperarse de un suceso. Las comprobaciones de disponibilidad ayudan a garantizar, de forma continua, que puede mantener sus aplicaciones multirregionales en un estado escalado y configurado para gestionar el tráfico de conmutación por error.

En este capítulo, se explica cómo modelar su aplicación en ARC para configurar la estructura que permita que funcionen las comprobaciones de disponibilidad mediante la creación de un grupo de recuperación y celdas que describan la aplicación. A continuación, puede seguir los pasos para añadir comprobaciones de preparación y niveles de preparación para que ARC pueda auditar la preparación de su aplicación.

Una vez creadas comprobaciones de preparación, puede monitorear el estado de preparación de sus recursos. Las comprobaciones de disponibilidad ayudan a garantizar que una réplica de una aplicación en espera y sus recursos coincidan con la réplica de producción de forma continua, lo que refleja la capacidad, las políticas de enrutamiento y otros detalles de configuración de la aplicación de producción. Si la réplica no coincide, puede añadir capacidad o cambiar una configuración para que las réplicas de las aplicaciones vuelvan a alinearse.

> **Important**
>
> Las comprobaciones de disponibilidad son muy útiles para verificar, de forma continua, que las configuraciones de las réplicas de las aplicaciones y los estados de ejecución estén alineados. Las comprobaciones de disponibilidad no deben utilizarse para indicar si su réplica de producción está en buen estado, ni debe confiar en las comprobaciones de disponibilidad como el principal desencadenante de la conmutación por error durante un desastre.

¿Qué es la verificación de disponibilidad en Amazon Application Recovery Controller (ARC)?

Un control de disponibilidad realizado por ARC realiza auditorías continuas (a intervalos de un minuto) para detectar incompatibilidades en la capacidad AWS aprovisionada, las cuotas de servicio, los límites de aceleración y las discrepancias de configuración y versión de los recursos incluidos en la verificación. Las comprobaciones de disponibilidad pueden informarle de estas diferencias para que pueda asegurarse de que cada réplica tiene la misma configuración y el mismo estado de ejecución. Si bien las comprobaciones de disponibilidad garantizan que las capacidades configuradas en todas las réplicas sean consistentes, no debe esperar que ellos decidan en su nombre cuál debe ser la capacidad de la réplica. Por ejemplo, debe comprender los requisitos de su aplicación para poder dimensionar sus grupos de Auto Scaling con suficiente capacidad de búfer en cada réplica para administrar si no hay otra celda disponible.

En cuanto a las cuotas, cuando ARC detecta una discrepancia y comprueba su disponibilidad, puede tomar medidas para alinear las cuotas de las réplicas aumentando la cuota inferior para que coincida con la cuota más alta. Cuando las cuotas coinciden, se muestra el estado de la comprobación de disponibilidad. `READY` (Ten en cuenta que este no es un proceso de actualización inmediato y que el tiempo total depende del tipo de recurso específico y de otros factores).

El primer paso es configurar las comprobaciones de disponibilidad para crear un grupo de recuperación que represente su aplicación. Cada grupo de recuperación incluye celdas para cada unidad individual de contención de fallos o réplica de la aplicación. A continuación, cree conjuntos de recursos para cada tipo de recurso de la aplicación y asocie las comprobaciones de disponibilidad a los conjuntos de recursos. Por último, asocie los recursos a los ámbitos de disponibilidad, de modo que pueda obtener información sobre el estado de disponibilidad de los recursos de un grupo de recuperación (su aplicación) o de celdas individuales (réplicas, que son regiones o zonas de disponibilidad ()). AZs

La disponibilidad (es decir, `READY` o`NOT READY`) se basa en los recursos que se encuentran dentro del ámbito de la comprobación de disponibilidad y en el conjunto de reglas para un tipo de recurso. Hay conjuntos de reglas de preparación para cada tipo de recurso, que las comprobaciones de ARC utilizan para auditar la disponibilidad de los recursos. El hecho de que un recurso lo esté `READY` o no depende de cómo se defina cada regla de preparación. Todas las reglas de preparación evalúan los recursos, pero algunas comparan los recursos entre sí y otras analizan información específica sobre cada recurso del conjunto de recursos.

Al añadir comprobaciones de disponibilidad, puede supervisar el estado de preparación de varias maneras: con EventBridge, en las acciones de la AWS Management Console API ARC o mediante ellas. También puede supervisar el estado de preparación de los recursos en diferentes contextos, incluida la preparación de las celdas y la preparación de su aplicación. Utilice la función de autorización multicuenta de ARC para facilitar la configuración y la supervisión de los recursos distribuidos desde una sola AWS cuenta.

Supervise las réplicas de las aplicaciones con comprobaciones de disponibilidad

ARC audita las réplicas de las aplicaciones mediante comprobaciones de disponibilidad para garantizar que cada una tenga la misma configuración y el mismo estado de ejecución. Una comprobación de disponibilidad audita continuamente la capacidad de los AWS recursos, la configuración, las AWS cuotas y las políticas de enrutamiento de una aplicación, información que puede utilizar para asegurarse de que las réplicas estén preparadas para la conmutación por error. Las comprobaciones de disponibilidad le ayudan a garantizar que su entorno de recuperación esté escalado y configurado para realizar la conmutación por error cuando sea necesario.

En las siguientes secciones se proporcionan más detalles sobre cómo funciona la comprobación de disponibilidad.

Comprobaciones de preparación y réplicas de sus aplicaciones

Para estar preparado para la recuperación, debe mantener suficiente capacidad sobrante en las réplicas en todo momento para absorber el tráfico de conmutación por error procedente de otra zona o región de disponibilidad. ARC inspecciona continuamente (una vez por minuto) la aplicación para garantizar que la capacidad aprovisionada coincida con todas las zonas o regiones de disponibilidad.

La capacidad que inspecciona ARC incluye, por ejemplo, el recuento de EC2 instancias de Amazon, las unidades de capacidad de lectura y escritura de Aurora y el tamaño del volumen de Amazon EBS. Si amplía la capacidad de la réplica principal para los valores de los recursos, pero se olvida de aumentar también los valores correspondientes en la réplica en espera, ARC detecta la falta de coincidencia para que pueda aumentar los valores en la réplica en espera.

> **Important**
>
> Las comprobaciones de disponibilidad son muy útiles para verificar, de forma continua, que las configuraciones de las réplicas de las aplicaciones y los estados de ejecución estén alineados. Las comprobaciones de disponibilidad no deben utilizarse para indicar si su réplica de producción está en buen estado, ni debe confiar en las comprobaciones de disponibilidad como el principal desencadenante de la conmutación por error durante un desastre.

En una configuración activa y en espera, debe decidir si debe fallar desde o hacia una celda en función de sus sistemas de supervisión y control de estado, y considerar las comprobaciones de disponibilidad como un servicio complementario a esos sistemas. Las comprobaciones de disponibilidad de ARC no son de alta disponibilidad, por lo que no debe depender de que las comprobaciones estén accesibles durante una interrupción. Además, es posible que los recursos que se comprueban tampoco estén disponibles durante un desastre.

Puede supervisar el estado de disponibilidad de los recursos de su aplicación en celdas específicas (AWS regiones o zonas de disponibilidad) o de toda la aplicación. Puede recibir una notificación cuando el estado de una verificación de disponibilidad cambie, por ejemplo`Not ready`, creando reglas en ella EventBridge. Para obtener más información, consulte Uso de la verificación de disponibilidad en ARC con Amazon EventBridge. También puede ver el estado de preparación en las AWS Management Console operaciones de la API o mediante ellas, como`get-recovery-`

`readiness`. Para obtener más información, consulte Operaciones de la API de verificación de disponibilidad.

Cómo funciona la comprobación de disponibilidad

ARC audita las réplicas de las aplicaciones mediante comprobaciones de disponibilidad para garantizar que cada una tenga la misma configuración y el mismo estado de ejecución.

Para estar preparado para la recuperación, por ejemplo, debe tener suficiente capacidad sobrante en todo momento para absorber el tráfico de conmutación por error procedente de otra zona o región de disponibilidad. ARC inspecciona continuamente (una vez por minuto) la aplicación para garantizar que la capacidad aprovisionada coincida con todas las zonas o regiones de disponibilidad. La capacidad que inspecciona ARC incluye, por ejemplo, el recuento de EC2 instancias de Amazon, las unidades de capacidad de lectura y escritura de Aurora y el tamaño del volumen de Amazon EBS. Si amplía la capacidad de la réplica principal para los valores de los recursos, pero se olvida de aumentar también los valores correspondientes en la réplica en espera, ARC detecta la falta de coincidencia para que pueda aumentar los valores en la réplica en espera.

> **Important**
>
> Las comprobaciones de disponibilidad son muy útiles para verificar, de forma continua, que las configuraciones de las réplicas de las aplicaciones y los estados de ejecución estén alineados. Las comprobaciones de disponibilidad no deben utilizarse para indicar si su réplica de producción está en buen estado, ni debe confiar en las comprobaciones de disponibilidad como el principal desencadenante de la conmutación por error durante un desastre.

En una configuración activa y en espera, debe decidir si debe fallar desde o hacia una celda en función de sus sistemas de supervisión y control de estado, y considerar las comprobaciones de disponibilidad como un servicio complementario a esos sistemas. Las comprobaciones de disponibilidad de ARC no son de alta disponibilidad, por lo que no debe depender de que las comprobaciones estén accesibles durante una interrupción. Además, es posible que los recursos que se comprueban tampoco estén disponibles durante un desastre.

Puede supervisar el estado de disponibilidad de los recursos de su aplicación en celdas específicas (AWS regiones o zonas de disponibilidad) o de toda la aplicación. Puede recibir una notificación cuando el estado de una verificación de disponibilidad cambie, por ejemplo`Not ready`, creando reglas en ella EventBridge. Para obtener más información, consulte Uso de la verificación de

disponibilidad en ARC con Amazon EventBridge. También puede ver el estado de preparación en las AWS Management Console operaciones de la API o mediante ellas, como`get-recovery-readiness`. Para obtener más información, consulte Operaciones de la API de verificación de disponibilidad.

Cómo determinan las reglas de preparación el estado de preparación

Las comprobaciones de disponibilidad del ARC determinan el estado de preparación en función de las reglas predefinidas para cada tipo de recurso y de la forma en que se definen esas reglas. El ARC incluye un grupo de reglas para cada tipo de recurso que admite. Por ejemplo, ARC tiene grupos de reglas de preparación para los clústeres de Amazon Aurora, los grupos de Auto Scaling, etc. Algunas reglas de preparación comparan los recursos de un conjunto entre sí y otras analizan información específica sobre cada recurso del conjunto de recursos.

No puede agregar, editar ni eliminar reglas de preparación ni grupos de reglas. Sin embargo, puedes crear una CloudWatch alarma de Amazon y crear una verificación de disponibilidad para monitorear el estado de la alarma. Por ejemplo, puede crear una CloudWatch alarma personalizada para supervisar los servicios de contenedores EKS de Amazon y crear una comprobación de disponibilidad para auditar el estado de preparación de la alarma.

Puede ver todas las reglas de preparación de cada tipo de recurso AWS Management Console al crear un conjunto de recursos, o puede ver las reglas de preparación más adelante navegando a la página de detalles de un conjunto de recursos. También puede ver las reglas de preparación en la siguiente sección:Reglas de preparación en ARC.

Cuando una verificación de disponibilidad audita un conjunto de recursos con un conjunto de reglas, la forma en que se define cada regla determina si el resultado será `READY` `NOT READY` para todos los recursos o si el resultado será diferente para los diferentes recursos. Además, puede ver el estado de preparación de varias maneras. Por ejemplo, puede ver el estado de preparación de un grupo de recursos de un conjunto de recursos o ver un resumen del estado de preparación de un grupo de recuperación o una celda (es decir, una AWS región o zona de disponibilidad, según cómo haya configurado el grupo de recuperación).

La redacción de la descripción de cada regla explica cómo evalúa los recursos para determinar el estado de preparación cuando se aplica esa regla. Se define una regla para inspeccionar cada recurso o inspeccionar todos los recursos de un conjunto de recursos para determinar si están listos. En concreto, las reglas funcionan de la siguiente manera:

- La regla inspecciona cada recurso del conjunto de recursos para garantizar una condición.

  - Si todos los recursos funcionan correctamente, todos los recursos se establecen comoREADY.
  - Si un recurso falla, ese recurso se establece como NOT READY y las demás celdas permanecenREADY.

  Por ejemplo: .MskClusterState:Inspecciona cada clúster de Amazon MSK para asegurarse de que se encuentra en un ACTIVE estado.
- La regla inspecciona todos los recursos del conjunto de recursos para garantizar una condición.
  - Si se garantiza la condición, todos los recursos se establecen comoREADY.
  - Si alguno no cumple la condición, todos los recursos se establecen comoNOT READY.

  Por ejemplo: .VpcSubnetCount:Inspecciona todos VPC subredes para asegurarse de que tienen el mismo número de subredes.
- Regla no crítica: la regla inspecciona todos los recursos del conjunto de recursos para garantizar una condición.
  - Si alguna falla, el estado de preparación no cambia. Una regla con este comportamiento tiene una nota en su descripción.

  Por ejemplo: .ElbV2CheckAzCount:Inspecciona cada Network Load Balancer para asegurarse de que esté conectado a una sola zona de disponibilidad. Nota: Esta regla no afecta al estado de preparación.

Además, ARC da un paso más en lo que respecta a las cuotas. Si una comprobación de disponibilidad detecta una discrepancia en las celdas de las cuotas de servicio (el valor máximo para la creación y las operaciones de los recursos) de cualquier recurso compatible, ARC aumenta automáticamente la cuota del recurso con la cuota más baja. Esto se aplica solo a las cuotas (límites). En cuanto a la capacidad, debe añadir capacidad adicional según sea necesario para las necesidades de su aplicación.

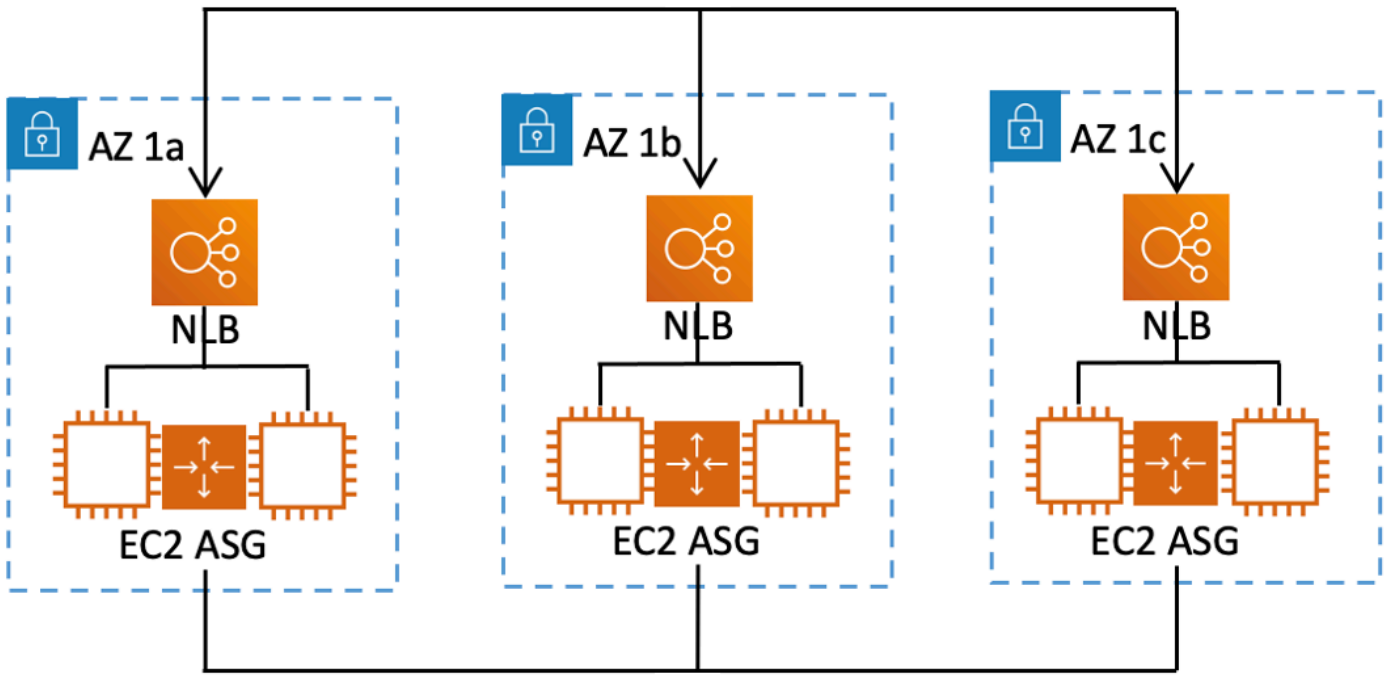
También puedes configurar una EventBridge notificación de Amazon para las comprobaciones de disponibilidad, por ejemplo, cuando el estado de una comprobación de preparación cambie aNOT READY. Luego, cuando se detecta una discrepancia en la configuración, le EventBridge envía una notificación para que pueda tomar las medidas correctivas necesarias para asegurarse de que las réplicas de las aplicaciones estén alineadas y preparadas para la recuperación. Para obtener más información, consulte Uso de la verificación de disponibilidad en ARC con Amazon EventBridge.

Cómo funcionan en conjunto las comprobaciones de preparación, los conjuntos de recursos y los ámbitos de preparación

Las comprobaciones de preparación siempre auditan los grupos de recursos de los conjuntos de recursos. Los conjuntos de recursos se crean (por separado o mientras se crea una comprobación de disponibilidad) para agrupar los recursos que se encuentran en las celdas (zonas o AWS regiones de disponibilidad) del grupo de recuperación de ARC, de modo que se puedan definir las comprobaciones de disponibilidad. Por lo general, un conjunto de recursos es un grupo del mismo tipo de recursos (como los balanceadores de carga de red), pero también pueden ser recursos de destino del DNS para comprobar el grado de aptitud arquitectónica.

Por lo general, se crea un conjunto de recursos y se comprueba la disponibilidad de cada tipo de recurso de la aplicación. Para comprobar la idoneidad de la arquitectura, se crean un recurso de destino de DNS de nivel superior y un conjunto de recursos global (a nivel de grupo de recuperación) para dicho recurso y, a continuación, se crean los recursos de destino de DNS de nivel de celda para un conjunto de recursos independiente.

El siguiente diagrama muestra un ejemplo de un grupo de recuperación con tres celdas (zonas de disponibilidad), cada una con un Network Load Balancer (NLB) y un grupo de Auto Scaling (ASG).



En este escenario, crearía un conjunto de recursos y una comprobación de disponibilidad para los tres balanceadores de carga de red, y un conjunto de recursos y una verificación de disponibilidad

para los tres grupos de Auto Scaling. Ahora tiene una verificación de disponibilidad para cada conjunto de recursos de su grupo de recuperación, por tipo de recurso.

Al crear los niveles de preparación de los recursos, puede agregar resúmenes de las comprobaciones de preparación para las celdas o los grupos de recuperación. Para especificar el alcance de preparación de un recurso, asocie el ARN de la celda o el grupo de recuperación a cada recurso de un conjunto de recursos. Puede hacerlo al crear una comprobación de disponibilidad para un conjunto de recursos.

Por ejemplo, si agrega una verificación de disponibilidad para un conjunto de recursos para los balanceadores de carga de red de este grupo de recuperación, puede agregar niveles de disponibilidad a cada NLB al mismo tiempo. En este caso, asociaría el ARN de la AZ 1a a la NLB en la AZ 1a, el ARN de la NLB y el ARN de `AZ 1b` a la NLB `AZ 1b` en. `AZ 1c` `AZ 1c` Al crear una verificación de preparación para los grupos de Auto Scaling, haría lo mismo, asignando ámbitos de preparación a cada uno de ellos al crear la verificación de preparación para el conjunto de recursos del grupo Auto Scaling.

Es opcional asociar los niveles de preparación al crear una comprobación de disponibilidad; sin embargo, le recomendamos encarecidamente que los establezca. Los alcances de preparación permiten a ARC mostrar el estado correcto `READY` o el estado de `NOT READY` preparación para las verificaciones resumidas de preparación de los grupos de recuperación y las verificaciones resumidas de preparación a nivel de celda. A menos que establezca los alcances de preparación, ARC no puede proporcionar estos resúmenes.

Tenga en cuenta que cuando agrega un recurso global o a nivel de aplicación, como una política de enrutamiento de DNS, no elige un grupo o celda de recuperación para el ámbito de preparación. En su lugar, eliges un recurso global (sin celda).

Comprobaciones de disponibilidad de los recursos de DNS objetivo: auditar la disponibilidad de los recursos

Con las comprobaciones de aptitud de los recursos de DNS Target en ARC, puede auditar la idoneidad arquitectónica y de resiliencia de su aplicación. Este tipo de comprobación de aptitud analiza continuamente la arquitectura de la aplicación y las políticas de enrutamiento de Amazon Route 53 para comprobar si existen dependencias entre zonas y regiones.

Una aplicación orientada a la recuperación tiene varias réplicas que están aisladas en zonas o AWS regiones de disponibilidad, de modo que las réplicas pueden fallar de forma independiente unas de otras. Si su aplicación necesita ajustarse para estar correctamente aislada en silos, ARC le sugerirá

cambios que puede realizar, si es necesario, para actualizar su arquitectura y garantizar que sea resistente y esté lista para la conmutación por error.

ARC detecta automáticamente el número y el alcance de las celdas (que representan réplicas o unidades de contención de fallos) de su aplicación y si las celdas están agrupadas en silos por zona de disponibilidad o por región. A continuación, ARC identifica los recursos de la aplicación en las celdas y le proporciona información sobre ellos, para determinar si están correctamente divididos en silos en zonas o regiones. Por ejemplo, si tiene celdas orientadas a zonas específicas, las comprobaciones de disponibilidad permiten comprobar si los balanceadores de carga y los objetivos situados detrás de ellos también están aislados en esas zonas.

Con esta información, puede determinar si hay cambios que deba realizar para alinear los recursos de sus celdas con las zonas o regiones correctas.

Para empezar, debe crear recursos de destino de DNS para su aplicación, así como conjuntos de recursos y comprobaciones de disponibilidad para ellos. Para obtener más información, consulte Obtener recomendaciones de arquitectura en ARC.

Comprobaciones de preparación y escenarios de recuperación ante desastres

Las comprobaciones de preparación para el ARC le permiten saber si sus aplicaciones y recursos están preparados para la recuperación, ya que le ayudan a asegurarse de que sus aplicaciones están escaladas para gestionar el tráfico de conmutación por error. Los estados de las comprobaciones de disponibilidad no deben utilizarse como señal para indicar que una réplica de producción está en buen estado. Sin embargo, puede utilizar las comprobaciones de disponibilidad como complemento de sus sistemas de supervisión de aplicaciones e infraestructuras o de comprobación del estado de sus sistemas para determinar si se debe producir un error en una réplica o en dirección a ella.

En una situación urgente o en caso de una interrupción del servicio, utilice una combinación de comprobaciones de estado y otra información para determinar si su dispositivo de reserva se ha ampliado, se encuentra en buen estado y preparado para que pueda conmutar por error el tráfico de producción. Por ejemplo, compruebe si los canarios que circulan contra su celda de reserva cumplen sus criterios de éxito, además de comprobar que los estados de comprobación de disponibilidad de la célula de reserva sí los cumplen. `READY`

Tenga en cuenta que las comprobaciones de preparación del ARC se realizan en una sola AWS región, el oeste de EE. UU. (Oregón), y durante una interrupción o un desastre, la información sobre las comprobaciones de disponibilidad podría quedar obsoleta o las comprobaciones podrían dejar de

estar disponibles. Para obtener más información, consulte Planos de datos y control para el control del enrutamiento.

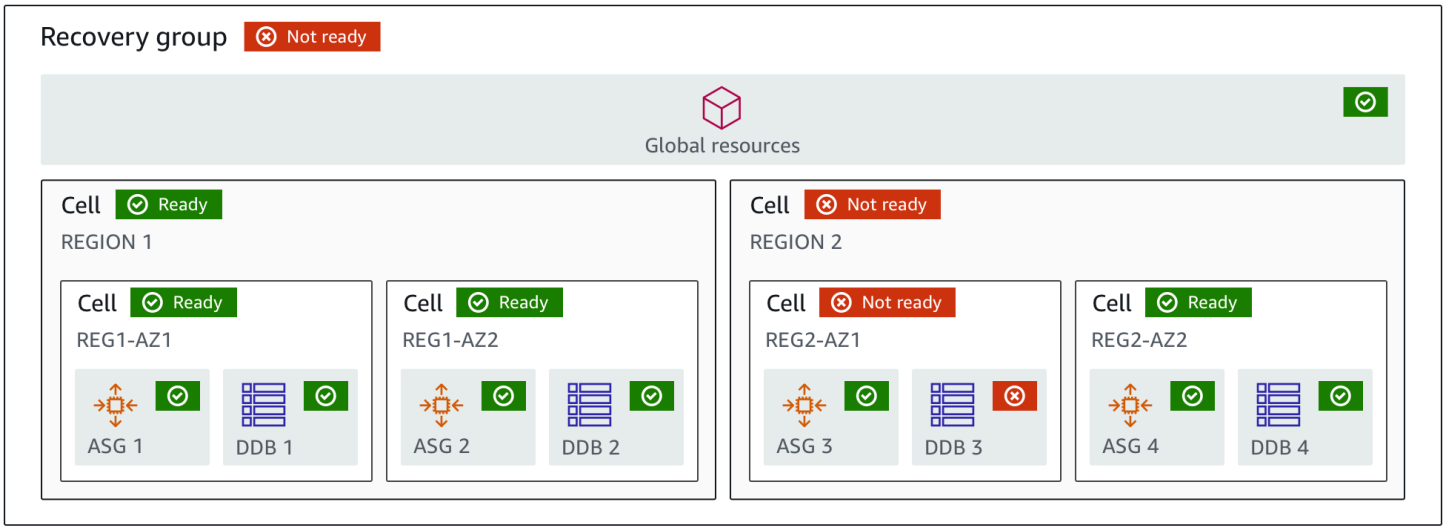
AWS Disponibilidad regional para comprobar si están listos

Para obtener información detallada sobre el soporte regional y los puntos de enlace de servicio para Amazon Application Recovery Controller (ARC), consulte los puntos de enlace y las cuotas de Amazon Application Recovery Controller (ARC) en la Referencia general de Amazon Web Services.

> **Note**
>
> La comprobación de disponibilidad en Amazon Application Recovery Controller (ARC) es una función global. Sin embargo, los recursos de verificación de disponibilidad se encuentran en la región EE.UU. Oeste (Oregón), por lo que debe especificar la región EE.UU. Oeste (Oregón) (especificar el parámetro`--region us-west-2`) en AWS CLI los comandos ARC regionales, por ejemplo, al crear recursos como conjuntos de recursos y comprobaciones de disponibilidad.

Comprobación de disponibilidad de los componentes

El siguiente diagrama ilustra un ejemplo de grupo de recuperación que está configurado para admitir la función de verificación de disponibilidad. Los recursos de este ejemplo se agrupan en celdas (por Región de AWS) y celdas anidadas (por zonas de disponibilidad) en un grupo de recuperación. Hay un estado de preparación general para el grupo de recuperación (aplicación), así como estados de preparación individuales para cada celda (región) y celda anidada (zona de disponibilidad).



Los siguientes son componentes de la función de verificación de disponibilidad de ARC.

Celda

Una celda define las réplicas o unidades independientes de conmutación por error de la aplicación. Agrupa todos los AWS recursos necesarios para que la aplicación se ejecute de forma independiente dentro de la réplica. Por ejemplo, puede tener un conjunto de recursos en una celda principal y otro conjunto en una celda en espera. Usted determina el límite de lo que incluye una celda, pero las celdas suelen representar una zona o región de disponibilidad. Puede tener varias celdas (celdas anidadas) dentro de una celda, por ejemplo, AZs dentro de una región. Cada celda anidada representa una unidad aislada de conmutación por error.

Grupo de recuperación

Las células se recolectan en un grupo de recuperación. Un grupo de recuperación representa una aplicación o un grupo de aplicaciones para las que desea comprobar si están preparadas para la conmutación por error. Se compone de dos o más celdas, o réplicas, que coinciden entre sí en términos de funcionalidad. Por ejemplo, si tiene una aplicación web replicada en us-east-1a y us-east-1b, donde us-east-1b es su entorno de conmutación por error, puede representar esta aplicación en ARC como un grupo de recuperación con dos celdas: una en us-east-1a y otra en us-east-1b. Un grupo de recuperación también puede incluir un recurso global, como una comprobación de estado de Route 53.

Recursos e identificadores de recursos

Al crear componentes para las comprobaciones de disponibilidad en ARC, se especifica un recurso, como una tabla de Amazon DynamoDB, un Network Load Balancer o un recurso de destino de DNS, mediante un identificador de recurso. Un identificador de recurso es el nombre de recurso de Amazon (ARN) del recurso o, en el caso de un recurso de destino de DNS, el identificador que ARC genera al crear el recurso.

Recurso de destino de DNS

Un recurso de destino de DNS es la combinación del nombre de dominio de la aplicación y otra información de DNS, como el AWS recurso al que apunta el dominio. Incluir un AWS recurso es opcional, pero si lo proporciona, debe ser un registro de recursos de Route 53 o un Network Load Balancer. Al proporcionar el AWS recurso, puede obtener recomendaciones de arquitectura más detalladas que pueden ayudarle a mejorar la resiliencia de recuperación de su aplicación. Puede crear conjuntos de recursos en ARC para los recursos de destino del DNS y, a continuación, crear una comprobación de disponibilidad del conjunto de recursos a fin de obtener recomendaciones de arquitectura para su aplicación. La comprobación de disponibilidad

también supervisa la política de enrutamiento de DNS de la aplicación, en función de las reglas de preparación de los recursos de destino del DNS.

Conjunto de recursos

Un conjunto de recursos es un conjunto de recursos, incluidos AWS los recursos o los recursos de destino del DNS, que abarca varias celdas. Por ejemplo, es posible que tenga un balanceador de carga en us-east-1a y otro en us-east-1b. Para supervisar la capacidad de recuperación de los balanceadores de carga, puedes crear un conjunto de recursos que incluya ambos balanceadores de carga y, a continuación, crear una verificación de disponibilidad para el conjunto de recursos. ARC comprobará continuamente la disponibilidad de los recursos del conjunto. También puede agregar un ámbito de preparación para asociar los recursos de un conjunto de recursos al grupo de recuperación que cree para su aplicación.

Regla de preparación

Las reglas de preparación son auditorías que ARC realiza comparándolas con un conjunto de recursos de un conjunto de recursos. ARC tiene un conjunto de reglas de preparación para cada tipo de recurso para el que admite las comprobaciones de disponibilidad. Cada regla incluye un identificador y una descripción que explica para qué inspecciona ARC los recursos.

Verificación de preparación

Una comprobación de disponibilidad supervisa un conjunto de recursos de la aplicación, como un conjunto de instancias de Amazon Aurora, para las que ARC está auditando la preparación para la recuperación. Las comprobaciones de disponibilidad pueden incluir la auditoría, por ejemplo, de las configuraciones de capacidad, AWS las cuotas o las políticas de enrutamiento. Por ejemplo, si desea auditar la preparación de sus grupos de Amazon EC2 Auto Scaling en dos zonas de disponibilidad, puede crear una verificación de preparación para un conjunto de recursos con dos recursosARNs, uno para cada grupo de Auto Scaling. Luego, para asegurarse de que cada grupo tenga la misma escala, ARC monitorea continuamente los tipos de instancias y los recuentos de los dos grupos.

Alcance de preparación

Un ámbito de preparación identifica la agrupación de recursos que abarca una verificación de preparación específica. El alcance de una comprobación de disponibilidad puede ser un grupo de recuperación (es decir, global para toda la aplicación) o una celda (es decir, una región o zona de disponibilidad). En el caso de un recurso que sea un recurso global para ARC, defina el nivel de preparación a nivel de grupo de recuperación o de recurso global. Por ejemplo, un chequeo de estado de Route 53 es un recurso global en ARC porque no es específico de una región o zona de disponibilidad.

Planos de datos y control para comprobar si están listos

Al planificar la conmutación por error y la recuperación ante desastres, tenga en cuenta la resistencia de sus mecanismos de conmutación por error. Le recomendamos que se asegure de que los mecanismos de los que depende durante la conmutación por error estén altamente disponibles, de modo que pueda utilizarlos cuando los necesite en caso de desastre. Por lo general, debe utilizar funciones de plano de datos para sus mecanismos siempre que pueda, a fin de obtener la máxima fiabilidad y tolerancia a los fallos. Teniendo esto en cuenta, es importante entender cómo se divide la funcionalidad de un servicio entre planos de control y planos de datos, y cuándo se puede confiar en una fiabilidad extrema con el plano de datos de un servicio.

Como ocurre con la mayoría de los AWS servicios, los planos de control y los planos de datos admiten la funcionalidad de la capacidad de verificación de disponibilidad. Si bien ambos están diseñados para ser fiables, un plano de control está optimizado para garantizar la coherencia de los datos, mientras que un plano de datos está optimizado para garantizar la disponibilidad. Un plano de datos está diseñado para ser resistente, de modo que puede mantener la disponibilidad incluso durante eventos disruptivos, cuando un plano de control podría no estar disponible.

En general, un plano de control permite realizar funciones de administración básicas, como crear, actualizar y eliminar recursos del servicio. Un plano de datos proporciona la funcionalidad principal de un servicio.

Para comprobar la disponibilidad, existe una única API, la API de preparación para la recuperación, tanto para el plano de control como para el plano de datos. Los controles de preparación y los recursos de preparación solo se encuentran en la región de EE. UU. Oeste (Oregón) (Oregón) (Región Oeste de EE. UU. [Oregón] (Oregón) (Oregón) El plano de control y el plano de datos para comprobar la disponibilidad son fiables, pero no están muy disponibles.

Para obtener más información sobre los planos de datos, los planos de control y cómo AWS se crean servicios para cumplir los objetivos de alta disponibilidad, consulte el artículo Static stability using Availability Zones en Amazon Builders' Library.

Etiquetado para comprobar la disponibilidad en Amazon Application Recovery Controller (ARC)

Las etiquetas son palabras o frases (metadatos) que se utilizan para identificar y organizar AWS los recursos. Puede añadir varias etiquetas a cada recurso, y cada etiqueta incluye una clave y un valor que usted define. Por ejemplo, la clave puede ser el entorno y el valor puede ser la producción. Puede buscar y filtrar sus recursos en función de las etiquetas que añada.

Puede etiquetar los siguientes recursos en la verificación de disponibilidad en ARC:

- Conjuntos de recursos
- Comprobador de preparación de

El etiquetado en ARC solo está disponible a través de la API, por ejemplo, mediante el AWS CLI.

Los siguientes son ejemplos de cómo etiquetar durante la comprobación de disponibilidad mediante el. 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
```

Para obtener más información, consulte la Guía TagResourcede referencia de la API Recovery Readiness para Amazon Application Recovery Controller (ARC).

Los precios de la verificación de disponibilidad en ARC

Usted paga un costo por hora por cada verificación de disponibilidad que configure.

Para obtener información detallada sobre los precios de ARC y ejemplos de precios, consulta los precios de ARC.

Configure un proceso de recuperación flexible para su aplicación

Para usar Amazon Application Recovery Controller (ARC) con AWS aplicaciones que se encuentran en varias AWS regiones, hay pautas que debe seguir para configurar sus aplicaciones para que sean resilientes, de modo que pueda respaldar la preparación para la recuperación de manera efectiva. A continuación, puede crear comprobaciones de disponibilidad para su aplicación y configurar controles de enrutamiento para redirigir el tráfico con fines de conmutación por error. También puede

revisar las recomendaciones que ofrece ARC sobre la arquitectura de su aplicación, que pueden mejorar la resiliencia.

> **Note**
>
> Si tiene una aplicación aislada por zonas de disponibilidad, considere la posibilidad de utilizar el cambio zonal o el cambio automático zonal para la recuperación de la conmutación por error. No es necesario realizar ninguna configuración para utilizar el cambio zonal o el cambio automático zonal a fin de recuperar de forma fiable las aplicaciones en caso de averías en las zonas de disponibilidad.
> Para alejar el tráfico de una zona de disponibilidad para los recursos del balanceador de carga, inicie un cambio zonal en la consola ARC o en la consola de Elastic Load Balancing. O bien, puede usar el AWS SDK AWS Command Line Interface o el SDK con acciones de API de cambio zonal. Para obtener más información, consulte Cambio zonal en ARC.

Para obtener más información sobre cómo empezar a utilizar configuraciones de conmutación por error resilientes, consulte. Introducción a la recuperación multirregional en Amazon Application Recovery Controller (ARC)

Mejores prácticas para comprobar la preparación en ARC

Recomendamos las siguientes prácticas recomendadas para comprobar la disponibilidad en Amazon Application Recovery Controller (ARC).

Agregue notificaciones para los cambios en el estado de preparación

Establece una regla en Amazon EventBridge para enviar una notificación cada vez que el estado de una verificación de disponibilidad cambie, por ejemplo, de `READY` a`NOT READY`. Cuando reciba una notificación, podrá investigar y solucionar el problema para asegurarse de que la aplicación y los recursos estén preparados para la conmutación por error en el momento previsto.

Puedes establecer EventBridge reglas para enviar notificaciones cuando se produzcan varios cambios en el estado de las comprobaciones de disponibilidad, por ejemplo, para tu grupo de recuperación (para tu solicitud), para una celda (por ejemplo, una AWS región) o para una comprobación de disponibilidad de un conjunto de recursos.

Para obtener más información, consulte Uso de la verificación de disponibilidad en ARC con Amazon EventBridge.

Operaciones de la API de verificación de disponibilidad

En la siguiente tabla se enumeran las operaciones de ARC que puede utilizar para preparar la recuperación (comprobación de la preparación), con enlaces a la documentación pertinente.

Para ver ejemplos de cómo utilizar las operaciones habituales de la API de preparación para la recuperación con la AWS Command Line Interface, consulte Ejemplos del uso de las operaciones de la API de verificación de la preparación para ARC con AWS CLI.

Acción	Uso de la consola ARC	Uso de la API ARC
Creación de una celda	Consulte Crear, actualizar y eliminar grupos de recuperación en ARC	Consulte CreateCell.
Consigue un móvil	Consulte Crear, actualizar y eliminar grupos de recuperación en ARC	Consulte GetCell.
Eliminar una celda	Consulte Crear, actualizar y eliminar grupos de recuperación en ARC	Consulte DeleteCell.
Actualizar una celda	N/A	Consulte UpdateCell
Listar las celdas de una cuenta	Consulte Crear, actualizar y eliminar grupos de recuperación en ARC	Consulte ListCells.
Creación de un grupo de recuperación	Consulte Crear, actualizar y eliminar grupos de recuperación en ARC	Consulte CreateRecoveryGroup.
Crea un grupo de recuperación	Consulte Crear, actualizar y eliminar grupos de recuperación en ARC	Consulte GetRecoveryGroup.

Acción	Uso de la consola ARC	Uso de la API ARC
Actualizar un grupo de recuperación	Consulte Crear, actualizar y eliminar grupos de recuperación en ARC	Consulte UpdateRecoveryGroup.
Eliminación de un grupo de recuperación	Consulte Crear, actualizar y eliminar grupos de recuperación en ARC	Consulte DeleteRecoveryGroup.
Descripción de grupos de recuperación	Consulte Crear, actualizar y eliminar grupos de recuperación en ARC	Consulte ListRecoveryGroups.
Creación de un conjunto de recursos	Consulte Creación y actualización de comprobaciones de preparación en ARC	Consulte CreateResourceSet.
Obtenga un conjunto de recursos	Consulte Creación y actualización de comprobaciones de preparación en ARC	Consulte GetResourceSet.
Actualización de un conjunto de recursos	Consulte Creación y actualización de comprobaciones de preparación en ARC	Consulte UpdateResourceSet.
Eliminar un conjunto de recursos	Consulte Creación y actualización de comprobaciones de preparación en ARC	Consulte DeleteResourceSet.
Enumeración de conjuntos de recursos	Consulte Creación y actualización de comprobaciones de preparación en ARC	Consulte ListResourceSets.
Cree una comprobación de disponibilidad	Consulte Creación y actualización de comprobaciones de preparación en ARC	Consulte CreateReadinessCheck.

Acción	Uso de la consola ARC	Uso de la API ARC
Obtenga una verificación de preparación	Consulte Creación y actualización de comprobaciones de preparación en ARC	Consulte GetReadinessCheck.
Actualice una verificación de preparación	Consulte Creación y actualización de comprobaciones de preparación en ARC	Consulte UpdateReadinessCheck.
Elimine una comprobación de disponibilidad	Consulte Creación y actualización de comprobaciones de preparación en ARC	Consulte DeleteReadinessCheck.
Lista de verificación de preparación	Consulte Creación y actualización de comprobaciones de preparación en ARC	Consulte ListReadinessChecks.
Enumere las reglas de preparación	Consulte Las descripciones de las reglas de preparación en ARC	Consulte ListRules.
Compruebe el estado de una verificación de disponibilidad completa	Consulte Supervisar el estado de preparación en ARC	Consulte GetReadinessCheckStatus.
Compruebe el estado de un recurso	Consulte Supervisar el estado de preparación en ARC	Consulte GetReadinessCheckResourceStatus.
Compruebe el estado de una celda	Consulte Supervisar el estado de preparación en ARC	Consulte GetCellReadinessSummary.
Compruebe el estado de un grupo de recuperación	Consulte Supervisar el estado de preparación en ARC	Consulte GetRecoveryGroupReadinessSummary.

Ejemplos del uso de las operaciones de la API de verificación de la preparación para ARC con AWS CLI

En esta sección se describen ejemplos de aplicaciones sencillas, que se utilizan AWS Command Line Interface para trabajar con las funciones de verificación de preparación de Amazon Application Recovery Controller (ARC) mediante operaciones de API. Los ejemplos tienen como objetivo ayudarlo a desarrollar una comprensión básica de cómo trabajar con las capacidades de verificación de preparación mediante la CLI.

Compruebe si los recursos de las réplicas de sus aplicaciones no coinciden en las auditorías de ARC. Para configurar las comprobaciones de disponibilidad de su aplicación, debe configurar (o modelar) los recursos de la aplicación en celdas ARC que se alineen con las réplicas que ha creado para la aplicación. A continuación, debe configurar comprobaciones de disponibilidad que auditen estas réplicas para asegurarse de que la réplica de la aplicación en espera y sus recursos coinciden con la réplica de producción, de forma continua

Veamos un caso sencillo en el que tiene una aplicación llamada Simple-Service que actualmente se ejecuta en la región Este de EE. UU. (Virginia del Norte) (us-east-1). También tiene una copia en espera de la aplicación de la región del Oeste de EE. UU. (Oregón) (us-west-2). En este ejemplo, configuraremos las verificaciones de preparación para comparar estas dos versiones de la aplicación. Esto nos permite asegurarnos de que la región en espera, Oeste de EE. UU. (Oregón), esté lista para recibir tráfico, en caso de que lo necesite en un escenario de conmutación por error.

Para obtener más información sobre el uso de AWS CLI, consulte la Referencia de AWS CLI comandos. Para obtener una lista de las acciones de preparación de la API y enlaces a más información, consulte Operaciones de la API de verificación de disponibilidad.

Las celdas de ARC representan los límites de los errores (como las zonas o regiones de disponibilidad) y se recopilan en grupos de recuperación. Un grupo de recuperación representa una aplicación para la que desea comprobar si está preparada para la conmutación por error. Para obtener más información acerca de los componentes de la verificación de preparación, consulte Comprobación de disponibilidad de los componentes .

> **Note**
>
> ARC es un servicio global que admite puntos finales en varios Regiones de AWS , pero debe especificar la región EE.UU. Oeste (Oregón) (es decir, especificar el parámetro`--region`

`us-west-2`) en la mayoría de los comandos CLI de ARC. Por ejemplo, para crear recursos como grupos de recuperación o comprobaciones de preparación.

Para el ejemplo de nuestra aplicación, comenzaremos por crear una celda para cada región en la que tengamos recursos. A continuación, crearemos un grupo de recuperación y, después, completaremos la configuración para una verificación de preparación.

1. Creación de celdas

1a. Cree una celda 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. Cree una celda 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. Ahora tenemos dos celdas. Llame a la API de `list-cells` para verificar que se hayan creado.

```
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. Creación de un grupo de recuperación

Los grupos de recuperación son el recurso de nivel superior para la preparación para la recuperación en ARC. Un grupo de recuperación representa una aplicación en su conjunto. En este paso, crearemos un grupo de recuperación para modelar una aplicación general y, a continuación, añadiremos las dos celdas que hemos creado.

2a. Cree un grupo de recuperación.

```
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": {}
```

```
}
```

2b. (Opcional) Para verificar que el grupo de recuperación se haya creado correctamente, llame a la API de `list-recovery-groups` .

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

Ahora que tenemos un modelo para nuestra aplicación, vamos a añadir los recursos que se van a supervisar. En ARC, un grupo de recursos que se desea supervisar se denomina conjunto de recursos. Los conjuntos de recursos incluyen recursos que son todos del mismo tipo. Comparamos los recursos de un conjunto de recursos entre sí para ayudar a determinar si una celda está preparada para la conmutación por error.

3. Creación de un conjunto de recursos

Supongamos que nuestro Simple-Service La aplicación es realmente muy simple y solo usa tablas de DynamoDB. Tiene una tabla de DynamoDB en us-east-1 y otra en us-west-2. Un conjunto de recursos también incluye un alcance de preparación, que identifica la celda en la que se encuentra cada recurso.

3a. Cree un conjunto de recursos que refleje nuestras Simple-Service recursos de la aplicación.

```
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. (Opcional) Para verificar lo que se incluye en el conjunto de recursos, llame a la API de `list-resource-sets`. Aquí se enumeran todos los conjuntos de recursos de una AWS cuenta. Aquí puede ver que solo tenemos el conjunto de recursos que hemos creado anteriormente.

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

Ahora hemos creado las celdas, el grupo de recuperación y el conjunto de recursos para modelar Simple-Service aplicación en ARC. A continuación, configuraremos verificaciones de preparación para supervisar la preparación de los recursos para la conmutación por error.

4. Cree una comprobación de disponibilidad

Una verificación de preparación aplica un conjunto de reglas a cada recurso del conjunto de recursos adjunto a la verificación. Las reglas son específicas para cada tipo de recurso. Es decir, hay distintas reglas para `AWS::DynamoDB::Table`, `AWS::EC2::Instance`, etc. Las reglas comprueban diversas dimensiones de un recurso, como la configuración, la capacidad (cuando esté disponible y se pueda aplicar), los límites (cuando esté disponible y se pueda aplicar) y las configuraciones de enrutamiento.

> **Note**
>
> Para ver las reglas que se aplican a un recurso en una verificación de preparación, puede usar la API de `get-readiness-check-resource-status`, tal y como se describe en el paso 5. Para ver una lista de todas las reglas de preparación de ARC, utilice `list-rules` o consulteLas descripciones de las reglas de preparación en ARC. ARC tiene un conjunto específico de reglas que se aplican a cada tipo de recurso; por el momento, no se pueden personalizar.

4a. Cree una comprobación de disponibilidad para el conjunto de recursos, 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": {}
}
```

4b. (Opcional) Para comprobar que la verificación de preparación se haya creado correctamente, ejecute la API de `list-readiness-checks`. Esta API muestra todas las verificaciones de preparación de una cuenta.

```
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. Supervisión de las verificaciones de preparación

Ahora que hemos modelado la aplicación y hemos añadido una verificación de preparación, ya podemos supervisar los recursos. Puede modelar la preparación de su aplicación en cuatro niveles: el nivel de verificación de preparación (un grupo de recursos), el nivel de recursos individuales, el nivel de celda (todos los recursos de una región o zona de disponibilidad) y el nivel de grupo de recuperación (la aplicación en su conjunto). A continuación, se proporcionan los comandos para obtener cada uno de estos tipos de estados de preparación.

5a. Consulte el estado de la verificación de preparación.

```
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"
    ]
}
```

5b. Consulte el estado detallado de preparación de un único recurso en una verificación de preparación, incluido el estado de cada regla que se compruebe.

```
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. Consulte el estado general de preparación de una celda.

```
aws route53-recovery-readiness --region us-west-2 get-cell-readiness-summary \
    --cell-name west-cell
```

```
{
    "Readiness": "READY",
    "ReadinessChecks": [
        {
            "Readiness": "READY",
            "ReadinessCheckName": "ImportantTableCheck"
        }
    ]
}
```

5d. Por último, consulte el nivel máximo de preparación de su aplicación, en el nivel de grupo de recuperación.

```
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"
        }
    ]
}
```

Trabaje con grupos de recuperación y verificaciones de preparación

En esta sección se describen y proporcionan los procedimientos para los grupos de recuperación y las comprobaciones de preparación, incluidas la creación, actualización y eliminación de estos recursos.

Crear, actualizar y eliminar grupos de recuperación en ARC

Un grupo de recuperación representa su aplicación en Amazon Application Recovery Controller (ARC). Por lo general, consta de dos o más celdas que son réplicas entre sí en términos de recursos y funcionalidad, de modo que puede realizar la conmutación por error de una a otra. Cada celda incluye los nombres de recursos de Amazon (ARNs) de los recursos activos de una AWS región o zona de disponibilidad. Los recursos pueden ser un balanceador de carga de Elastic Load Balancing, un grupo de Auto Scaling u otros recursos. La celda correspondiente que representa a otra zona o región tiene recursos en espera del mismo tipo que los de la celda activa: un balanceador de carga, un grupo de Auto Scaling, etc.

Una celda representa réplicas de su aplicación. Las comprobaciones de disponibilidad en ARC le ayudan a determinar si su aplicación está lista para la conmutación por error de una réplica a otra. Sin embargo, debe tomar la decisión de realizar un error desde o hacia una réplica en función de sus sistemas de supervisión y control de estado, y considerar las comprobaciones de disponibilidad como un servicio complementario a esos sistemas.

La preparación comprueba los recursos de auditoría para determinar si están preparados en función de un conjunto de reglas predefinidas para ese tipo de recurso. Después de crear el grupo de recuperación con las réplicas, añada las comprobaciones de aptitud para ARC de los recursos de la aplicación, de modo que ARC pueda garantizar que las réplicas tengan la misma configuración y configuración a lo largo del tiempo.

Temas

- Creación de grupos de recuperación
- Actualizar y eliminar grupos y celdas de recuperación

Creación de grupos de recuperación

En los pasos de esta sección se explica cómo crear un grupo de recuperación en la consola ARC. Para obtener información sobre el uso de las operaciones de la API de preparación para la recuperación con Amazon Application Recovery Controller (ARC), consulte Operaciones de la API de verificación de disponibilidad.

Para crear un grupo de recuperación

1. Abra la consola ARC enhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Elija Comprobación de disponibilidad.

3. En la página de preparación para la recuperación, elija Crear y, a continuación, elija un grupo de recuperación.
4. Ingrese un nombre para el grupo de recuperación y a continuación, elija Next.
5. Elija Crear celdas y a continuación, elija Añadir celda.
6. Escriba un nombre para la celda. Por ejemplo, si tiene una réplica de la aplicación en EE. UU. Oeste (Norte de California), puede agregar una celda llamada`MyApp-us-west-1`.
7. Elija Agregar celda y añada un nombre para una segunda celda. Por ejemplo, si tiene una réplica en EE. UU. Este (Ohio), puede agregar una celda llamada `MyApp-us-east-2`.
8. Si desea agregar celdas anidadas (réplicas en zonas de disponibilidad dentro de las regiones), elija Acción, elija Agregar celda anidada y, a continuación, escriba un nombre.
9. Cuando haya agregado todas las celdas y las celdas anidadas para las réplicas de las aplicaciones, elija Siguiente.
10. Revisa tu grupo de recuperación y, a continuación, selecciona Crear grupo de recuperación.

Actualizar y eliminar grupos y celdas de recuperación

Los pasos de esta sección explican cómo actualizar y eliminar un grupo de recuperación y cómo eliminar una celda de la consola ARC. Para obtener información sobre el uso de las operaciones de la API de preparación para la recuperación con Amazon Application Recovery Controller (ARC), consulte Operaciones de la API de verificación de disponibilidad.

Para actualizar o eliminar un grupo de recuperación o eliminar una celda

1. Abra la consola ARC enhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Elija Comprobación de disponibilidad.
3. En la página de preparación para la recuperación, elija un grupo de recuperación.
4. Para trabajar con un grupo de recuperación, selecciona Acción y, a continuación, selecciona Editar grupo de recuperación o Eliminar grupo de recuperación.
5. Al editar un grupo de recuperación, puede añadir o quitar celdas o celdas anidadas.
   - Para agregar una celda, elija Agregar celda.
   - Para eliminar una celda, en la etiqueta Acción situada junto a la celda, selecciona Eliminar celda.

Creación y actualización de comprobaciones de preparación en ARC

Esta sección proporciona los procedimientos para las comprobaciones de disponibilidad y los conjuntos de recursos, incluida la creación, actualización y eliminación de estos recursos.

Crear y actualizar una verificación de preparación

En los pasos de esta sección se explica cómo crear una comprobación de disponibilidad en la consola ARC. Para obtener información sobre el uso de las operaciones de la API de preparación para la recuperación con Amazon Application Recovery Controller (ARC), consulte Operaciones de la API de verificación de disponibilidad.

Para actualizar una comprobación de disponibilidad, puede editar el conjunto de recursos para la comprobación de disponibilidad, añadir o eliminar recursos o cambiar el alcance de preparación de un recurso.

Para crear una verificación de preparación

1. Abra la consola ARC enhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Elija Comprobación de disponibilidad.
3. En la página de preparación, elija Crear y, a continuación, elija una comprobación de disponibilidad.
4. Introduzca un nombre para la comprobación de disponibilidad, elija el tipo de recurso que desee comprobar y, a continuación, seleccione Siguiente.
5. Agrega un conjunto de recursos para tu verificación de disponibilidad. Un conjunto de recursos es un grupo de recursos del mismo tipo en réplicas diferentes. Seleccione una de las siguientes opciones:

   - Cree una verificación de preparación con los recursos de un conjunto de recursos que ya haya creado.
   - Cree un nuevo conjunto de recursos.

   Si decide crear un conjunto de recursos nuevo, ingrese un nombre para el conjunto de recursos y seleccione Agregar.
6. Copie y pegue los nombres de los recursos de Amazon (ARNs) uno por uno para cada recurso que desee incluir en el conjunto y, a continuación, seleccione Siguiente.

> **Tip**
>
> Para ver ejemplos y más información sobre el formato ARN que ARC espera para cada tipo de recurso, consulte. Tipos de recursos y formatos de ARN en ARC

7. Si lo desea, consulte las reglas de preparación que se utilizarán cuando ARC compruebe el tipo de recurso que incluyó en esta comprobación de disponibilidad. A continuación, elija Siguiente.
8. (Opcional) En el nombre del grupo de recuperación, elija un grupo de recuperación al que asociar la comprobación de disponibilidad y, a continuación, para cada ARN de recurso, elija una celda (región o zona de disponibilidad) en el menú desplegable en el que se encuentra el recurso. Si se trata de un recurso a nivel de aplicación, como una política de enrutamiento de DNS, elija un recurso global (sin celda).

   Esto especifica los ámbitos de preparación de los recursos en la comprobación de disponibilidad.

   > **Important**
   >
   > Si bien este paso es opcional, se deben agregar los ámbitos de preparación para obtener información resumida sobre la preparación del grupo y las células de recuperación. Si omite este paso y no asocia la verificación de preparación con los recursos de su grupo de recuperación y selecciona aquí los ámbitos de preparación, ARC no podrá devolver información resumida sobre la preparación del grupo o las celdas de recuperación.

9. Elija Next (Siguiente).
10. Revisa la información de la página de confirmación y, a continuación, selecciona Crear comprobación de preparación.

Para eliminar una verificación de preparación

1. Abra la consola ARC enhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Elija Comprobación de disponibilidad.
3. Seleccione una comprobación de disponibilidad y, en Acciones, seleccione Eliminar.

Creación y edición de conjuntos de recursos

Normalmente, se crea un conjunto de recursos como parte de la creación de una comprobación de disponibilidad, pero también se puede crear un conjunto de recursos por separado. También puede editar un conjunto de recursos para añadir o eliminar recursos. Los pasos de esta sección explican cómo crear o editar un conjunto de recursos en la consola ARC. Para obtener información sobre el uso de las operaciones de la API de preparación para la recuperación con Amazon Application Recovery Controller (ARC), consulte Operaciones de la API de verificación de disponibilidad.

Creación de un conjunto de recursos

1. Abra la consola de Route 53 en https://console.aws.amazon.com/route53/casa.
2. En Application Recovery Controller, elija Conjuntos de recursos.
3. Seleccione Crear.
4. Introduzca un nombre para el conjunto de recursos y, a continuación, elija el tipo de recurso que desee incluir en el conjunto.
5. Seleccione Agregar y, a continuación, ingrese el nombre de recurso de Amazon (ARN) del recurso que desea agregar al conjunto.
6. Cuando haya terminado de añadir recursos, elija Crear conjunto de recursos.

Para editar un conjunto de recursos

1. Abra la consola ARC enhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Elija Comprobación de disponibilidad.
3. En Conjuntos de recursos, selecciona Acción y, a continuación, selecciona Editar.
4. Realice una de las siguientes acciones:
   - Para eliminar un recurso del conjunto, seleccione Eliminar.
   - Para añadir un recurso al conjunto, seleccione Añadir y, a continuación, introduzca el nombre de recurso de Amazon (ARN) para el recurso.
5. También puede editar el ámbito de preparación del recurso para asociarlo a una celda diferente para la comprobación de disponibilidad.
6. Seleccione Guardar.

Supervisar el estado de preparación en ARC

Puede ver si su aplicación está lista en Amazon Application Recovery Controller (ARC) en los siguientes niveles:

- El nivel de verificación de disponibilidad de los recursos de un conjunto de recursos
- El nivel de recursos individuales
- El nivel de celda (réplica de la aplicación) para todos los recursos de una zona o AWS región de disponibilidad
- El nivel de grupo de recuperación de la aplicación en su conjunto

Puede recibir notificaciones sobre los cambios en el estado de preparación o puede supervisar los cambios en el estado de preparación en la consola de Route 53 o mediante los comandos de ARC CLI.

Notificación del estado de preparación

Puedes usar Amazon EventBridge para configurar reglas basadas en eventos para monitorear los recursos de ARC y notificarte los cambios en el estado de preparación. Para obtener más información, consulte Uso de la verificación de disponibilidad en ARC con Amazon EventBridge.

Supervisión del estado de preparación en la consola ARC

El siguiente procedimiento describe cómo supervisar la preparación para la recuperación en el AWS Management Console.

1. Abra la consola ARC enhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Elija Comprobación de disponibilidad.
3. En la página de preparación, en el grupo de recuperación, consulte el estado de preparación del grupo de recuperación de cada grupo de recuperación (aplicación).

   También puede ver la preparación de celdas específicas o recursos individuales.

Supervisión del estado de preparación mediante comandos CLI

En esta sección se proporcionan ejemplos de AWS CLI comandos que se pueden usar para ver el estado de preparación de la aplicación y los recursos en diferentes niveles.

Preparación para un conjunto de recursos

El estado de una verificación de preparación que creó para un conjunto de recursos (un grupo de recursos).

```
aws route53-recovery-readiness --region us-west-2 get-readiness-check-status --readiness-check-name ReadinessCheckName
```

Preparación para un solo recurso

Para obtener el estado de un único recurso en una comprobación de disponibilidad, incluido el estado de cada regla de preparación que se compruebe, especifique el nombre de la comprobación de disponibilidad y un ARN del recurso. Por ejemplo:

```
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"
```

Preparación para una celda

El estado de una sola celda, es decir, una región o zona de disponibilidad.

```
aws route53-recovery-readiness --region us-west-2 get-cell-readiness-summary --cell-name CellName
```

Preparación para una solicitud

El estado de la solicitud en general, a nivel del grupo de recuperación.

```
aws route53-recovery-readiness --region us-west-2 get-recovery-group-readiness-summary --recovery-group-name RecoveryGroupName
```

Obtener recomendaciones de arquitectura en ARC

Si ya tiene una aplicación, Amazon Application Recovery Controller (ARC) puede evaluar la arquitectura de la aplicación y las políticas de enrutamiento para ofrecer recomendaciones para modificar el diseño a fin de mejorar la resiliencia de recuperación de la aplicación. Tras crear un grupo de recuperación en ARC que represente su aplicación, siga los pasos de esta sección para obtener recomendaciones para la arquitectura de la aplicación.

Le recomendamos que especifique un recurso de destino para el recurso de destino de DNS de su grupo de recuperación, si aún no lo ha especificado, para que podamos ofrecer recomendaciones

más detalladas. Cuando proporciona información adicional, ARC puede proporcionarle mejores recomendaciones. Por ejemplo, si introduce un registro de recursos de Amazon Route 53 o un Network Load Balancer como recurso de destino, ARC puede proporcionarle información sobre si ha creado el número óptimo de celdas para su grupo de recuperación.

Tenga en cuenta lo siguiente para los recursos de destino de DNS:

- Especifique solo un registro de recursos de Route 53 o un Network Load Balancer para un recurso de destino.
- Cree solo un recurso de destino de DNS para cada grupo de recuperación.
- Recomendado: cree un recurso de destino de DNS para cada celda.
- Agrupe los recursos de destino del DNS en un conjunto de recursos con una comprobación de disponibilidad.

En el siguiente procedimiento se explica cómo crear recursos de destino de DNS y obtener recomendaciones de arquitectura para su aplicación.

Para obtener recomendaciones para actualizar su arquitectura

1. Abra la consola ARC enhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Elija Comprobación de disponibilidad.
3. En Nombre del grupo de recuperación, elija el grupo de recuperación que represente su aplicación.
4. En la página de detalles del grupo de recuperación, en el menú Acción, seleccione Obtener recomendaciones de arquitectura para este grupo de recuperación.
5. Si aún no ha creado una comprobación de disponibilidad de los recursos de destino de DNS, cree una para que ARC pueda ofrecer recomendaciones de arquitectura. Elija Crear un recurso de destino de DNS.

   Para más información acerca de recursos de objetivo DNS, consulte Comprobación de disponibilidad de los componentes .
6. Para crear un conjunto de recursos para un recurso de destino de DNS, debe crear una comprobación de disponibilidad. Introduzca un nombre para la comprobación de disponibilidad y, a continuación, para el tipo de comprobación de disponibilidad, elija el recurso de destino de DNS.
7. Introduzca un nombre para el conjunto de recursos.

8. Introduzca los atributos de la aplicación, incluidos el nombre DNS, el ARN de la zona alojada y el ID del conjunto de registros.

   > **Tip**
   >
   > Para ver el formato del ARN de una zona alojada, consulte Formato ARN de la zona alojada en. Tipos de recursos y formatos de ARN en ARC

   Opcionalmente, pero se recomienda encarecidamente, elegir Agregar atributo opcional y proporcionar un ARN de Network Load Balancer o el registro de recursos de Route 53 de su dominio.

9. (Opcional) En la configuración del grupo de recuperación, elija una celda para el recurso de destino de DNS para establecer el alcance de disponibilidad.
10. Elija Crear conjunto de recursos.
11. En la página de detalles del grupo de recuperación, selecciona Obtener recomendaciones de arquitectura. ARC muestra un conjunto de recomendaciones en la página.

Revise la lista de recomendaciones. Luego, puedes decidir si quieres hacer cambios y cómo hacerlo para mejorar la capacidad de recuperación de tu aplicación.

Crear autorizaciones multicuenta en ARC

Es posible que tenga sus recursos distribuidos en varias AWS cuentas, lo que puede dificultar la obtención de una visión integral del estado de su aplicación. También puede dificultar la obtención de la información necesaria para tomar decisiones rápidas. Para agilizar esta comprobación de disponibilidad en Amazon Application Recovery Controller (ARC), puede utilizar la autorización multicuenta.

La autorización multicuenta en ARC funciona con la función de verificación de disponibilidad. Con la autorización multicuenta, puede utilizar una AWS cuenta central para supervisar los recursos que se encuentran en varias AWS cuentas. En cada cuenta que tenga recursos que desee supervisar, usted autoriza a la cuenta central a tener acceso a esos recursos. A continuación, la cuenta central puede crear comprobaciones de disponibilidad de los recursos de todas las cuentas y, desde la cuenta central, puede supervisar la preparación de los recursos para la conmutación por error.

> **Note**
>
> La configuración de autorización entre cuentas no está disponible en la consola. En su lugar, utilice las operaciones de la API ARC para configurar y trabajar con la autorización multicuenta. Para ayudarle a empezar, en esta sección se proporcionan ejemplos de AWS CLI comandos.

Supongamos que una aplicación tiene una cuenta que tiene recursos en la región Oeste de EE. UU. (Oregón) (us-west-2) y también hay una cuenta que tiene recursos que desea monitorear en la región Este de EE. UU. (Norte de Virginia) (us-east-1). ARC puede permitir el acceso para monitorear ambos conjuntos de recursos desde una cuenta, us-west-2, mediante la autorización entre cuentas.

Por ejemplo, supongamos que tiene las siguientes cuentas: AWS

- Cuenta en el oeste de EE. UU.: 999999999999
- Cuenta en el este de EE. UU.: 111111111111

En la cuenta us-east-1 (111111111111), podemos habilitar la autorización entre cuentas para permitir el acceso de la cuenta us-west-2 (9999) especificando el nombre de recurso de Amazon (ARN) para el usuario (root) de la cuenta de IAM us-west-2:. `arn:aws:iam::999999999999:root` Tras crear la autorización, la cuenta us-west-2 puede añadir los recursos que son propiedad de us-east-1 a los conjuntos de recursos y crear comprobaciones de preparación para que se ejecuten en los conjuntos de recursos.

El siguiente ejemplo ilustra la configuración de la autorización multicuenta para una cuenta. Debe habilitar la autorización multicuenta en cada cuenta adicional que tenga AWS recursos que desee agregar y supervisar en ARC.

> **Note**
>
> ARC es un servicio global que admite puntos finales en varias AWS regiones, pero debe especificar la región EE.UU. Oeste (Oregón) (es decir, especificar el parámetro`--region us-west-2`) en la mayoría de los comandos CLI de ARC.

El siguiente AWS CLI comando muestra cómo configurar la autorización entre cuentas para este ejemplo:

```
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
```

Para deshabilitar esta autorización, haga lo siguiente:

```
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
```

Para registrar una cuenta específica para todas las cuentas para las que has autorizado varias cuentas, usa el `list-cross-account-authorizations` comando. Tenga en cuenta que en este momento no puede realizar el check-in en la otra dirección. Es decir, no hay ninguna operación de API que puedas usar con un perfil de cuenta para enumerar todas las cuentas para las que se ha concedido una autorización multicuenta para añadir y supervisar recursos.

```
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"
    ]
}
```

Reglas de preparación, tipos de recursos y ARNS

En esta sección se incluye información de referencia sobre las reglas de preparación, las descripciones y los tipos de recursos admitidos, así como el formato de los nombres de recursos de Amazon (ARNs) que se utilizan para los conjuntos de recursos.

Las descripciones de las reglas de preparación en ARC

En esta sección se enumeran las descripciones de las reglas de preparación para todos los tipos de recursos compatibles con Amazon Application Recovery Controller (ARC). Para ver una lista de los tipos de recursos compatibles con ARC, consulteTipos de recursos y formatos de ARN en ARC.

También puede ver las descripciones de las reglas de preparación en la consola ARC o mediante una operación de API, haciendo lo siguiente:

- Para ver las reglas de preparación en la consola, siga los pasos del siguiente procedimiento:Ver las reglas de preparación en la consola.
- Para ver las reglas de preparación mediante la API, consulte la ListRulesoperación.

Temas

- Reglas de preparación en ARC
- Ver las reglas de preparación en la consola

Reglas de preparación en ARC

En esta sección se muestra el conjunto de reglas de preparación para cada tipo de recurso que admite ARC.

Al revisar las descripciones de las reglas, verá que la mayoría de ellas incluyen los términos Inspecciona todas o Inspecciona cada una de ellas. Para entender cómo estos términos explican el funcionamiento de una regla en el contexto de una verificación de preparación y obtener más información sobre cómo el ARC establece el estado de preparación, consulte Cómo las reglas de preparación determinan el estado de preparación.

Reglas de preparación

El ARC audita los recursos mediante las siguientes reglas de preparación.

Etapas de Amazon API Gateway de Amazon API Gateway versión 1

- ApiGwV1ApiKeyCount: inspecciona todas las etapas de API Gateway para garantizar que tengan el mismo número de claves de API vinculadas a ellas.
- ApiGwV1ApiKeySource: Inspecciona todas las etapas de API Gateway para asegurarse de que tienen el mismo valor para`API Key Source`.
- ApiGwV1BasePath: inspecciona todas las etapas de API Gateway para garantizar que estén vinculadas a la misma ruta base.
- ApiGwV1BinaryMediaTypes: inspecciona todas las etapas de API Gateway para asegurarse de que admiten los mismos tipos de medios binarios.
- ApiGwV1CacheClusterEnabled: inspecciona todas las etapas de API Gateway para asegurarse de que todas `Cache Cluster` estén habilitadas o ninguna esté habilitada.

- ApiGwV1CacheClusterSize: Inspecciona todas las etapas de API Gateway para garantizar que tengan las mismas`Cache Cluster Size`. Si una tiene un valor mayor, las demás se marcan como NO LISTAS.
- ApiGwV1CacheClusterStatus: Inspecciona todas las etapas de API Gateway para asegurarse de que están en el estado DISPONIBLE. `Cache Cluster`
- ApiGwV1DisableExecuteApiEndpoint: inspecciona todas las etapas de API Gateway para asegurarse de que todas estén `Execute API Endpoint` deshabilitadas o ninguna esté deshabilitada.
- ApiGwV1DomainName: inspecciona todas las etapas de API Gateway para garantizar que estén vinculadas al mismo nombre de dominio.
- ApiGwV1EndpointConfiguration: inspecciona todas las etapas de API Gateway para garantizar que estén vinculadas a un dominio con la misma configuración de punto final.
- ApiGwV1EndpointDomainNameStatus: inspecciona todas las etapas de API Gateway para garantizar que el nombre de dominio al que están vinculadas esté en el estado DISPONIBLE.
- ApiGwV1MethodSettings: Inspecciona todas las etapas de API Gateway para asegurarse de que tienen el mismo valor para`Method Settings`.
- ApiGwV1MutualTlsAuthentication: Inspecciona todas las etapas de API Gateway para asegurarse de que tienen el mismo valor para`Mutual TLS Authentication`.
- ApiGwV1Policy: inspecciona todas las etapas de API Gateway para asegurarse de que todas utilizan políticas de nivel de API o ninguna lo hace.
- ApiGwV1RegionalDomainName: inspecciona todas las etapas de API Gateway para garantizar que estén vinculadas al mismo nombre de dominio regional. Nota: Esta regla no afecta al estado de preparación.
- ApiGwV1ResourceMethodConfigs: inspecciona todas las etapas de API Gateway para asegurarse de que tienen una jerarquía de recursos similar, incluidas las configuraciones relacionadas.
- ApiGwV1SecurityPolicy: Inspecciona todas las etapas de API Gateway para asegurarse de que tienen el mismo valor para`Security Policy`.
- ApiGwV1Quotas: inspecciona todos los grupos de API Gateway para asegurarse de que cumplen con las cuotas (límites) gestionadas por Service Quotas.
- ApiGwV1UsagePlans: inspecciona todas las etapas de API Gateway para asegurarse de que estén vinculadas `Usage Plans` con la misma configuración.

Etapas de Amazon API Gateway de Amazon API Gateway 2

- ApiGwV2ApiKeySelectionExpression: Inspecciona todas las etapas de API Gateway y se asegura de que tengan el mismo valor para`API Key Selection Expression`.
- ApiGwV2ApiMappingSelectionExpression: Inspecciona todas las etapas de API Gateway para asegurarse de que tienen el mismo valor para`API Mapping Selection Expression`.
- ApiGwV2CorsConfiguration: inspecciona todas las etapas de API Gateway para asegurarse de que tienen la misma configuración relacionada con CORS.
- ApiGwV2DomainName: inspecciona todas las etapas de API Gateway para garantizar que estén vinculadas al mismo nombre de dominio.
- ApiGwV2DomainNameStatus: inspecciona todas las etapas de API Gateway para garantizar que el nombre de dominio esté en el estado DISPONIBLE.
- ApiGwV2EndpointType: Inspecciona todas las etapas de API Gateway para asegurarse de que tienen el mismo valor para`Endpoint Type`.
- ApiGwV2Quotas: inspecciona todos los grupos de API Gateway para asegurarse de que cumplen con las cuotas (límites) gestionadas por Service Quotas.
- ApiGwV2MutualTlsAuthentication: Inspecciona todas las etapas de API Gateway para asegurarse de que tienen el mismo valor para`Mutual TLS Authentication`.
- ApiGwV2ProtocolType: Inspecciona todas las etapas de API Gateway para asegurarse de que tienen el mismo valor para`Protocol Type`.
- ApiGwV2RouteConfigs: inspecciona todas las etapas de API Gateway para asegurarse de que tienen la misma jerarquía de rutas con la misma configuración.
- ApiGwV2RouteSelectionExpression: Inspecciona todas las etapas de API Gateway para asegurarse de que tienen el mismo valor para`Route Selection Expression`.
- ApiGwV2RouteSettings: Inspecciona todas las etapas de API Gateway para asegurarse de que tienen el mismo valor para`Default Route Settings`.
- ApiGwV2SecurityPolicy: Inspecciona todas las etapas de API Gateway para asegurarse de que tienen el mismo valor para`Security Policy`.
- ApiGwV2StageVariables: Inspecciona todas las etapas de API Gateway para garantizar que todas tengan las `Stage Variables` mismas que las demás etapas.
- ApiGwV2ThrottlingBurstLimit: Inspecciona todas las etapas de API Gateway para asegurarse de que tienen el mismo valor para`Throttling Burst Limit`.
- ApiGwV2ThrottlingRateLimit: Inspecciona todas las etapas de API Gateway para asegurarse de que tienen el mismo valor para`Throttling Rate Limit`.

Clústeres de Amazon Aurora

- RdsClusterStatus: inspecciona cada cúmulo de Aurora para asegurarse de que tiene un estado de `AVAILABLE` o`BACKING-UP`.
- RdsEngineMode: Inspecciona todos los clústeres de Aurora para asegurarse de que tienen el mismo valor para`Engine Mode`.
- RdsEngineVersion: Inspecciona todos los clústeres de Aurora para asegurarse de que tienen el mismo valor para`Major Version`.
- RdsGlobalReplicaLag: Inspecciona cada cúmulo de Aurora para asegurarse de que `Global Replica Lag` dura menos de 30 segundos.
- RdsNormalizedCapacity: inspecciona todos los clústeres de Aurora para garantizar que tengan una capacidad normalizada dentro del 15% del máximo del conjunto de recursos.
- RdsInstanceType: inspecciona todos los clústeres de Aurora para asegurarse de que tienen los mismos tipos de instancias.
- RdsQuotas: Inspecciona todos los clústeres de Aurora para asegurarse de que cumplen con las cuotas (límites) que administra Service Quotas.

Grupos de escalado automático

- AsgMinSizeAndMaxSize: Inspecciona todos los grupos de Auto Scaling para asegurarse de que tienen los mismos tamaños de grupo mínimo y máximo.
- AsgAZCount: Inspecciona todos los grupos de Auto Scaling para asegurarse de que tienen el mismo número de zonas de disponibilidad.
- AsgInstanceTypes: Inspecciona todos los grupos de Auto Scaling para asegurarse de que tienen los mismos tipos de instancias. Nota: Esta regla no afecta al estado de preparación.
- AsgInstanceSizes: Inspecciona todos los grupos de Auto Scaling para asegurarse de que tienen los mismos tamaños de instancia.
- AsgNormalizedCapacity: Inspecciona todos los grupos de Auto Scaling para asegurarse de que tienen una capacidad normalizada dentro del 15% del máximo del conjunto de recursos.
- AsgQuotas: Inspecciona todos los grupos de Auto Scaling para asegurarse de que cumplen con las cuotas (límites) que administra Service Quotas.

CloudWatch alarmas

- CloudWatchAlarmState: Inspecciona CloudWatch las alarmas para asegurarse de que ninguna de ellas esté en el `INSUFFICIENT_DATA` estado `ALARM` o.

Puertas de enlace de cliente

- CustomerGatewayIpAddress: Inspecciona todas las pasarelas de los clientes para asegurarse de que tienen la misma dirección IP.
- CustomerGatewayState: Inspecciona las pasarelas de los clientes para asegurarse de que cada una esté en el estado. `AVAILABLE`
- CustomerGatewayVPNType: Inspecciona todas las pasarelas de los clientes para asegurarse de que tienen el mismo tipo de VPN.

DNS target resources

- DnsTargetResourceHostedZoneConfigurationRule: Inspecciona todos los recursos de destino del DNS para asegurarse de que tienen el mismo ID de zona alojada de Amazon Route 53 y de que cada zona alojada no es privada. Nota: Esta regla no afecta al estado de preparación.
- DnsTargetResourceRecordSetConfigurationRule: Inspecciona todos los recursos de destino del DNS para asegurarse de que tienen el mismo tiempo de vida de la memoria caché (TTL) del registro de recursos y de que TTLs son inferiores o iguales a 300.
- DnsTargetResourceRoutingRule: inspecciona cada recurso de destino de DNS asociado a un conjunto de registros de recursos de alias para asegurarse de que enruta el tráfico al nombre de DNS configurado en el recurso de destino. Nota: Esta regla no afecta al estado de preparación.
- DnsTargetResourceHealthCheckRule: Inspecciona todos los recursos de destino del DNS para garantizar que las comprobaciones de estado estén asociadas a sus conjuntos de registros de recursos cuando proceda y no de otra manera. Nota: Esta regla no afecta al estado de preparación.

Tablas de Amazon DynamoDB

- DynamoConfiguration: inspecciona todas las tablas de DynamoDB para asegurarse de que tienen las mismas claves, atributos, cifrado del lado del servidor y configuraciones de transmisiones.
- DynamoTableStatus: inspecciona cada tabla de DynamoDB para asegurarse de que su estado es ACTIVO.
- DynamoCapacity: inspecciona todas las tablas de DynamoDB para garantizar que las capacidades de lectura y escritura aprovisionadas estén dentro del 20% de las capacidades máximas del conjunto de recursos.
- DynamoPeakRcuWcu: inspecciona cada tabla de DynamoDB para asegurarse de que ha tenido picos de tráfico similares a los de las demás tablas, a fin de garantizar la capacidad aprovisionada.

- DynamoGsiPeakRcuWcu: inspecciona cada tabla de DynamoDB para asegurarse de que tiene una capacidad máxima de lectura y escritura similar a la de las demás tablas, a fin de garantizar la capacidad aprovisionada.
- DynamoGsiConfig: inspecciona todas las tablas de DynamoDB que tienen índices secundarios globales para asegurarse de que utilizan el mismo índice, esquema clave y proyección.
- DynamoGsiStatus: inspecciona todas las tablas de DynamoDB que tienen índices secundarios globales para garantizar que los índices secundarios globales tengan un estado ACTIVO.
- DynamoGsiCapacity: inspecciona todas las tablas de DynamoDB que tienen índices secundarios globales para garantizar que las tablas tengan capacidades de lectura de GSI y de escritura de GSI aprovisionadas dentro del 20% de las capacidades máximas del conjunto de recursos.
- DynamoReplicationLatency: inspecciona todas las tablas de DynamoDB que son tablas globales para asegurarse de que tienen la misma latencia de replicación.
- DynamoAutoScalingConfiguration: inspecciona todas las tablas de DynamoDB que tienen activado Auto Scaling para garantizar que tengan las mismas capacidades de lectura y escritura mínima, máxima y objetivo.
- DynamoQuotas: inspecciona todas las tablas de DynamoDB para asegurarse de que se ajustan a las cuotas (límites) que administra Service Quotas.

Elastic Load Balancing (Classic Load Balancers)

- ElbV1CheckAzCount: inspecciona cada Classic Load Balancer para asegurarse de que esté conectado a una sola zona de disponibilidad. Nota: Esta regla no afecta al estado de preparación.
- ElbV1AnyInstances: Inspecciona todos los balanceadores de carga clásicos para asegurarse de que tienen al menos una instancia. EC2
- ElbV1AnyInstancesHealthy: inspecciona todos los balanceadores de carga clásicos para asegurarse de que tienen al menos una instancia en buen estado. EC2
- ElbV1Scheme: Inspecciona todos los balanceadores de carga clásicos para asegurarse de que tienen el mismo esquema de balanceadores de carga.
- ElbV1HealthCheckThreshold: inspecciona todos los balanceadores de carga clásicos para asegurarse de que tienen el mismo valor límite de verificación de estado.
- ElbV1HealthCheckInterval: inspecciona todos los balanceadores de carga clásicos para asegurarse de que tienen el mismo valor de intervalo de comprobación de estado.

- ElbV1CrossZoneRoutingEnabled: inspecciona todos los balanceadores de carga clásicos para asegurarse de que tienen el mismo valor para el equilibrio de carga entre zonas (ACTIVADO o DESACTIVADO).
- ElbV1AccessLogsEnabledAttribute: inspecciona todos los balanceadores de carga clásicos para asegurarse de que tienen el mismo valor para los registros de acceso (ACTIVADOS o DESACTIVADOS).
- ElbV1ConnectionDrainingEnabledAttribute: inspecciona todos los balanceadores de carga clásicos para asegurarse de que tienen el mismo valor de agotamiento de conexiones (ACTIVADO o DESACTIVADO).
- ElbV1ConnectionDrainingTimeoutAttribute: inspecciona todos los balanceadores de carga clásicos para asegurarse de que tienen el mismo valor de tiempo de espera de descarga de conexiones.
- ElbV1IdleTimeoutAttribute: inspecciona todos los balanceadores de carga clásicos para asegurarse de que tienen el mismo valor de tiempo de espera de inactividad.
- ElbV1ProvisionedCapacityLcuCount: inspecciona todos los balanceadores de carga clásicos con una LCU aprovisionada superior a 10 para asegurarse de que se encuentran dentro del 20% de la LCU más aprovisionada del conjunto de recursos.
- ElbV1ProvisionedCapacityStatus: inspecciona el estado de la capacidad aprovisionada en cada Classic Load Balancer para asegurarse de que no tenga el valor DISABLED o PENDING.

Volúmenes de Amazon EBS

- EbsVolumeEncryption: Inspecciona todas EBS volúmenes para asegurarse de que tienen el mismo valor de cifrado (ACTIVADO o DESACTIVADO).
- EbsVolumeEncryptionDefault: inspecciona todos EBS los volúmenes para asegurarse de que tienen el mismo valor de cifrado de forma predeterminada (ACTIVADO o DESACTIVADO).
- EbsVolumeIops: inspecciona todos EBS volúmenes para garantizar que tengan las mismas operaciones de entrada/salida por segundo (IOPS).
- EbsVolumeKmsKeyId: Inspecciona todos EBS volúmenes para asegurarse de que tienen el mismo ID de AWS KMS clave predeterminado.
- EbsVolumeMultiAttach: inspecciona todos EBS volúmenes para asegurarse de que tienen el mismo valor para la conexión múltiple (ACTIVADA o DESACTIVADA).
- EbsVolumeQuotas: Inspecciona todos EBS volúmenes para garantizar que se ajustan a las cuotas (límites) establecidas por Service Quotas.
- EbsVolumeSize: Inspecciona todos EBS volúmenes para asegurarse de que tienen el mismo tamaño legible.

- EbsVolumeState: Inspecciona todos EBS volúmenes para asegurarse de que tienen el mismo estado de volumen.
- EbsVolumeType: Inspecciona todos EBS volúmenes para asegurarse de que tienen el mismo tipo de volumen.

AWS Lambda funciones

- LambdaMemorySize: inspecciona todas las funciones de Lambda para asegurarse de que tienen el mismo tamaño de memoria. Si una tiene más memoria, las demás aparecen marcadas. `NOT READY`
- LambdaFunctionTimeout: inspecciona todas las funciones de Lambda para asegurarse de que tienen el mismo valor de tiempo de espera. Si una tiene un valor mayor, las demás se marcan. `NOT READY`
- LambdaFunctionRuntime: inspecciona todas las funciones de Lambda para garantizar que todas tengan el mismo tiempo de ejecución.
- LambdaFunctionReservedConcurrentExecutions: inspecciona todas las funciones de Lambda para asegurarse de que todas tienen el mismo valor para. `Reserved Concurrent Executions` Si una tiene un valor mayor, las demás se marcan. `NOT READY`
- LambdaFunctionDeadLetterConfig: inspecciona todas las funciones de Lambda para asegurarse de que todas tienen `Dead Letter Config` un valor definido o que ninguna lo tiene.
- LambdaFunctionProvisionedConcurrencyConfig: inspecciona todas las funciones de Lambda para asegurarse de que tienen el mismo valor para. `Provisioned Concurrency`
- LambdaFunctionSecurityGroupCount: inspecciona todas las funciones de Lambda para asegurarse de que tienen el mismo valor para. `Security Groups`
- LambdaFunctionSubnetIdCount: inspecciona todas las funciones de Lambda para asegurarse de que tienen el mismo valor para. `Subnet Ids`
- LambdaFunctionEventSourceMappingMatch: inspecciona todas las funciones de Lambda para asegurarse de que todas las propiedades `Event Source Mapping` elegidas coinciden entre sí.
- LambdaFunctionLimitsRule: Inspecciona todas las funciones de Lambda para asegurarse de que se ajustan a las cuotas (límites) gestionadas por Service Quotas.

Application Load Balancers y Network Load Balancers

- ElbV2CheckAzCount: inspecciona cada Network Load Balancer para asegurarse de que esté conectado a una sola zona de disponibilidad. Nota: Esta regla no afecta al estado de preparación.

- ElbV2TargetGroupsCanServeTraffic: inspecciona cada Network Load Balancer y Application Load Balancer para asegurarse de que tienen al menos una instancia de Amazon en buen estado. EC2
- ElbV2State: inspecciona cada Network Load Balancer y Application Load Balancer para asegurarse de que están en ese estado. `ACTIVE`
- ElbV2IpAddressType: inspecciona todos los balanceadores de carga de red y los balanceadores de carga de aplicaciones para asegurarse de que tienen los mismos tipos de direcciones IP.
- ElbV2Scheme: inspecciona todos los balanceadores de carga de red y los balanceadores de carga de aplicaciones para asegurarse de que tienen el mismo esquema.
- ElbV2Type: Inspecciona todos los balanceadores de carga de red y los balanceadores de carga de aplicaciones para asegurarse de que son del mismo tipo.
- ElbV2S3LogsEnabled: inspecciona todos los balanceadores de carga de red y los balanceadores de carga de aplicaciones para asegurarse de que tienen el mismo valor para los registros de acceso al servidor Amazon S3 (HABILITADO o DESHABILITADO).
- ElbV2DeletionProtection: Inspecciona todos los balanceadores de carga de red y los balanceadores de carga de aplicaciones para asegurarse de que tienen el mismo valor de protección contra la eliminación (ACTIVADO o DESACTIVADO).
- ElbV2IdleTimeoutSeconds: Inspecciona todos los balanceadores de carga de red y los balanceadores de carga de aplicaciones para asegurarse de que tienen el mismo valor durante los segundos de tiempo de inactividad.
- ElbV2HttpDropInvalidHeaders: inspecciona todos los balanceadores de carga de red y los balanceadores de carga de aplicaciones para asegurarse de que tienen el mismo valor para los encabezados no válidos de HTTP.
- ElbV2Http2Enabled: inspecciona todos los balanceadores de carga de red y los balanceadores de carga de aplicaciones para asegurarse de que tienen el mismo valor para HTTP2 (ACTIVADO o DESACTIVADO).
- ElbV2CrossZoneEnabled: Inspecciona todos los balanceadores de carga de red y los balanceadores de carga de aplicaciones para asegurarse de que tienen el mismo valor para el equilibrio de carga entre zonas (ACTIVADO o DESACTIVADO).
- ElbV2ProvisionedCapacityLcuCount: inspecciona todos los balanceadores de carga de red y los balanceadores de carga de aplicaciones con una LCU aprovisionada superior a 10 para asegurarse de que se encuentran dentro del 20% de la LCU más aprovisionada del conjunto de recursos.

- ElbV2ProvisionedCapacityEnabled: Inspecciona el estado de la capacidad aprovisionada de todos los balanceadores de carga de red y los balanceadores de carga de aplicaciones para asegurarse de que no tengan el valor DESHABILITADO o PENDIENTE.

Clústeres de Amazon MSK

- MskClusterClientSubnet: inspecciona cada clúster de MSK para asegurarse de que solo tiene dos o solo tres subredes de clientes.
- MskClusterInstanceType: inspecciona todos los clústeres de MSK para asegurarse de que tienen el mismo tipo de EC2 instancia de Amazon.
- MskClusterSecurityGroups: Inspecciona todos los clústeres de MSK para asegurarse de que tienen los mismos grupos de seguridad.
- MskClusterStorageInfo: Inspecciona todos los clústeres de MSK para asegurarse de que tienen el mismo tamaño de volumen de almacenamiento de EBS. Si uno tiene un valor mayor, los demás aparecen marcados como NO LISTOS.
- MskClusterACMCertificate: inspecciona todos los clústeres de MSK para asegurarse de que tienen la misma lista de certificados de autorización de clientes. ARNs
- MskClusterServerProperties: Inspecciona todos los clústeres de MSK para asegurarse de que tienen el mismo valor para. `Current Broker Software Info`
- MskClusterKafkaVersion: Inspecciona todos los clústeres de MSK para asegurarse de que tienen la misma versión de Kafka.
- MskClusterEncryptionInTransitInCluster: inspecciona todos los clústeres de MSK para asegurarse de que tienen el mismo valor para. `Encryption In Transit In Cluster`
- MskClusterEncryptionInClientBroker: inspecciona todos los clústeres de MSK para asegurarse de que tienen el mismo valor para. `Encryption In Transit Client Broker`
- MskClusterEnhancedMonitoring: inspecciona todos los clústeres de MSK para asegurarse de que tienen el mismo valor para. `Enhanced Monitoring`
- MskClusterOpenMonitoringInJmx: inspecciona todos los clústeres de MSK para asegurarse de que tienen el mismo valor para. `Open Monitoring JMX Exporter`
- MskClusterOpenMonitoringInNode: Inspecciona todos los clústeres de MSK para asegurarse de que tienen el mismo valor para `Open Monitoring Not Exporter.`
- MskClusterLoggingInS3: inspecciona todos los clústeres de MSK para asegurarse de que tienen el mismo valor para. `Is Logging in S3`
- MskClusterLoggingInFirehose: inspecciona todos los clústeres de MSK para asegurarse de que tienen el mismo valor para. `Is Logging In Firehose`

- MskClusterLoggingInCloudWatch: inspecciona todos los clústeres de MSK para asegurarse de que tienen el mismo valor para. `Is Logging Available In CloudWatch Logs`
- MskClusterNumberOfBrokerNodes: inspecciona todos los clústeres de MSK para asegurarse de que tienen el mismo valor para. `Number of Broker Nodes` Si uno tiene un valor mayor, los demás se marcan como NO LISTOS.
- MskClusterState: inspecciona cada clúster de MSK para asegurarse de que se encuentra en un estado ACTIVO.
- MskClusterLimitsRule: Inspecciona todas las funciones de Lambda para asegurarse de que se ajustan a las cuotas (límites) gestionadas por Service Quotas.

Comprobaciones de estado de Amazon Route 53

- R53HealthCheckType: Inspecciona cada comprobación de estado de Route 53 para asegurarse de que no es del tipo CALCULATED y de que todas las comprobaciones son del mismo tipo.
- R53HealthCheckDisabled: Inspecciona cada chequeo de estado de Route 53 para asegurarse de que no tenga el estado DESACTIVADO.
- R53HealthCheckStatus: Inspecciona cada comprobación de estado de Route 53 para asegurarse de que se ha realizado CORRECTAMENTE.
- R53HealthCheckRequestInterval: Inspecciona todos los controles de estado de Route 53 para garantizar que todos tengan el mismo valor para`Request Interval`.
- R53HealthCheckFailureThreshold: Inspecciona todos los controles de estado de Route 53 para garantizar que todos tengan el mismo valor para `Failure Threshold.`
- R53HealthCheckEnableSNI: Inspecciona todos los controles de estado de Route 53 para garantizar que todos tengan el mismo valor para `Enable SNI.`
- R53HealthCheckSearchString: Inspecciona todos los controles de estado de Route 53 para garantizar que todos tengan el mismo valor para `Search String.`
- R53HealthCheckRegions: Inspecciona todos los controles de estado de Route 53 para garantizar que todos tengan la misma lista de AWS regiones.
- R53HealthCheckMeasureLatency: Inspecciona todos los controles de estado de Route 53 para garantizar que todos tengan el mismo valor para`Measure Latency`.
- R53HealthCheckInsufficientDataHealthStatus: Inspecciona todos los controles de estado de Route 53 para garantizar que todos tengan el mismo valor para`Insufficient Data Health Status`.

- R53HealthCheckInverted: Inspecciona todos los controles de estado de Route 53 para asegurarse de que estén todos invertidos o no estén invertidos.
- R53HealthCheckResourcePath: Inspecciona todos los controles de estado de Route 53 para garantizar que todos tengan el mismo valor para`Resource Path`.
- R53HealthCheckCloudWatchAlarm: Inspecciona todas las comprobaciones de estado de Route 53 para garantizar que las CloudWatch alarmas asociadas a ellas tengan los mismos ajustes y configuraciones.

Suscripciones a Amazon SNS

- SnsSubscriptionProtocol: Inspecciona todas las suscripciones de SNS para asegurarse de que tienen el mismo protocolo.
- SnsSubscriptionSqsLambdaEndpoint: inspecciona todas las suscripciones de SNS que tienen puntos de enlace Lambda o SQS para asegurarse de que tienen puntos de enlace diferentes.
- SnsSubscriptionNonAwsEndpoint: inspecciona todas las suscripciones de SNS que tienen un tipo de punto final que no es de AWS servicio, por ejemplo, el correo electrónico, para asegurarse de que las suscripciones tienen el mismo punto final.
- SnsSubscriptionPendingConfirmation: inspecciona todas las suscripciones de SNS para asegurarse de que tienen el mismo valor para «Confirmaciones pendientes».
- SnsSubscriptionDeliveryPolicy: Inspecciona todas las suscripciones de redes sociales que utilizan HTTP/S para garantizar que tengan el mismo valor durante el «período de entrega efectivo».
- SnsSubscriptionRawMessageDelivery: Inspecciona todas las suscripciones de redes sociales para asegurarse de que tienen el mismo valor para «Entrega de mensajes sin procesar».
- SnsSubscriptionFilter: inspecciona todas las suscripciones de redes sociales para asegurarse de que tienen el mismo valor en «Política de filtros».
- SnsSubscriptionRedrivePolicy: Inspecciona todas las suscripciones de SNS para asegurarse de que tienen el mismo valor para la «Política de redrive».
- SnsSubscriptionEndpointEnabled: Inspecciona todas las suscripciones de SNS para asegurarse de que tienen el mismo valor para «Endpoint Enabled».
- SnsSubscriptionLambdaEndpointValid: inspecciona todas las suscripciones de SNS que tienen puntos de enlace de Lambda para asegurarse de que tienen puntos de enlace de Lambda válidos.
- SnsSubscriptionSqsEndpointValidRule: Inspecciona todas las suscripciones de SNS que utilizan puntos de conexión de SQS para asegurarse de que tienen puntos de conexión de SQS válidos.

- SnsSubscriptionQuotas: inspecciona todas las suscripciones de SNS para asegurarse de que se ajustan a las cuotas (límites) que gestiona Service Quotas.

Temas de Amazon SNS

- SnsTopicDisplayName: inspecciona todos los temas de SNS para asegurarse de que tienen el mismo valor para. `Display Name`
- SnsTopicDeliveryPolicy: Inspecciona todos los temas de SNS que tienen suscriptores de HTTPS para asegurarse de que tienen los mismos suscriptores. `EffectiveDeliveryPolicy`
- SnsTopicSubscription: inspecciona todos los temas de SNS para asegurarse de que tienen el mismo número de suscriptores para cada uno de sus protocolos.
- SnsTopicAwsKmsKey: Inspecciona todos los temas del SNS para asegurarse de que todos los temas o ninguno de ellos tengan una clave. AWS KMS
- SnsTopicQuotas: inspecciona todos los temas de SNS para asegurarse de que se ajustan a las cuotas (límites) gestionadas por Service Quotas.

Colas de Amazon SQS

- SqsQueueType: Inspecciona todas las colas de SQS para asegurarse de que todas tienen el mismo valor. `Type`
- SqsQueueDelaySeconds: Inspecciona todas las colas de SQS para asegurarse de que todas tienen el mismo valor para. `Delay Seconds`
- SqsQueueMaximumMessageSize: Inspecciona todas las colas de SQS para asegurarse de que todas tienen el mismo valor para. `Maximum Message Size`
- SqsQueueMessageRetentionPeriod: Inspecciona todas las colas de SQS para asegurarse de que todas tienen el mismo valor para. `Message Retention Period`
- SqsQueueReceiveMessageWaitTimeSeconds: Inspecciona todas las colas de SQS para asegurarse de que todas tienen el mismo valor para. `Receive Message Wait Time Seconds`
- SqsQueueRedrivePolicyMaxReceiveCount: Inspecciona todas las colas de SQS para asegurarse de que todas tienen el mismo valor para. `Redrive Policy Max Receive Count`
- SqsQueueVisibilityTimeout: Inspecciona todas las colas de SQS para asegurarse de que todas tienen el mismo valor para. `Visibility Timeout`
- SqsQueueContentBasedDeduplication: Inspecciona todas las colas de SQS para asegurarse de que todas tienen el mismo valor para. `Content-Based Deduplication`

- SqsQueueQuotas: Inspecciona todas las colas de SQS para asegurarse de que se ajustan a las cuotas (límites) gestionadas por Service Quotas.

Amazon VPCs

- VpcCidrBlock: Inspecciona todos VPCs para asegurarse de que todos tienen el mismo valor para el tamaño de la red de bloques CIDR.
- VpcCidrBlocksSameProtocolVersion: inspecciona todos los VPCs que tienen los mismos bloques CIDR para asegurarse de que tienen el mismo valor para el número de versión del Protocolo de flujo de Internet.
- VpcCidrBlocksStateInAssociationSets: inspecciona todos los conjuntos de asociaciones de bloques de CIDR VPCs para asegurarse de que todos tienen bloques de CIDR en un mismo estado. `ASSOCIATED`
- VpcIpv6CidrBlocksStateInAssociationSets: inspecciona todos los conjuntos de asociaciones de bloques de CIDR VPCs para asegurarse de que todos tienen bloques de CIDR con el mismo número de direcciones.
- VpcCidrBlocksInAssociationSets: Inspecciona todos los conjuntos de asociaciones de bloques del CIDR VPCs para asegurarse de que todos tienen el mismo tamaño.
- VpcIpv6CidrBlocksInAssociationSets: Inspecciona todos los conjuntos de asociaciones de bloques del IPv6 CIDR VPCs para asegurarse de que tienen el mismo tamaño.
- VpcState: inspecciona cada VPC para asegurarse de que se encuentra en `AVAILABLE` un estado.
- VpcInstanceTenancy: Inspecciona todos VPCs para asegurarse de que todos tienen el mismo valor para. `Instance Tenancy`
- VpcIsDefault: Inspecciona todos VPCs para asegurarse de que tienen el mismo valor para `Is Default.`
- VpcSubnetState: inspecciona cada subred de VPC para asegurarse de que se encuentra en un estado DISPONIBLE.
- VpcSubnetAvailableIpAddressCount: inspecciona cada subred de VPC para asegurarse de que tiene un recuento de direcciones IP disponible superior a cero.
- VpcSubnetCount: inspecciona todas las subredes de VPC para asegurarse de que tienen el mismo número de subredes.
- VpcQuotas: inspecciona todas las subredes de VPC para asegurarse de que cumplen con las cuotas (límites) que administra Service Quotas.

AWS VPN conexiones

- VpnConnectionsRouteCount: Inspecciona todas las conexiones VPN para asegurarse de que tienen al menos una ruta y también el mismo número de rutas.
- VpnConnectionsEnableAcceleration: Inspecciona todas las conexiones VPN para asegurarse de que tienen el mismo valor para. `Enable Accelerations`
- VpnConnectionsStaticRoutesOnly: Inspecciona todas las conexiones VPN para asegurarse de que tienen el mismo valor para `Static Routes Only.`
- VpnConnectionsCategory: Inspecciona todas las conexiones VPN para asegurarse de que tienen una categoría de. `VPN`
- VpnConnectionsCustomerConfiguration: Inspecciona todas las conexiones VPN para asegurarse de que tienen el mismo valor para. `Customer Gateway Configuration`
- VpnConnectionsCustomerGatewayId: Inspecciona cada conexión VPN para asegurarse de que tiene conectada una pasarela de cliente.
- VpnConnectionsRoutesState: Inspecciona todas las conexiones VPN para asegurarse de que están en buen estado. `AVAILABLE`
- VpnConnectionsVgwTelemetryStatus: Inspecciona cada conexión VPN para asegurarse de que su estado VGW es de. `UP`
- VpnConnectionsVgwTelemetryIpAddress: Inspecciona cada conexión VPN para asegurarse de que tiene una dirección IP externa diferente para cada telemetría de VGW.
- VpnConnectionsTunnelOptions: Inspecciona todas las conexiones VPN para asegurarse de que tienen las mismas opciones de túnel.
- VpnConnectionsRoutesCidr: Inspecciona todas las conexiones VPN para asegurarse de que tienen los mismos bloques CIDR de destino.
- VpnConnectionsInstanceType: Inspecciona todas las conexiones VPN para asegurarse de que tienen las mismas conexiones. `Instance Type`

AWS VPN pasarelas

- VpnGatewayState: Inspecciona todas las pasarelas VPN para asegurarse de que estén en un estado DISPONIBLE.
- VpnGatewayAsn: Inspecciona todas las pasarelas VPN para asegurarse de que tienen el mismo ASN.
- VpnGatewayType: Inspecciona todas las pasarelas VPN para asegurarse de que son del mismo tipo.

- VpnGatewayAttachment: Inspecciona todas las pasarelas VPN para asegurarse de que tienen las mismas configuraciones de conexión.

Ver las reglas de preparación en la consola

Puede ver las reglas de preparación en las AWS Management Console listas de cada tipo de recurso.

Para ver las reglas de preparación en la consola

1. Abra la consola ARC enhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. Elija Comprobación de disponibilidad.
3. En Tipo de recurso, elija el tipo de recurso cuyas reglas desee ver.

Tipos de recursos y formatos de ARN en ARC

Al crear un conjunto de recursos en Amazon Application Recovery Controller (ARC), se especifica el tipo de recurso que se va a incluir en el conjunto y los nombres de los recursos de Amazon (ARNs) para cada uno de los recursos que se van a incluir. ARC espera un formato de ARN específico para cada tipo de recurso. En esta sección se enumeran los tipos de recursos compatibles con ARC y los formatos de ARN asociados a cada uno de ellos.

El formato específico depende del recurso. Cuando proporciones un ARN, reemplaza el *italicized* texto por la información específica del recurso.

> **Note**
>
> Tenga en cuenta que el formato de ARN que ARC requiere para los recursos puede diferir del formato de ARN que el propio servicio requiere para sus recursos. Por ejemplo, es posible que los formatos de ARN que se describen en las secciones de tipo de recurso de cada servicio de la Referencia de autorización del servicio no incluyan el Cuenta de AWS ID u otra información que ARC necesita para admitir las funciones del servicio ARC.

AWS::ApiGateway::Stage

Una etapa Versión 1 de Amazon API Gateway:

- Formato de ARN: `arn:partition:apigateway:region:account:/restapis/api-id/stages/stage-name`

  Ejemplo: `arn:aws:apigateway:us-east-1:111122223333:/restapis/123456789/stages/ExampleStage`

  Para obtener más información, consulte Referencia de Nombre de recurso de Amazon (ARN) y puerta de enlace.

AWS::ApiGatewayV2::Stage

Una etapa Versión 1 de Amazon API Gateway:

- Formato de ARN: `arn:partition:apigateway:region:account:/apis/api-id/stages/stage-name`

  Ejemplo: `arn:aws:apigateway:us-east-1:111122223333:/apis/123456789/stages/ExampleStage`

  Para obtener más información, consulte Referencia de Nombre de recurso de Amazon (ARN) y puerta de enlace.

AWS::CloudWatch::Alarm

Una CloudWatch alarma de Amazon.

- Formato de ARN: `arn:partition:cloudwatch:region:account:alarm:alarm-name`

  Ejemplo: `arn:aws:cloudwatch:us-west-2:111122223333:alarm:test-alarm-1`

  Para obtener más información, consulta Tipos de recursos definidos por Amazon CloudWatch.

AWS::DynamoDB::Table

Una tabla de Amazon DynamoDB.

- Formato de ARN: `arn:partition:dynamodb:region:account:table/table-name`

  Ejemplo: `arn:aws:dynamodb:us-west-2:111122223333:table/BigTable`

  Para obtener más información, consulte Recursos y operaciones de DynamoDB.

AWS::EC2::CustomerGateway

Un dispositivo de puerta de enlace de cliente

- Formato de ARN: `arn:partition:ec2:region:account:customer-gateway/CustomerGatewayId`

  Ejemplo: `arn:aws:ec2:us-west-2:111122223333:customer-gateway/vcg-123456789`

  Para obtener más información, consulta Tipos de recursos definidos por Amazon EC2.

AWS::EC2::Volume

Volumen de Amazon EBS

- Formato de ARN: `arn:partition:ec2:region:account:volume/VolumeId`

  Ejemplo: `arn:aws:ec2:us-west-2:111122223333:volume/volume-of-cylinder-is-pi`

  Para obtener más información, consulte Referencia de Nombre de recurso de Amazon (ARN) y puerta de enlace.

AWS::ElasticLoadBalancing::LoadBalancer

Un equilibrador de carga clásico.

- Formato de ARN: `arn:partition:elasticloadbalancing:region:account:loadbalancer/LoadBalancerN`

  Ejemplo: `arn:aws:elasticloadbalancing:us-west-2:111122223333:loadbalancer/123456789abcbdeCLB`

  Para obtener más información, consulte Recursos Elastic Load Balancing.

AWS::ElasticLoadBalancingV2::LoadBalancer

Un equilibrador de carga de red o un equilibrador de carga de aplicación.

- Formato ARN para Network Load Balancer: `arn:partition:elasticloadbalancing:region:account:loadbalancer/net/LoadBalancerName`

  Ejemplo de Network Load Balancer: `arn:aws:elasticloadbalancing:us-west-2:111122223333:loadbalancer/net/sandbox-net/123456789acbdeNLB`

- Formato ARN para Application Load Balancer: `arn:partition:elasticloadbalancing:region:account:loadbalancer/app/LoadBalancerName`

Ejemplo de Application Load Balancer: `arn:aws:elasticloadbalancing:us-west-2:111122223333:loadbalancer/app/sandbox-alb/123456789acbdeALB`

Para obtener más información, consulte Recursos Elastic Load Balancing.

AWS::Lambda::Function

Una AWS Lambda función.

- Formato de ARN: `arn:`*`partition`*`:lambda:`*`region`*`:`*`account`*`:function:`*`FunctionName`*

  Ejemplo: `arn:aws:lambda:us-west-2:111122223333:function:my-function`

  Para obtener más información, consulte la sección Recursos y condiciones para acciones Lambda.

AWS::MSK::Cluster

Un clúster de Amazon MSK

- Formato de ARN: `arn:`*`partition`*`:kafka:`*`region`*`:`*`account`*`:cluster/`*`ClusterName`*`/`*`UUID`*

  Ejemplo: `arn:aws:kafka:us-east-1:111122223333:cluster/demo-cluster-1/123456-1111-2222-3333`

  Para obtener más información, consulte Tipos de recurso definidos por Amazon Managed Streaming for Apache Kafka.

AWS::RDS::DBCluster

Un clúster de base de datos de Aurora

- Formato de ARN: `arn:`*`partition`*`:rds:`*`region`*`:`*`account`*`:cluster:`*`DbClusterInstanceName`*

  Ejemplo: `arn:aws:rds:us-west-2:111122223333:cluster:database-1`

  Para obtener más información, consulte Trabajar con Amazon Resource Names (ARNs) en Amazon RDS.

AWS::Route53::HealthCheck

Una comprobación de estado de Amazon Route 53

- Formato de ARN: `arn:`*`partition`*`:route53:::healthcheck/`*`Id`*

Ejemplo: `arn:aws:route53:::healthcheck/123456-1111-2222-3333`

AWS::SQS::Queue

Una cola de Amazon SQS

- Formato de ARN: `arn:`*`partition`*`:sqs:`*`region`*`:`*`account`*`:`*`QueueName`*

  Ejemplo: `arn:aws:sqs:us-west-2:111122223333:StandardQueue`

  Para obtener más información, consulte Recursos y operaciones de Amazon Simple Queue Service.

AWS::SNS::Topic

Un tema de Amazon SNS.

- Formato de ARN: `arn:`*`partition`*`:sns:`*`region`*`:`*`account`*`:`*`TopicName`*

  Ejemplo: `arn:aws:sns:us-west-2:111122223333:TopicName`

  Para obtener más información, consulte Formato ARN de recurso de Amazon SNS.

AWS::SNS::Subscription

una suscripción a Amazon SNS.

- Formato de ARN: `arn:`*`partition`*`:sns:`*`region`*`:`*`account`*`:`*`TopicName`*`:`*`SubscriptionId`*

  Ejemplo: `arn:aws:sns:us-west-2:111122223333:TopicName:12345678901234567890`

AWS::EC2::VPC

Una nube virtual privada (VPC).

- Formato de ARN: `arn:`*`partition`*`:ec2:`*`region`*`:`*`account`*`:vpc/`*`VpcId`*

  Ejemplo: `arn:aws:ec2:us-west-2:111122223333:vpc/vpc-123456789`

  Para obtener más información, consulte Recursos de VPC.

AWS::EC2::VPNConnection

Una conexión de red privada virtual (VPN).

- Formato de ARN: `arn:`*`partition`*`:ec2:`*`region`*`:`*`account`*`:vpn-connection/`*`VpnConnectionId`*

Ejemplo: `arn:aws:ec2:us-west-2:111122223333:vpn-connection/vpn-123456789`

Para obtener más información, consulta Tipos de recursos definidos por Amazon EC2.

AWS::EC2::VPNGateway

Una puerta de enlace de red privada virtual (VPN).

- Formato de ARN: `arn:`*`partition`*`:ec2:`*`region`*`:`*`account`*`:vpn-gateway/`*`VpnGatewayId`*

  Ejemplo: `arn:aws:ec2:us-west-2:111122223333:vpn-gateway/vgw-123456789acbdefgh`

  Para obtener más información, consulta Tipos de recursos definidos por Amazon EC2.

AWS::Route53RecoveryReadiness::DNSTargetResource

Un recurso de destino de DNS para las comprobaciones de disponibilidad incluye el tipo de registro DNS, el nombre de dominio, el ARN de la zona hospedada de Route 53 y el ARN del ARN de Network Load Balancer o el ID del conjunto de registros de Route 53.

- Formato ARN para la zona alojada: `arn:`*`partition`*`:route53::`*`account`*`:hostedzone/`*`Id`*

  Ejemplo de una zona alojada: `arn:aws:route53::111122223333:hostedzone/abcHostedZone`

  NOTA: Debe incluir el ID de la cuenta en la zona alojada ARNs, tal y como se especifica aquí. El ID de cuenta es obligatorio para que ARC pueda sondear el recurso. El formato es intencionalmente diferente del formato ARN que requiere Amazon Route 53, que se describe en los tipos de recursos del servicio de Route 53 en la Referencia de autorización de servicio.

- Formato ARN para Network Load Balancer: `arn:`*`partition`*`:elasticloadbalancing:`*`region`*`:`*`account`*`:loadbalancer/net/`*`LoadBalancerName`*

  Ejemplo de Network Load Balancer: `arn:aws:elasticloadbalancing:us-west-2:111122223333:loadbalancer/net/sandbox-net/123456789acbdefgh`

  Para obtener más información, consulte Recursos Elastic Load Balancing.

Registro y supervisión para comprobar la disponibilidad en Amazon Application Recovery Controller (ARC)

Puede utilizar Amazon y Amazon CloudWatch EventBridge para supervisar la verificación de disponibilidad en Amazon Application Recovery Controller (ARC), a fin de analizar patrones y ayudar a solucionar problemas. AWS CloudTrail

> **Note**
>
> Debe ver CloudWatch las métricas y los registros de ARC en la región EE.UU. Oeste (Oregón), tanto en la consola como cuando utilice la AWS CLI. Cuando utilice la AWS CLI, especifique la región EE.UU. Oeste (Oregón) para su comando mediante la inclusión del siguiente parámetro:`--region us-west-2`.

Temas

- Uso de Amazon CloudWatch con verificación de disponibilidad en ARC
- Registrar las llamadas a la API de verificación de disponibilidad mediante AWS CloudTrail
- Uso de la verificación de disponibilidad en ARC con Amazon EventBridge

Uso de Amazon CloudWatch con verificación de disponibilidad en ARC

Amazon Application Recovery Controller (ARC) publica puntos de datos en Amazon CloudWatch para sus comprobaciones de disponibilidad. CloudWatch le permite recuperar estadísticas sobre esos puntos de datos como un conjunto ordenado de datos de series temporales, conocidos como métricas. Una métrica es una variable que hay que monitorizar y los puntos de datos son los valores de esa variable a lo largo del tiempo. Por ejemplo, puede supervisar el tráfico en una AWS región durante un período de tiempo específico. Cada punto de datos tiene una marca temporal asociada y una unidad de medida opcional.

Puede utilizar estas métricas para comprobar si el sistema funciona de acuerdo con lo esperado. Por ejemplo, puede crear una CloudWatch alarma para supervisar una métrica específica e iniciar una acción (como enviar una notificación a una dirección de correo electrónico) si la métrica se sale de lo que considera un rango aceptable.

Para obtener más información, consulta la Guía del CloudWatch usuario de Amazon.

Temas

- Métricas de ARC
- Estadísticas de las métricas de ARC
- Vea CloudWatch las métricas en ARC

Métricas de ARC

El espacio de nombres de `AWS/Route53RecoveryReadiness` incluye las siguientes métricas.

Métrica	Descripción
`ReadinessChecks`	Representa el número de comprobaciones de preparación procesadas por ARC. La métrica se puede dimensionar según sus estados, que se indican a continuación. Unidad: `Count`. Criterios del informe: hay un valor distinto de cero. Estadísticas: la única estadística útil es `Sum`. Dimensiones • `READY` • `NOT_READY` • `NOT_AUTHORIZED` • `UNKNOWN`
`Resources`	Representa la cantidad de recursos procesados por ARC, que se pueden dimensionar según su identificador de recursos, tal como lo define la API. Unidad: `Count`. Criterios del informe: hay un valor distinto de cero. Estadísticas: la única estadística útil es `Sum`.

Métrica	Descripción
	Dimensiones • `ResourceSetType` : Estos son los tipos de recursos, filtrados por la cantidad de recursos por tipo determinado evaluados por ARC Por ejemplo: `AWS::CloudWatch::Alarm` .

Estadísticas de las métricas de ARC

CloudWatch proporciona estadísticas basadas en los puntos de datos métricos publicados por ARC. Las estadísticas son agregaciones de los datos de las métricas correspondientes al periodo especificado. Cuando se solicitan estadísticas, el flujo de datos devuelto se identifica mediante el nombre de la métrica y su dimensión. Una dimensión es un par de nombre/valor que identifica una métrica de forma inequívoca.

Los siguientes son ejemplos de combinaciones de métricas y dimensiones que pueden resultarle útiles:

- Vea el número de comprobaciones de preparación evaluadas por ARC para determinar su estado de preparación.
- Vea la cantidad total de recursos para un tipo de conjunto de recursos determinado evaluado por ARC.

Vea CloudWatch las métricas en ARC

Puede ver las CloudWatch métricas de ARC mediante la CloudWatch consola o el AWS CLI. En la consola, estas métricas se muestran en gráficos de monitorización.

Debe ver CloudWatch las métricas de ARC en la región EE.UU. Oeste (Oregón), tanto en la consola como cuando utilice la AWS CLI. Cuando utilice la AWS CLI, especifique la región EE.UU. Oeste (Oregón) para su comando incluyendo el siguiente parámetro:`--region us-west-2`.

Para ver las métricas mediante la CloudWatch consola

1. Abra la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, seleccione Métricas.
3. Seleccione el espacio de nombres de Route53 RecoveryReadiness.

4. (Opcional) Para ver una métrica en todas las dimensiones, escriba su nombre en el campo de búsqueda.

Para ver las métricas mediante el AWS CLI

Utilice el siguiente comando list-metrics para obtener una lista de las métricas disponibles:

```
aws cloudwatch list-metrics --namespace AWS/Route53RecoveryReadiness --region us-west-2
```

Para obtener las estadísticas de una métrica mediante el AWS CLI

Use el siguiente get-metric-statisticscomando para obtener las estadísticas de una métrica y una dimensión especificadas. Tenga en cuenta que CloudWatch trata cada combinación única de dimensiones como una métrica independiente. No se pueden recuperar estadísticas utilizando combinaciones de dimensiones que no se han publicado expresamente. Debe especificar las mismas dimensiones que se utilizaron al crear las métricas.

El siguiente ejemplo muestra el total de comprobaciones de preparación evaluadas, por minuto, para una cuenta en 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
```

A continuación, se muestra un ejemplo de salida 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"
        }
    ]
}
```

Registrar las llamadas a la API de verificación de disponibilidad mediante AWS CloudTrail

está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en ARC. CloudTrail captura todas las llamadas a la API de ARC como eventos. Las llamadas capturadas incluyen llamadas desde la consola ARC y llamadas en código a las operaciones de la API ARC.

Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos de ARC. Si no configura una ruta, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos.

Con la información recopilada por CloudTrail, puede determinar la solicitud que se realizó a ARC, la dirección IP desde la que se realizó la solicitud, quién la hizo, cuándo se realizó y detalles adicionales.

Para obtener más información CloudTrail, consulte la Guía AWS CloudTrail del usuario.

Información sobre ARC en CloudTrail

CloudTrail está habilitada en tu cuenta Cuenta de AWS al crear la cuenta. Cuando se produce una actividad en ARC, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS

servicio en el historial de eventos. Puede ver, buscar y descargar eventos recientes en su Cuenta de AWS. Para obtener más información, consulte Trabajar con el historial de CloudTrail eventos.

Para tener un registro continuo de tus eventos Cuenta de AWS, incluidos los eventos de ARC, crea una ruta. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las Regiones de AWS. La ruta registra los eventos de todas las regiones de la AWS partición y envía los archivos de registro al bucket de Amazon S3 que especifique. Además, puede configurar otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para más información, consulte los siguientes temas:

- Introducción a la creación de registros de seguimiento
- CloudTrail servicios e integraciones compatibles
- Configuración de las notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de CloudTrail registro de varias regiones y recibir archivos de CloudTrail registro de varias cuentas

Todas las acciones de ARC se registran CloudTrail y documentan en la Guía de referencia de la API de preparación de recuperación para Amazon Application Recovery Controller, la Guía de referencia de la API de configuración de control de recuperación para Amazon Application Recovery Controller y la Guía de referencia de la API de control de enrutamiento para Amazon Application Recovery Controller. Por ejemplo, las llamadas a `UpdateRoutingControlState` y `CreateRecoveryGroup` las acciones generan entradas en los archivos de CloudTrail registro. `CreateCluster`

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con credenciales de usuario root o AWS Identity and Access Management (IAM).
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro AWS servicio.

Para obtener más información, consulte el elemento userIdentity de CloudTrail .

Visualización de los eventos ARC en el historial de eventos

CloudTrail le permite ver los eventos recientes en el historial de eventos. Para ver los eventos de las solicitudes de la API ARC, debe seleccionar EE.UU. Oeste (Oregón) en el selector de regiones situado en la parte superior de la consola. Para obtener más información, consulte Cómo trabajar con el historial de CloudTrail eventos en la Guía del AWS CloudTrail usuario.

Descripción de las entradas de los archivos de registro ARC

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

En el siguiente ejemplo, se muestra una entrada de CloudTrail registro que demuestra la `CreateRecoveryGroup` acción de comprobación de disponibilidad.

```
{
    "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"
}
```


Uso de la verificación de disponibilidad en ARC con Amazon EventBridge

Con Amazon EventBridge, puede configurar reglas basadas en eventos que supervisen sus recursos de comprobación de disponibilidad en Amazon Application Recovery Controller (ARC) y, a continuación, iniciar acciones específicas que utilicen otros AWS servicios. Por ejemplo, puedes establecer una regla para el envío de notificaciones por correo electrónico señalando un tema de Amazon SNS cuando el estado de una comprobación de disponibilidad cambie de LISTO a NO LISTO.

> **Note**
>
> ARC solo publica EventBridge eventos para comprobar la preparación en la región US West (Oregon) (AWS us-west-2). Para recibir EventBridge los eventos y comprobar si están listos, crea EventBridge reglas en la región EE.UU. Oeste (Oregón).

Puedes crear reglas en Amazon EventBridge para actuar en el siguiente evento de verificación de preparación para el ARC:

- Verificación de disponibilidad. El evento especifica si el estado de preparación del grupo de recuperación cambia, por ejemplo, de LISTO a NO LISTO.

Para capturar eventos de ARC específicos que le interesen, defina patrones específicos de eventos que EventBridge pueda utilizar para detectarlos. Los patrones de eventos de tienen la misma estructura que los eventos con los que coinciden. El patrón cita los campos para los que se desea encontrar coincidencias y proporciona los valores que está buscando.

Los eventos se emiten en la medida de lo posible. En circunstancias operativas normales, se envían desde ARC a prácticamente EventBridge en tiempo real. Sin embargo, pueden surgir situaciones que retrasen o impidan la entrega de un evento.

Para obtener información sobre cómo funcionan EventBridge las reglas con los patrones de eventos, consulte Eventos y patrones de eventos en EventBridge.

Supervise un recurso de verificación de preparación con EventBridge

Con él EventBridge, puede crear reglas que definan las acciones que se deben tomar cuando ARC emita eventos para los recursos de verificación de preparación.

Para escribir o copiar y pegar un patrón de eventos en la EventBridge consola, en la consola, seleccione la opción Introducir mi propia opción. Para ayudarle a determinar los patrones de eventos que podrían serle útiles, en este tema se incluyen ejemplos de patrones de eventos de preparación.

Para crear una regla para un evento de recurso, realice lo siguiente:

1. Abre la EventBridge consola de Amazon en https://console.aws.amazon.com/events/.
2. Región de AWS Para crear la regla, selecciona US West (Oregon). Esta es la región requerida para los eventos de preparación.

3. Seleccione Creación de regla.
4. Ingrese un Name (Nombre) para la regla y opcionalmente, una descripción.
5. Para Bus de eventos, deje el valor predeterminado, predeterminado.
6. Elija Next (Siguiente).
7. En el paso Crear un patrón de eventos, en Origen del evento, deje el valor predeterminado, Eventos de AWS .
8. En Ejemplo de evento, elija Introducir el mío.
9. Para Ejemplos de eventos, escriba o copie y pegue un patrón de eventos. Para ver ejemplos, consulte la siguiente sección.

Ejemplos de patrones de eventos de preparación

Los patrones de eventos tienen la misma estructura que los eventos con los que coinciden. El patrón cita los campos para los que se desea encontrar coincidencias y proporciona los valores que está buscando.

Puede copiar y pegar los patrones de eventos de esta sección EventBridge para crear reglas que pueda usar para monitorear las acciones y los recursos de ARC.

Los siguientes patrones de eventos proporcionan ejemplos que puede utilizar EventBridge para la función de comprobación de la preparación de ARC.

- Seleccione todos los eventos de la verificación de preparación de ARC.

```
{
    "source": [
        "aws.route53-recovery-readiness"
    ]
}
```

- Seleccione solo los eventos relacionados con las celdas.

```
{
    "source": [
        "aws.route53-recovery-readiness"
    ],
    "detail-type": [
        "Route 53 Application Recovery Controller cell readiness status change"
    ]
```

```
}
```

- Seleccione solo los eventos relacionados con una celda específica llamada *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"
    ]
}
```

- Seleccione solo los eventos en los que se encuentre el estado de algún grupo de recuperación, celda o comprobación de disponibilidad *NOT READY*.

```
{
   "source":[
      "aws.route53-recovery-readiness"
   ],
   "detail-type":{
      "new-state":{
         "readiness-status":[
            "NOT_READY"
         ]
      }
   }
}
```

- Seleccione solo eventos cuando cualquier grupo de recuperación, celda o verificación de disponibilidad se convierta en algo distinto *READY*

```
{
   "source":[
      "aws.route53-recovery-readiness"
   ],
   "detail":{
      "new-state":{
         "readiness-status":[
            {
```

```
                "anything-but":"READY"
            }
         ]
      }
   }
}
```

El siguiente es un ejemplo de un evento de ARC para un cambio en el estado de preparación de un grupo de recuperación:

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

El siguiente es un ejemplo de un evento ARC para un cambio de estado de preparación de una célula:

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

El siguiente es un ejemplo de un evento ARC para un cambio en el estado de una comprobación de disponibilidad:

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

Especifique un grupo de CloudWatch registros para usarlo como destino

Al crear una EventBridge regla, debe especificar el destino al que se envían los eventos que coinciden con la regla. Para obtener una lista de los objetivos disponibles EventBridge, consulte Objetivos disponibles en la EventBridge consola. Uno de los destinos que puedes añadir a una EventBridge regla es un grupo de CloudWatch registros de Amazon. En esta sección se describen los requisitos para añadir grupos de CloudWatch registros como objetivos y se proporciona un procedimiento para añadir un grupo de registros al crear una regla.

Para agregar un grupo de CloudWatch registros como destino, puede realizar una de las siguientes acciones:

- Cree un nuevo grupo de registros
- Elija un grupo de registros existente

Si especifica un nuevo grupo de registros mediante la consola al crear una regla, crea EventBridge automáticamente el grupo de registros. Asegúrese de que el grupo de registros que utilice como destino para la EventBridge regla comience por`/aws/events`. Si desea elegir un grupo de registros existente, tenga en cuenta que solo los grupos de registros que comiencen por `/aws/events` aparecen como opciones en el menú desplegable. Para obtener más información, consulta Crear un nuevo grupo de registros en la Guía del CloudWatch usuario de Amazon.

Si crea o usa un grupo de CloudWatch registros para usarlo como destino mediante CloudWatch operaciones fuera de la consola, asegúrese de configurar los permisos correctamente. Si usa la consola para agregar un grupo de registros a una EventBridge regla, la política basada en recursos del grupo de registros se actualiza automáticamente. Sin embargo, si usa el SDK AWS Command Line Interface o un AWS SDK para especificar un grupo de registros, debe actualizar la política basada en recursos para el grupo de registros. El siguiente ejemplo de política ilustra los permisos que debe definir en una política basada en recursos para el grupo de registros:

```
{
  "Statement": [
    {
      "Action": [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Effect": "Allow",
      "Principal": {
```

```
        "Service": [
          "events.amazonaws.com",
          "delivery.logs.amazonaws.com"
        ]
      },
      "Resource": "arn:aws:logs:region:account:log-group:/aws/events/*:*",
      "Sid": "TrustEventsToStoreLogEvent"
    }
  ],
  "Version": "2012-10-17"
}
```

No puede configurar una política basada en recursos para un grupo de registros mediante la consola. Para añadir los permisos necesarios a una política basada en recursos, utilice la operación de API. CloudWatch PutResourcePolicy A continuación, puede utilizar el comando describe-resource-policiesCLI para comprobar que la política se ha aplicado correctamente.

Para crear una regla para un evento de recurso y especificar un objetivo de grupo de CloudWatch registros

1. Abre la EventBridge consola de Amazon en https://console.aws.amazon.com/events/.
2. Elige en Región de AWS qué quieres crear la regla.
3. Seleccione Crear regla y, a continuación, introduzca cualquier información sobre esa regla, como el patrón de eventos o los detalles de la programación.

   Para obtener más información sobre la creación de EventBridge reglas de preparación, consulte Supervisar un recurso de verificación de preparación con EventBridge.
4. En la página Seleccione el destino, elija CloudWatchcomo objetivo.
5. Elija un grupo de CloudWatch registros en el menú desplegable.

Identity and Access Management para comprobar la disponibilidad en ARC

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a los AWS recursos. Los administradores de IAM controlan quién puede autenticarse (iniciar sesión) y quién puede autorizarse (tener permisos) para usar los recursos de ARC. La IAM es una Servicio de AWS opción que puede utilizar sin coste adicional.

Contenido

- Cómo funciona la verificación de disponibilidad en Amazon Application Recovery Controller (ARC) con IAM
- Ejemplos de políticas basadas en la identidad para comprobar la preparación en ARC
- Uso de un rol vinculado al servicio para comprobar la preparación en ARC
- AWS políticas gestionadas para comprobar la preparación en ARC

Cómo funciona la verificación de disponibilidad en Amazon Application Recovery Controller (ARC) con IAM

Antes de usar IAM para administrar el acceso a ARC, infórmese sobre las funciones de IAM disponibles para su uso con ARC.

Antes de utilizar IAM para gestionar el acceso a la comprobación de preparación en Amazon Application Recovery Controller (ARC), infórmese sobre las funciones de IAM disponibles para su uso con la comprobación de preparación.

Funciones de IAM que puede utilizar con la comprobación de disponibilidad en Amazon Application Recovery Controller (ARC)

Característica de IAM	Soporte de verificación de disponibilidad
Políticas basadas en identidades	Sí
Políticas basadas en recursos	No
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política	Sí
ACLs	No
ABAC (etiquetas en políticas)	Sí
Credenciales temporales	Sí
Permisos de entidades principales	Sí
Roles de servicio	No

Característica de IAM	Soporte de verificación de disponibilidad
Roles vinculados al servicio	Sí

Para obtener una visión general y de alto nivel del funcionamiento de AWS los servicios con la mayoría de las funciones de IAM, consulte AWS los servicios que funcionan con IAM en la Guía del usuario de IAM.

Políticas basadas en la identidad para comprobar la preparación

Compatibilidad con las políticas basadas en identidad: sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está asociada. Para obtener más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de las políticas de JSON de IAM en la Guía del usuario de IAM.

Para ver ejemplos de políticas ARC basadas en la identidad, consulte. Ejemplos de políticas basadas en identidad en Amazon Application Recovery Controller (ARC)

Políticas basadas en recursos incluidas en la verificación de disponibilidad

Admite políticas basadas en recursos: no

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico.

Acciones políticas para la verificación de la preparación

Compatibilidad con las acciones de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Las acciones políticas suelen tener el mismo nombre que la operación de AWS API asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de acciones de ARC para comprobar la disponibilidad, consulte Acciones definidas por Amazon Route 53 Recovery Readiness en la Referencia de autorización de servicio.

Las acciones políticas en ARC para comprobar la disponibilidad utilizan los siguientes prefijos antes de la acción:

```
route53-recovery-readiness
```

Para especificar varias acciones en una única instrucción, sepárelas con comas. Por ejemplo, los siguientes:

```
"Action": [
      "route53-recovery-readiness:action1",
      "route53-recovery-readiness:action2"
         ]
```

Puede utilizar caracteres comodín (*) para especificar varias acciones . Por ejemplo, para especificar todas las acciones que comiencen con la palabra `Describe`, incluya la siguiente acción:

```
"Action": "route53-recovery-readiness:Describe*"
```

Para ver ejemplos de políticas de ARC basadas en la identidad para comprobar la disponibilidad, consulte. Ejemplos de políticas basadas en la identidad para comprobar la preparación en ARC

Recursos de políticas para la verificación de la preparación

Compatibilidad con los recursos de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puedes realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puedes hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utiliza un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

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

Para ver una lista de acciones de ARC para el cambio zonal, consulte Acciones definidas por Amazon Route 53 Recovery Readiness.

Para ver ejemplos de políticas de ARC basadas en la identidad para la verificación de la preparación, consulte. Ejemplos de políticas basadas en la identidad para comprobar la preparación en ARC

Condiciones de la política: claves para la verificación de la disponibilidad

Compatibilidad con claves de condición de políticas específicas del servicio: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puedes realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puedes crear expresiones condicionales que utilizan operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación `AND` lógica. Si especifica varios valores para una única clave de condición, AWS evalúa la condición mediante una `OR` operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puedes utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puedes conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para más información, consulta Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

Para ver una lista de acciones de ARC para comprobar la preparación, consulte Claves de condición de Amazon Route 53 Recovery Readiness

Para ver las acciones y los recursos que puede utilizar con una clave de condición con verificación de disponibilidad, consulte Acciones definidas por Amazon Route 53 Recovery Readiness

Para ver ejemplos de políticas de ARC basadas en la identidad para la comprobación de la disponibilidad, consulte. Ejemplos de políticas basadas en la identidad para comprobar la preparación en ARC

Listas de control de acceso (ACLs) en fase de verificación de disponibilidad

Soportes ACLs: No

Las listas de control de acceso (ACLs) controlan qué directores (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLs son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Control de acceso basado en atributos (ABAC) con verificación de disponibilidad

Compatibilidad con ABAC (etiquetas en las políticas): parcial

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos. En AWS, estos atributos se denominan etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a muchos AWS recursos. El etiquetado de entidades y recursos es el primer paso de ABAC. A continuación, designa las políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso al que se intenta acceder.

ABAC es útil en entornos que crecen con rapidez y ayuda en situaciones en las que la administración de las políticas resulta engorrosa.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte Definición de permisos con la autorización de ABAC en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

Recovery Readiness (verificación de preparación) es compatible con ABAC.

Uso de credenciales temporales con verificación de preparación

Compatibilidad con credenciales temporales: sí

Algunas Servicios de AWS no funcionan cuando inicias sesión con credenciales temporales. Para obtener información adicional, incluida información sobre cuáles Servicios de AWS funcionan con credenciales temporales, consulta Cómo Servicios de AWS funcionan con IAM en la Guía del usuario de IAM.

Utiliza credenciales temporales si inicia sesión en ellas AWS Management Console mediante cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accedes AWS mediante el enlace de inicio de sesión único (SSO) de tu empresa, ese proceso crea automáticamente credenciales temporales. También crea credenciales temporales de forma automática cuando inicia sesión en la consola como usuario y luego cambia de rol. Para obtener más información sobre el cambio de roles, consulte Cambio de un usuario a un rol de IAM (consola) en la Guía del usuario de IAM.

Puedes crear credenciales temporales manualmente mediante la AWS CLI API o. AWS A continuación, puede utilizar esas credenciales temporales para acceder AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para obtener más información, consulte Credenciales de seguridad temporales en IAM.

Permisos principales entre servicios para comprobar si están listos

Admite sesiones de acceso directo (FAS): sí

Cuando utilizas una entidad de IAM (usuario o rol) para realizar acciones en ella AWS, se te considera principal. Las políticas conceden permisos a una entidad principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. En este caso, debe tener permisos para realizar ambas acciones.

Para ver si una acción en la verificación de disponibilidad requiere acciones dependientes adicionales en una política, consulte Amazon Route 53 Recovery Readiness

Funciones de servicio para comprobar la disponibilidad

Compatible con roles de servicio: No

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

Funciones vinculadas al servicio para comprobar la preparación

Admite roles vinculados a servicios: sí

Un rol vinculado al servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Para obtener más información sobre la creación o administración de funciones vinculadas al servicio de ARC, consulte. Uso de un rol vinculado al servicio para comprobar la preparación en ARC

Para más información sobre cómo crear o administrar roles vinculados a servicios, consulta Servicios de AWS que funcionan con IAM. Busque un servicio en la tabla que incluya `Yes` en la columna Rol vinculado a un servicio. Seleccione el vínculo Sí para ver la documentación acerca del rol vinculado a servicios para ese servicio.

Ejemplos de políticas basadas en la identidad para comprobar la preparación en ARC

De forma predeterminada, los usuarios y los roles no tienen permiso para crear o modificar los recursos de ARC. Tampoco pueden realizar tareas mediante la AWS Management Console, AWS Command Line Interface (AWS CLI) o la AWS API. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puedes añadir las políticas de IAM a roles y los usuarios puedes asumirlos.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM (consola) en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos por ARC, incluido el ARNs formato de cada uno de los tipos de recursos, consulte Acciones, recursos y claves de condición de Amazon Application Recovery Controller (ARC) en la Referencia de autorización de servicios.

Temas

- Prácticas recomendadas sobre las políticas
- Ejemplo: compruebe si está listo para acceder a la consola
- Ejemplos: acciones de la API de verificación de disponibilidad para comprobar la disponibilidad

Prácticas recomendadas sobre las políticas

Las políticas basadas en la identidad determinan si alguien puede crear, eliminar o acceder a los recursos de ARC de su cuenta. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulta las políticas administradas por AWS o las políticas administradas por AWS para funciones de tarea en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulta Políticas y permisos en IAM en la Guía del usuario de IAM.
- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo AWS CloudFormation. Para obtener más información, consulta Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.

- Utiliza el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Validación de políticas con el Analizador de acceso de IAM en la Guía del usuario de IAM.
- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para exigir la MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para más información, consulte Acceso seguro a la API con MFA en la Guía del usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Ejemplo: compruebe si está listo para acceder a la consola

Para acceder a la consola Amazon Application Recovery Controller (ARC), debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre los recursos ARC de su propiedad Cuenta de AWS. Si crea una política basada en identidades que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

No es necesario que concedas permisos mínimos de consola a los usuarios que solo realicen llamadas a la API AWS CLI o a la AWS API. En su lugar, permite el acceso únicamente a las acciones que coincidan con la operación de API que intentan realizar.

Para garantizar que los usuarios y los roles puedan seguir utilizando la consola de comprobación de disponibilidad cuando solo se permita el acceso a determinadas operaciones de la API, adjunte también a las entidades una política `ReadOnly` AWS gestionada de comprobación de disponibilidad. Para obtener más información, consulta la página de verificación de disponibilidad: comprobar la preparación de las políticas gestionadas o Añadir permisos a un usuario en la Guía del usuario de IAM.

Para realizar algunas tareas, los usuarios deben tener permiso para crear el rol vinculado al servicio que está asociado a la verificación de disponibilidad en ARC. Para obtener más información, consulte Uso de un rol vinculado al servicio para comprobar la preparación en ARC.

Para que los usuarios tengan acceso completo al uso de las funciones de verificación de disponibilidad a través de la consola, adjunte al usuario una política como la siguiente:

```
{
    "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": "*"
        }
    ]
}
```

Ejemplos: acciones de la API de verificación de disponibilidad para comprobar la disponibilidad

Para garantizar que un usuario pueda utilizar las acciones de la API de ARC para trabajar con el plano de control de la comprobación de disponibilidad de ARC (por ejemplo, para crear grupos de recuperación, conjuntos de recursos y comprobaciones de disponibilidad), adjunte una política que corresponda a las operaciones de la API con las que el usuario debe trabajar, tal y como se describe a continuación.

Para realizar algunas tareas, los usuarios deben tener permiso para crear el rol vinculado al servicio que está asociado a la verificación de disponibilidad en ARC. Para obtener más información, consulte Uso de un rol vinculado al servicio para comprobar la preparación en ARC.

Para trabajar con las operaciones de la API para comprobar la disponibilidad, adjunta al usuario una política como la siguiente:

```
{
    "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": "*"
        }
    ]
}
```

Uso de un rol vinculado al servicio para comprobar la preparación en ARC

Amazon Application Recovery Controller utiliza AWS Identity and Access Management funciones vinculadas a servicios (IAM). Un rol vinculado a un servicio es un tipo único de rol de IAM que está vinculado directamente a un servicio, en este caso, ARC. ARC predefine las funciones vinculadas al servicio e incluyen todos los permisos que el servicio requiere para llamar a otros AWS servicios en su nombre con fines específicos.

Los roles vinculados al servicio facilitan la configuración de ARC, ya que no es necesario añadir manualmente los permisos necesarios. ARC define los permisos de sus funciones vinculadas al servicio y, a menos que se defina lo contrario, solo ARC puede asumir sus funciones. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se pueda asociar a ninguna otra entidad de IAM.

Solo puede eliminar un rol vinculado a servicios después de eliminar sus recursos relacionados. Esto protege sus recursos de ARC porque no puede eliminar inadvertidamente el permiso de acceso a los recursos.

Para obtener información sobre otros servicios que admiten funciones vinculadas a servicios, consulte AWS Servicios que funcionan con IAM y busque los servicios que tengan la palabra Sí en la columna Función vinculada a servicios. Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado a servicios en cuestión.

ARC tiene las siguientes funciones vinculadas al servicio, que se describen en este capítulo:

- ARC utiliza la función vinculada al servicio denominada Route53 RecoveryReadinessServiceRolePolicy para acceder a los recursos y las configuraciones y comprobar su disponibilidad.
- ARC utiliza la función vinculada al servicio denominada así para las ejecuciones de práctica de cambio automático, para monitorear las CloudWatch alarmas de Amazon y los AWS Health Dashboard eventos de los clientes proporcionados por el cliente, y para iniciar las ejecuciones de práctica.

Permisos de rol vinculados al servicio para Route53 RecoveryReadinessServiceRolePolicy

ARC utiliza un rol vinculado a un servicio denominado Route53 RecoveryReadinessServiceRolePolicy para acceder a los recursos y las configuraciones y comprobar si están listos. En esta sección se describen los permisos del rol vinculado al servicio y la información sobre cómo crear, editar y eliminar el rol.

Permisos de rol vinculados al servicio para Route53 RecoveryReadinessServiceRolePolicy

Este rol vinculado al servicio utiliza la política administrada `Route53RecoveryReadinessServiceRolePolicy`.

El rol RecoveryReadinessServiceRolePolicy vinculado al servicio de Route53 confía en que el siguiente servicio asuma el rol:

- `route53-recovery-readiness.amazonaws.com`

Para ver los permisos de esta política, consulte Route53 RecoveryReadinessServiceRolePolicy en la Referencia de políticas administradas.AWS

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Creación del rol vinculado al servicio de Route53 para ARC RecoveryReadinessServiceRolePolicy

No es necesario crear manualmente el rol vinculado al servicio de Route53. RecoveryReadinessServiceRolePolicy Al crear la primera verificación de disponibilidad o autorización entre cuentas en la AWS Management Console, la o la AWS API AWS CLI, ARC crea automáticamente la función vinculada al servicio.

Si elimina este rol vinculado a servicios y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Al crear la primera verificación de disponibilidad o autorización entre cuentas, ARC vuelve a crear el rol vinculado al servicio para usted.

Edición del rol vinculado al servicio de Route53 para ARC RecoveryReadinessServiceRolePolicy

ARC no permite editar el rol vinculado al servicio de Route53. RecoveryReadinessServiceRolePolicy Después de crear un rol vinculado al servicio, no podrá cambiar el nombre del rol, ya que otras entidades podrían hacer referencia al rol. Sin embargo, puede editar la descripción del rol mediante IAM. Para obtener más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM.

Eliminar el rol vinculado al servicio de Route53 para ARC RecoveryReadinessServiceRolePolicy

Si ya no necesita usar una característica o servicio que requieran un rol vinculado a un servicio, le recomendamos que elimine dicho rol. Así no tendrá una entidad no utilizada que no se supervise ni mantenga de forma activa. Sin embargo, debe limpiar los recursos de su rol vinculado al servicio antes de eliminarlo manualmente.

Una vez que haya eliminado las comprobaciones de disponibilidad y las autorizaciones entre cuentas, podrá eliminar la función vinculada al servicio de Route53. RecoveryReadinessServiceRolePolicy Para obtener más información acerca de las comprobaciones de disponibilidad, consulte Verificación de disponibilidad en ARC. Para obtener más información sobre autorizaciones entre cuentas, consulte Crear autorizaciones multicuenta en ARC.

> **Note**
>
> Si el servicio ARC utiliza el rol al intentar eliminar los recursos, es posible que no se pueda eliminar el rol de servicio. En tal caso, espere unos minutos e intente eliminar de nuevo el rol.

Para eliminar manualmente el rol vinculado a servicios mediante IAM

Utilice la consola de IAM AWS CLI, la o la AWS API para eliminar la función vinculada al servicio de Route53RecoveryReadinessServiceRolePolicy. Para obtener más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

Actualizaciones de la función vinculada al servicio ARC para comprobar si está lista

Para ver las actualizaciones de las políticas AWS administradas para las funciones vinculadas al servicio de ARC, consulte la tabla de actualizaciones de políticas AWS administradas de ARC.

También puede suscribirse a las alertas RSS automáticas en la página del historial del documento ARC.

AWS políticas gestionadas para comprobar la preparación en ARC

Una política AWS administrada es una política independiente creada y administrada por AWS. AWS Las políticas administradas están diseñadas para proporcionar permisos para muchos casos de uso comunes, de modo que pueda empezar a asignar permisos a usuarios, grupos y funciones.

Ten en cuenta que es posible que las políticas AWS administradas no otorguen permisos con privilegios mínimos para tus casos de uso específicos, ya que están disponibles para que los usen todos los AWS clientes. Se recomienda definir políticas administradas por el cliente específicas para sus casos de uso a fin de reducir aún más los permisos.

No puedes cambiar los permisos definidos en AWS las políticas administradas. Si AWS actualiza los permisos definidos en una política AWS administrada, la actualización afecta a todas las identidades principales (usuarios, grupos y roles) a las que está asociada la política. AWS es más probable que actualice una política AWS administrada cuando Servicio de AWS se lance una nueva o cuando estén disponibles nuevas operaciones de API para los servicios existentes.

Para obtener más información, consulte Políticas administradas de AWS en la Guía del usuario de IAM.

AWS política gestionada: Route53 RecoveryReadinessServiceRolePolicy

No puede asociar `Route53RecoveryReadinessServiceRolePolicy` a sus entidades IAM. Esta política está asociada a un rol vinculado a un servicio que permite a Amazon Application Recovery Controller (ARC) acceder a los AWS servicios y recursos que ARC utiliza o administra. Para obtener más información, consulte Uso de un rol vinculado al servicio para comprobar la preparación en ARC.

AWS política gestionada: 53 AmazonRoute RecoveryReadinessFullAccess

Puede adjuntar `AmazonRoute53RecoveryReadinessFullAccess` a sus entidades de IAM. Esta política otorga acceso total a las acciones para trabajar con la preparación para la recuperación (verificación de la preparación) en ARC. Asocie esta política a usuarios IAM y otras entidades principales que necesiten un acceso completo a las acciones de disponibilidad de recuperación.

Para ver los permisos de esta política, consulte la sección AmazonRoute53 RecoveryReadinessFullAccess en la Referencia de políticas AWS gestionadas.

AWS política gestionada: AmazonRoute 53 RecoveryReadinessReadOnlyAccess

Puede adjuntar `AmazonRoute53RecoveryReadinessReadOnlyAccess` a sus entidades de IAM. Esta política otorga acceso de solo lectura a las acciones para trabajar con la preparación para la recuperación en ARC. Resulta útil para los usuarios que necesitan ver los estados de preparación y las configuraciones de los grupos de recuperación. Estos usuarios no pueden crear, actualizar ni eliminar recursos de disponibilidad.

Para ver los permisos de esta política, consulte la sección AmazonRoute53 RecoveryReadinessReadOnlyAccess en la Referencia de políticas AWS gestionadas.

Actualizaciones de las políticas AWS gestionadas para garantizar su adecuación

Para obtener más información sobre las actualizaciones de las políticas AWS gestionadas para comprobar su disponibilidad en ARC desde que este servicio comenzó a realizar el seguimiento de estos cambios, consulteActualizaciones de las políticas AWS gestionadas de Amazon Application Recovery Controller (ARC). Para recibir alertas automáticas sobre los cambios en esta página, suscríbase a la fuente RSS de la página del historial de documentos de ARC.

Cuotas para comprobar la disponibilidad

La comprobación de disponibilidad en Amazon Application Recovery Controller (ARC) está sujeta a las siguientes cuotas (anteriormente denominadas límites).

Entidad	Cuota
Número de grupos de recuperación por cuenta de	5
Número de celdas por cuenta	15
Número de celdas anidadas por celda	3
Número de celdas por grupo de recuperación	3
Número de recursos por celda	10
Número de recursos por grupo de recuperación	10
Número de recursos por conjunto de recursos	6

Entidad	Cuota
Número de conjuntos de recursos por cuenta	200
Número de comprobaciones de disponibilidad por cuenta	200
Número de autorizaciones de entre las cuentas	100

Conmutador de región en ARC

Puede utilizar el conmutador regional de ARC para organizar tareas de recuperación complejas y a gran escala para los recursos de sus aplicaciones en todas AWS las cuentas, a fin de garantizar la continuidad empresarial y reducir la sobrecarga operativa. El conmutador de región proporciona una solución centralizada y observable que puede realizar manualmente o automatizar mediante activadores de CloudWatch alarmas de Amazon. Si una Región de AWS falla, puede ejecutar los planes que haya creado utilizando el cambio de región para realizar una conmutación por error o cambiar sus recursos a otra región. Esto garantiza que su aplicación pueda seguir funcionando correctamente Región de AWS.

El conmutador regional se basa en el concepto de un plan, que usted diseña y configura para sus necesidades de recuperación específicas. Cada plan incluye flujos de trabajo que se componen de pasos. Un paso ejecuta uno o más bloques de ejecución, cuyo conmutador de región se ejecuta en paralelo o en secuencia, para completar la recuperación de una aplicación. Cada bloque de ejecución gestiona una tarea diferente, como la conmutación de recursos o la gestión del redireccionamiento del tráfico de la aplicación. Para obtener aún más flexibilidad, puede crear planes anidados, añadiendo planes secundarios a un plan general para padres.

El cambio de región incluye lo siguiente:

- Support for active/passive and active/active configuration. Puede realizar la conmutación por error y la conmutación por recuperación si tiene una configuración active/passive multirregional, o cambiar y volver si la aplicación está configurada como en varias regiones. active/active
- Soporte multicuenta para los recursos de la aplicación que incluya en la recuperación de la aplicación. También puede compartir los planes de cambio de región entre cuentas.

- Conmutación o conmutación por error automática, mediante la activación de la ejecución del plan en función de las alarmas de Amazon. CloudWatch O bien, puede optar por ejecutar un plan de cambio de región manualmente.
- Paneles de control con todas las funciones que le brindan visibilidad en tiempo real del proceso de recuperación.
- Un plano de datos en cada uno Región de AWS, para que puedas ejecutar tu plan de cambio de región sin depender de la región que vayas a desactivar.

El cambio de región lo gestiona en su totalidad. AWS El uso de Region Switch le permite beneficiarse de la resiliencia de una plataforma de recuperación que se centra en los requisitos específicos de su aplicación, en lugar de crear y mantener scripts y recopilar manualmente los datos sobre las recuperaciones.

Acerca de Region Switch

Con el cambio de región, puede organizar los pasos específicos para cambiar el lugar en el Región de AWS que se ejecuta su aplicación multirregional.

El cambio de región se basa en el concepto de un plan, que usted diseña y configura para sus necesidades de recuperación específicas. Cada plan incluye flujos de trabajo que se componen de pasos. Un paso ejecuta uno o más bloques de ejecución, cuyo conmutador de región se ejecuta en paralelo o en secuencia, para completar la recuperación de una aplicación. Cada bloque de ejecución gestiona una tarea diferente, como la conmutación de recursos o la gestión del redireccionamiento del tráfico de la aplicación. Para una flexibilidad aún mayor, puede crear planes anidados añadiendo planes secundarios.

Cada vez que crea o actualiza un plan, Region Switch realiza una evaluación del plan para garantizar que no haya problemas con los permisos de IAM, la configuración de los recursos o la capacidad de ejecución. Region Switch realiza estas evaluaciones con regularidad y genera una advertencia ante cualquier problema que detecte.

Region Switch también calcula un valor de tiempo de recuperación real para cada ejecución del plan, a fin de ayudarle a evaluar si el plan cumple sus objetivos. Puede ver el tiempo de recuperación y otros detalles sobre la ejecución del plan en los paneles de control de los cambios de región del AWS Management Console. Para obtener más información, consulte Paneles de control para cambiar de región.

Para obtener más información sobre cada una de estas áreas del cambio de región, consulte las siguientes secciones.

Planes de cambio de región

Un plan de cambio de región es el recurso de nivel superior del cambio de región. Debe adaptar su plan a una aplicación multirregional específica. Un plan le permite crear flujos de trabajo para recuperar sus aplicaciones mediante la ejecución de una serie de bloques de ejecución que cambian de región para activar o desactivar la aplicación y sus recursos, incluidos los recursos multicuenta, en la forma Región de AWS que usted especifique.

Un plan se compone de uno o más flujos de trabajo que permiten activar o desactivar uno específico. Región de AWS Puede configurar los bloques de ejecución de un flujo de trabajo para que se ejecuten secuencialmente o puede especificar que algunos de los bloques se ejecuten en paralelo.

En el caso de un plan que configure para un enfoque active/passive multirregional, debe crear un flujo de trabajo que pueda usarse para activar cualquiera de sus regiones o dos flujos de trabajo de activación independientes, uno para cada región. En el caso de un plan que configure para un enfoque activo/activo, debe crear un flujo de trabajo para activar sus regiones y otro para desactivarlas.

Regiones de AWS son ubicaciones geográficas de todo el mundo donde se AWS agrupan los centros de datos. Cada región está diseñada para estar completamente aislada de las demás regiones, lo que proporciona estabilidad y tolerancia a los errores. Al utilizar el cambio de región, debe tener en cuenta en qué regiones está desplegada su aplicación y qué regiones desea utilizar para la recuperación.

El cambio de región permite la recuperación entre dos de las dos Regiones de AWS regiones en las que el servicio esté disponible. Al configurar un plan de cambio de región, debe especificar las regiones en las que está implementada la aplicación y el enfoque de recuperación que desea utilizar: active/passive o activo/activo.

Por ejemplo, puede tener un enfoque active/passive multirregional con us-east-1 como región principal y us-west-2 como región de reserva. Para recuperar su aplicación de un problema operativo que afecte a la aplicación en us-east-1, puede ejecutar su plan de cambio de región para activar la us-west-2. Esto daría como resultado que la aplicación cambiara de recursos en us-east-1 a recursos en us-west-2.

Los planes de cambio de región se ejecutan con los permisos asociados a la función de IAM que especificas al crear el plan.

Puede crear varios planes, uno para cada una de sus aplicaciones multirregionales, y, a continuación, organizar la recuperación de todos estos planes en el orden que desee mediante la creación de un plan principal. Un plan principal es un plan que utiliza los bloques de ejecución del plan de cambio de región como pasos. La jerarquía de planes está limitada a dos niveles (padre e hijo), pero puede incluir varios planes secundarios en el mismo plan principal.

Flujos de trabajo y bloques de ejecución

Después de crear un plan de cambio de región, debe agregar uno o más flujos de trabajo al plan para definir los pasos que desea que lleve a cabo el plan para la recuperación de la aplicación. Para cada flujo de trabajo, agrega bloques de ejecución para completar tareas específicas, como ampliar los recursos o actualizar los controles de enrutamiento para redirigir el tráfico. Los bloques de ejecución te permiten especificar estas tareas y el orden en que se completan. Al crear planes anidados, también puedes organizar el orden en el que varias aplicaciones se recuperan en la región que estás activando.

Puede añadir bloques de ejecución en un flujo de trabajo de forma secuencial o puede añadir uno o más bloques de ejecución en paralelo. Además, según el recurso, puede tener la opción de ejecutar un bloque de ejecución con una ejecución correcta (planificada) o mala (no planificada).

- Ejecución correcta: flujo de trabajo de ejecución planificada. Cuando su entorno esté en buen estado, podrá utilizar el eficiente flujo de trabajo para ejecutar todos los pasos y ejecutar el plan de forma ordenada.
- Ejecución desordenada: una ejecución no planificada. El lamentable modo de flujo de trabajo utiliza solo los pasos y acciones necesarios. Este modo cambia el comportamiento de los bloques de ejecución en un flujo de trabajo u omite bloques de ejecución específicos.

Por último, también puede configurar recursos multicuenta para un bloque de ejecución. En primer lugar, debe configurar los permisos siguiendo las instrucciones deSoporte multicuenta en el cambio de región. Una vez configuradas las funciones de IAM requeridas, puede añadir recursos entre cuentas a los bloques de ejecución de los flujos de trabajo de su plan. Para añadir recursos multicuenta, al añadir un bloque de ejecución, debe especificar un rol de IAM objetivo que tenga permisos para el recurso de otro. Cuentas de AWS También debes especificar el identificador externo que proporcionaste en la política de confianza para el rol multicuenta. Para obtener más información sobre la creación de las funciones de IAM necesarias, consulte. Acceso a recursos entre cuentas

Para obtener más información sobre los flujos de trabajo, consulteCree flujos de trabajo de planes de cambio de región. Para obtener información detallada sobre cada tipo de bloque de ejecución, incluidos los pasos de configuración, su funcionamiento y qué se evalúa como parte de la evaluación del plan, consulteAñada bloques de ejecución.

Evaluación del plan

La evaluación del plan es un proceso automatizado que Region Switch ejecuta cuando se crea o actualiza un plan y, posteriormente, cada 30 minutos, durante el estado estable. El proceso de evaluación verifica varios aspectos críticos de la configuración del plan y de los recursos. Las evaluaciones incluyen la verificación de los permisos de IAM, las configuraciones de los recursos y la capacidad de ejecución.

Si el conmutador de región detecta un problema que podría impedir la correcta ejecución del plan, generará una advertencia de evaluación del plan, que aparecerá resaltada en la página de detalles del plan de la consola. También puedes consumir las advertencias de evaluación del plan con Amazon EventBridge, o puedes ver las advertencias mediante la API de cambio de región.

Puedes ver los detalles y las soluciones sugeridas para los problemas que surjan en la evaluación del plan en la pestaña Evaluación del plan, en la página de detalles del plan. Le recomendamos que también pruebe la recuperación de las aplicaciones ejecutando su plan de cambio de región y que no se base únicamente en la evaluación del plan de cambio de región para comprobar que su plan de recuperación funcionará como espera.

Alarmas regionales y tiempo de recuperación real

El conmutador de región calcula un valor de tiempo de recuperación real para cada ejecución del plan, que puede consultar después de la ejecución del plan. El tiempo de recuperación real se muestra en la página de detalles de ejecución del plan, de modo que puede compararlo con el objetivo de tiempo de recuperación que especificó al crear el plan.

El tiempo de recuperación real se calcula como el tiempo total que tarda en completarse la ejecución de un plan y cualquier tiempo adicional que transcurra antes de que las CloudWatch alarmas de Amazon específicas que configure vuelvan a un estado verde.

Para poder calcular un tiempo de recuperación real y preciso para la ejecución del plan, añada CloudWatch alarmas regionales de Amazon a un plan de cambio de región que proporcionen una señal sobre el estado de su aplicación en cada región. Cuando se ejecuta un plan, Region Switch utiliza estas alarmas de estado de la aplicación para determinar cuándo la aplicación vuelve a estar

en buen estado. A continuación, Region Switch calcula el tiempo de recuperación real en función del tiempo que tarda el plan en ejecutarse, sumado al tiempo que tarda la aplicación en volver a funcionar correctamente, en función de las alarmas de estado de la aplicación que especifique.

Regiones de AWS

El cambio de región está disponible en todos los modelos comerciales Regiones de AWS.

Para obtener información detallada sobre el soporte regional y los puntos de enlace de servicio para Amazon Application Recovery Controller (ARC), consulte los puntos de enlace y las cuotas de Amazon Application Recovery Controller (ARC) en la Referencia general de Amazon Web Services.

Componentes del cambio de región

Los siguientes son los componentes y conceptos de la función de cambio de región de Amazon Application Recovery Controller (ARC).

Plan

Un plan es el proceso de recuperación fundamental de su aplicación. Para crear un plan, debe crear uno o más flujos de trabajo con bloques de ejecución que se ejecutarán en secuencia o en paralelo. A continuación, cuando se produce una avería regional, se ejecuta el plan para completar la recuperación de la aplicación cambiando la aplicación para que se ejecute en una región en buen estado.

Plan para niños

Un plan secundario es un plan autónomo que se puede ejecutar desde un plan principal para coordinar escenarios de recuperación de aplicaciones más complejos. Puedes anidar los planes de cambio de región en un nivel.

Flujo de trabajo

Un plan de cambio de región incluye uno o más flujos de trabajo. Un flujo de trabajo se compone de bloques de ejecución que usted especifica para que se ejecuten en paralelo o en secuencia, que completan la activación o desactivación de una región como parte de un plan de recuperación. En el caso de un plan que configure con un active/passive enfoque, debe crear un flujo de trabajo que pueda usarse para activar cualquiera de sus regiones o flujos de trabajo de activación independientes, uno para cada región. En el caso de un plan que configure para un active/active enfoque, debe crear un flujo de trabajo para activar sus regiones y un flujo de trabajo para desactivarlas.

Bloque de ejecución

Agrega bloques de ejecución de cambios de región a los flujos de trabajo del plan de cambio de región. Los bloques de ejecución le permiten especificar la recuperación de varias aplicaciones o recursos en una región que se active. Al añadir un bloque de ejecución a un flujo de trabajo, puede añadirlo en secuencia con otros bloques o en paralelo con uno o varios bloques más.

Configuraciones elegantes y desgraciadas

Puede optar por ejecutar bloques de ejecución específicos con una ejecución correcta (planificada) o mala (no planificada). Cuando su entorno esté en buen estado, podrá utilizar el eficiente flujo de trabajo para ejecutar todos los pasos y ejecutar el plan de forma ordenada. El desordenado modo de flujo de trabajo utiliza solo los pasos y acciones necesarios. Cuando ejecutas un plan en modo irregular, cambia el comportamiento de los bloques de ejecución en un flujo de trabajo u omite bloques de ejecución específicos, según el tipo de bloque de ejecución.

Los tipos específicos de bloques de ejecución tienen un comportamiento diferente cuando se ejecutan de forma irregular. Los detalles sobre estas diferencias se describen en la sección que incluye detalles sobre cada tipo de bloque de ejecución. Para obtener más información, consulte Añada bloques de ejecución.

Configuraciones de Active/active and active/passive

Existen dos enfoques principales para crear una configuración flexible para una aplicación en varias regiones: active/passive activa/activa. El conmutador de región admite la recuperación de aplicaciones para ambos enfoques.

Con una active/passive configuración, se implementan dos réplicas de la aplicación en dos regiones diferentes, y el tráfico de clientes solo se dirige a una región.

Con una active/active configuración, se implementan dos réplicas en dos regiones diferentes, pero ambas réplicas procesan el trabajo o reciben tráfico.

Planifique la ejecución

Cuando se ejecuta un plan de cambio de región, se implementa la recuperación de una aplicación cuando una región se ve afectada, activando una región en buen estado para la aplicación y el tráfico que recibe. Con una active/active configuración, también ejecutas un plan para desactivar la región afectada.

Alarmas de estado de la aplicación

Las alarmas de estado de las aplicaciones son CloudWatch alarmas que se especifican en un plan para indicar el estado de la aplicación en cada región. El conmutador de región utiliza las alarmas de estado de las aplicaciones para ayudar a determinar el tiempo de recuperación real después de cambiar de región para implementar la recuperación.

Desencadenadores

Puede utilizar los activadores del cambio de región para automatizar la recuperación de las aplicaciones. Cuando creas un disparador, especificas una o más CloudWatch alarmas de Amazon que indican el estado de tu aplicación. Cuando las alarmas pasan a un estado de alarma, Region Switch ejecuta automáticamente el plan de recuperación correspondiente.

Paneles

El conmutador de región incluye paneles de control en los que puede realizar un seguimiento de los detalles sobre la ejecución del plan en tiempo real.

Planos de datos y control para el cambio de región

Al planificar la conmutación por error y la recuperación ante desastres, tenga en cuenta la resistencia de sus mecanismos de conmutación por error. Le recomendamos que se asegure de que los mecanismos de los que depende durante la conmutación por error estén altamente disponibles, de modo que pueda utilizarlos cuando los necesite en caso de desastre. Por lo general, debe utilizar funciones de plano de datos para sus mecanismos siempre que pueda, a fin de obtener la máxima fiabilidad y tolerancia a los fallos. Teniendo esto en cuenta, es importante entender cómo se divide la funcionalidad de un servicio entre planos de control y planos de datos, y cuándo se puede confiar en una fiabilidad extrema con el plano de datos de un servicio.

Como ocurre con muchos AWS servicios, la funcionalidad de la capacidad del conmutador regional está respaldada por un plano de control y planos de datos. Si bien ambos tipos están diseñados para ser fiables, un plano de control está optimizado para garantizar la coherencia de los datos, mientras que un plano de datos está optimizado para garantizar la disponibilidad. Un plano de datos está diseñado para ser resistente, de modo que puede mantener la disponibilidad incluso durante eventos disruptivos, cuando un plano de control podría no estar disponible.

En general, un plano de control permite realizar funciones de administración básicas, como crear, actualizar y eliminar recursos del servicio. Un plano de datos proporciona la funcionalidad principal de un servicio. Por ello, le recomendamos que utilice las operaciones del plano de datos cuando la

disponibilidad sea importante, por ejemplo, cuando necesite obtener información sobre un plan de cambio de región durante una interrupción.

En el caso del cambio de región, los planos de control y los planos de datos se dividen de la siguiente manera:

- El plano de control del conmutador de región está ubicado en la región EE. UU. Este (Virginia del Norte) (us-east-1) y está diseñado para usarse únicamente para la administración de servicios, es decir, para crear y actualizar planes, no para la recuperación, es decir, para ejecutar planes. Las operaciones de la API del plano de control de la configuración del conmutador regional no están muy disponibles.
- El conmutador de región tiene planos de datos independientes en cada uno Región de AWS. Debe utilizar el plano de datos para las acciones de recuperación, es decir, para ejecutar los planes de cambio de región. Para obtener una lista de las operaciones del plan de datos, consulte Operaciones de la API de cambio de región. Estas operaciones del plano de datos del cambio de región están muy disponibles.

El conmutador de región proporciona una consola independiente en cada una de ellas Región de AWS, que invoca las operaciones de la API del plano de datos para las tareas de recuperación, de modo que puede utilizar la consola de la región que está activando para ejecutar planes de recuperación de aplicaciones. Para obtener más información sobre las consideraciones clave a la hora de preparar y completar una operación de recuperación con el conmutador de región, consulteMejores prácticas para el cambio de región en ARC.

Para obtener más información sobre los planos de datos, los planos de control y cómo AWS se crean servicios para cumplir los objetivos de alta disponibilidad, consulte el artículo Static stability using Availability Zones en Amazon Builders' Library.

Etiquetado para el conmutador de región ARC;

Las etiquetas son palabras o frases (metadatos) que se utilizan para identificar y organizar AWS los recursos. Puede añadir varias etiquetas a cada recurso, y cada etiqueta incluye una clave y un valor que usted define. Por ejemplo, la clave puede ser el entorno y el valor puede ser la producción. Puede buscar y filtrar sus recursos en función de las etiquetas que añada.

Puede etiquetar el siguiente recurso en el cambio de región de ARC:

- Planes

El etiquetado en ARC solo está disponible a través de la API, por ejemplo, mediante el AWS CLI.

Los siguientes son ejemplos de etiquetado en un conmutador de región mediante el. AWS CLI

```
aws arc-region-switch --region us-east-1 create-plan --plan-name example-plan --tags Region=IAD,Stage=Prod
```

Para obtener más información, consulte la Guía TagResourcede referencia de la API de cambio de región para Amazon Application Recovery Controller (ARC).

Precios

Usted paga un coste mensual fijo por cada plan de cambio de región que configure.

Para obtener información detallada sobre los precios de ARC y ejemplos de precios, consulte los precios de ARC.

Mejores prácticas para el cambio de región en ARC

Recomendamos las siguientes prácticas recomendadas para la preparación de la recuperación y la conmutación por error con el cambio de región en Amazon Application Recovery Controller (ARC).

Temas

- Mantenga seguras y siempre accesibles las AWS credenciales diseñadas específicamente y de larga duración
- Elija valores TTL más bajos para los registros de DNS involucrados en la conmutación por error
- Reserve la capacidad necesaria para las aplicaciones críticas
- Utilice las operaciones de la API del plano de datos, extremadamente fiables, para enumerar y obtener información sobre los planes de cambio de región
- Pruebe la conmutación por error con ARC

Mantenga seguras y siempre accesibles las AWS credenciales diseñadas específicamente y de larga duración

> En un escenario de recuperación ante desastres (DR), reduzca al mínimo las dependencias del sistema mediante un enfoque sencillo para acceder a las tareas de recuperación AWS y realizarlas. Cree credenciales de IAM de larga duración específicas para las tareas de DR y

guárdelas de forma segura en una caja fuerte física en las instalaciones o en un almacén virtual para acceder a ellas cuando sea necesario. Con IAM, puede gestionar de forma centralizada las credenciales de seguridad, como las claves de acceso y los permisos de acceso a AWS los recursos. En el caso de tareas no relacionadas con DR, le recomendamos que siga utilizando el acceso federado mediante los servicios de AWS , como, por ejemplo, AWS Single Sign-On.

Elija valores TTL más bajos para los registros de DNS involucrados en la conmutación por error

En el caso de los registros de DNS que pueda necesitar cambiar como parte del mecanismo de conmutación por error, especialmente los registros cuyo estado se haya comprobado, se recomienda utilizar valores de TTL más bajos. Configurar un TTL de 60 o 120 segundos es una opción común para esta situación.

La configuración TTL (tiempo de vida) de DNS indica a los solucionadores de DNS cuánto tiempo deben almacenar en caché un registro antes de solicitar uno nuevo. Cuando selecciona un TTL, inicia un compromiso entre latencia y fiabilidad y la capacidad de respuesta a los cambios. Con TTL más cortos en un registro, los solucionadores de DNS detectan las actualizaciones del registro más rápido, ya que deben realizar consultas con más frecuencia.

Para obtener más información, consulte Elija valores de TTL para los registros de DNS en Prácticas recomendadas para registros de DNS de Amazon Route 53.

Reserve la capacidad necesaria para las aplicaciones críticas

El conmutador regional incluye tipos de bloques de ejecución que ayudan a escalar los recursos informáticos como parte de la recuperación. Si utiliza estos bloques de ejecución en un plan, el cambio de región no garantiza que se alcance la capacidad informática deseada. Si tiene una aplicación esencial y necesita garantizar el acceso a la capacidad, le recomendamos que reserve la capacidad.

Existen estrategias que puede seguir para reservar la capacidad de cómputo en una región secundaria y, al mismo tiempo, limitar los costos. Para obtener más información, consulte Pilot light con capacidad reservada: Cómo optimizar los costes de recuperación ante desastres mediante reservas de capacidad bajo demanda.

Utilice las operaciones de la API del plano de datos, extremadamente fiables, para enumerar y obtener información sobre los planes de cambio de región

Utilice las operaciones de la API del plano de datos para trabajar con su plan de cambio de región y ejecutarlo durante un evento. Para obtener una lista de las operaciones del plano de datos del cambio de región, consulte Operaciones de la API de cambio de región.

La consola de conmutación de región de cada región utiliza las operaciones del plano de datos para ejecutar los planes de conmutación de región. También puede llamar a las operaciones de la API del plano de datos utilizando AWS CLI o ejecutando el código que escriba con uno de los AWS SDKs. ARC ofrece una fiabilidad extrema con la API en el plano de datos.

Pruebe la recuperación de aplicaciones con ARC

Pruebe la recuperación de las aplicaciones con regularidad con un conmutador de región ARC, para activar una pila de aplicaciones secundaria en otra Región de AWS, o para cambiar a una configuración activa-activa ejecutando un plan de cambio de región para desactivar una de las regiones.

Es importante que te asegures de que los planes de cambio de región que has creado estén alineados con los recursos correctos de tu pila y de que todo funcione como esperabas. Debe probarlo después de configurar el conmutador de región para su entorno y continuar realizando pruebas periódicamente para comprobar que los procesos de recuperación funcionan correctamente. Realice estas pruebas con regularidad, antes de que se produzca una situación de error, para evitar el tiempo de inactividad de sus usuarios.

Tutorial: Cree un plan de cambio de active/passive región

Este tutorial le guiará a través de la creación de un plan de cambio de active/passive región para una aplicación que se ejecute en la us-east-1 y se recupere en la us-west-2. El ejemplo incluye EC2 instancias de Amazon para computación, Amazon Aurora Global Database para almacenamiento y Amazon Route 53 para DNS.

En este tutorial, completará los siguientes pasos:

- Cree un plan de cambio de región
- Cree los flujos de trabajo y los bloques de ejecución del plan
- Cree un bloque de ejecución grupal de EC2 Auto Scaling
- Cree dos bloques de ejecución de aprobación manual
- Cree dos bloques de ejecución de Lambda de acciones personalizadas
- Cree un bloque de ejecución de Amazon Aurora Global Database
- Cree un bloque de control de enrutamiento ARC
- Ejecute el plan de conmutación regional

Requisitos previos

Antes de comenzar este tutorial, compruebe que cumple los siguientes requisitos previos en ambas regiones:

- Funciones de IAM con los permisos adecuados
- EC2 Grupos de Auto Scaling
- Funciones Lambda para la página de mantenimiento y el vallado
- Base de datos global de Aurora
- Controles de enrutamiento ARC

Paso 1: Crear el plan de cambio regional

1. En la consola de cambio de región, elija Crear un plan de cambio de región.
2. Proporcione los siguientes detalles:
   - Región principal: elija us-east-1
   - Región de espera: elija us-west-2
   - Objetivo de tiempo de recuperación (RTO) deseado (opcional)
   - Función de IAM: introduzca la función de IAM de ejecución del plan. Esta función de IAM permite a Region Switch llamar a los AWS servicios durante la ejecución.
3. Seleccione Crear.

(Opcional) Añada recursos de diferentes AWS cuentas a su plan de cambio de región:

1. Cree el rol multicuenta:
   - En la cuenta que aloja el recurso, cree un rol de IAM.
   - Agregue permisos para los recursos específicos a los que accederá el plan.
   - Agregue una política de confianza que permita que el rol de ejecución asuma el nuevo rol.
   - Introduce y anota un identificador externo que utilizarás como secreto compartido.
2. Configura el recurso en tu plan:
   - Cuando añada el recurso a su plan, especifique dos campos adicionales:
     - crossAccountRole: El ARN del rol que creó en el paso 1
     - ExternalID: el ID externo que ingresó en el paso 1

Ejemplo de configuración para un bloque de ejecución de EC2 Auto Scaling que accede a los recursos de la cuenta 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"
}
```

Permisos necesarios:

- La función de ejecución debe tener el AssumeRole permiso sts: para la función multicuenta.
- El rol multicuenta debe tener permisos solo para los recursos específicos a los que se accede.
- La política de confianza del rol multicuenta debe incluir:
  - La cuenta del rol de ejecución como entidad de confianza.
  - La condición de identificación externa.

Antes de ejecutar el plan, el conmutador de región verificará lo siguiente:

- La función de ejecución puede asumir la función multicuenta.
- El rol multicuenta tiene los permisos necesarios.
- El ID externo coincide con la política de confianza.

Paso 2: Cree los flujos de trabajo y los bloques de ejecución del plan

1. En la página de detalles del plan de cambio de región, selecciona Crear flujos de trabajo.
2. Seleccione Crear el mismo flujo de trabajo de activación para todas las regiones.
3. Introduzca una descripción del flujo de trabajo de activación de una región (opcional). Esto se utilizará para identificar fácilmente el flujo de trabajo al ejecutar el plan.
4. Elija Guardar y continuar.
5. Elija Añadir un paso y, a continuación, seleccione Ejecutar en secuencia.

6. Seleccione el bloque de ejecución de EC2 Auto Scaling y, a continuación, elija Añadir y editar. Este bloque te permitirá empezar a aumentar la capacidad en la región pasiva.
7. En el panel derecho, configura el bloque:
   - Nombre del paso: Introduzca «Escala»
   - Descripción del paso (opcional)
   - ARN del grupo Auto Scaling para us-east-1: El ARN de su ASG en us-east-1
   - ARN del grupo Auto Scaling para us-west-2: El ARN de su ASG en us-west-2
   - Porcentaje que coincide con la capacidad de la región de origen: introduzca 100
   - Método de supervisión de la capacidad: déjelo como «Más reciente»
   - Tiempo de espera (opcional)
8. Selecciona Guardar paso.
9. Selecciona Añadir un paso.
10. Seleccione el bloque de ejecución de la aprobación manual y agréguelo a la ventana de diseño. Este bloque permite la verificación humana antes de continuar.
11. En el panel derecho, configura el bloque:
    - Nombre del paso: Introduzca «Aprobación manual antes de la configuración»
    - Descripción del paso (opcional)
    - Función de aprobación de IAM: la función que debe asumir un usuario para aprobar la ejecución
    - Tiempo de espera (opcional). Cuando se agote el tiempo de espera, la ejecución se detiene y puedes volver a intentarlo, omitirlo o cancelarlo.
12. Selecciona Guardar paso.
13. Selecciona Añadir un paso.
14. Seleccione el bloque de ejecución Lambda de acción personalizada y, a continuación, elija Agregar y editar. Este bloque publica una página de mantenimiento en la región que se está activando.
15. En el panel derecho, configura el bloque:
    - Nombre del paso: ingrese «Mostrar página de mantenimiento»
    - Descripción del paso (opcional)

- ARN lambda para activar us-east-1: el ARN de la página de mantenimiento La función Lambda implementada en us-east-1
- ARN lambda para activar us-west-2: el ARN de la página de mantenimiento La función Lambda implementada en us-west-2
- Región para ejecutar la función Lambda: elija Ejecutar en la región de activación
- Tiempo de espera (opcional)
- Intervalo de reintento (opcional)

16. Selecciona Guardar paso.
17. Selecciona Añadir un paso.
18. Seleccione un segundo bloque de ejecución de Lambda de acción personalizada y, a continuación, elija Agregar y editar. Este bloque activa un mecanismo de bloqueo en la región activa que garantiza que la región que se está desactivando ya no pueda aceptar tráfico.
19. En el panel derecho, configura el bloque:

    - Nombre del paso: Introduzca «Esgrima»
    - Descripción del paso (opcional)
    - ARN lambda para activar us-east-1: el ARN de la función Lambda de esgrima implementada en us-east-1
    - ARN lambda para activar us-west-2: el ARN de la función Lambda de esgrima implementada en us-west-2
    - Región para ejecutar la función Lambda: elija Ejecutar en la región de desactivación
    - Tiempo de espera (opcional)
    - Intervalo de reintento (opcional)

20. Selecciona Guardar paso.
21. Selecciona Añadir un paso.
22. Seleccione el bloque de ejecución de la aprobación manual y, a continuación, elija Añadir y editar. Este bloque solicita la aprobación de un miembro del equipo.
23. En el panel derecho, configura el bloque:

    - Nombre del paso: Introduzca la aprobación manual antes de cambiar la base de datos y el DNS
    - Descripción del paso (opcional)

- Función de aprobación de IAM: la función que debe asumir un usuario para poder aprobar la ejecución
- Tiempo de espera (opcional)

24. Selecciona Guardar paso.
25. Selecciona Añadir un paso.
26. Seleccione el bloque de ejecución de Aurora Global Database y, a continuación, elija Agregar y editar. Este bloque desencadena un cambio de base de datos global de Aurora (sin pérdida de datos). Para obtener más información, consulte Uso de la conmutación o la conmutación por error para la base de datos global de Aurora en la Guía del usuario de Aurora.
27. En el panel derecho, configure el bloque:

    - Nombre del paso: Introduzca la conmutación a Aurora
    - Descripción del paso (opcional)
    - Identificador de base de datos global de Aurora: nombre del clúster de Aurora
    - El ARN del clúster se utiliza para activar el us-east-1: El ARN del clúster Aurora en us-east-1
    - El ARN del clúster se utiliza para activar el us-west-2: El ARN del clúster Aurora en us-west-2
    - Seleccione la opción para la base de datos Aurora: elija Switchover
    - Tiempo de espera (opcional)

28. Selecciona Guardar paso.
29. Selecciona Añadir un paso.
30. Seleccione el bloque de ejecución del control de enrutamiento ARC y, a continuación, elija Agregar y editar. Este bloque realiza una conmutación por error de DNS para desplazar el tráfico a la región pasiva.
31. En el panel derecho, configura el bloque:

    - Nombre del paso: Ingresa Toggle DNS
    - Descripción del paso (opcional)
    - Controles de enrutamiento utilizados para activar el us-east-1: elija Agregar controles de enrutamiento
    - Tiempo de espera: introduzca un valor de tiempo de espera.

32. Elija Agregar control de enrutamiento:

    - ARN de control de enrutamiento: el ARN del control de enrutamiento que controla us-east-1

- Estado de control de enrutamiento: seleccione Activado

33. Vuelva a seleccionar Añadir control de enrutamiento:
    - ARN de control de enrutamiento: el ARN del control de enrutamiento que controla us-west-2
    - Estado de control de enrutamiento: seleccione Desactivado
34. Seleccione Save.
35. Controles de enrutamiento utilizados para activar el us-west-2: elija Agregar controles de enrutamiento
36. Elija Agregar control de enrutamiento:
    - ARN de control de enrutamiento: el ARN del control de enrutamiento que controla us-west-2
    - Estado de control de enrutamiento: seleccione Activado
37. Vuelva a seleccionar Añadir control de enrutamiento:
    - ARN de control de enrutamiento: el ARN del control de enrutamiento que controla us-east-1
    - Estado de control de enrutamiento: seleccione Desactivado
38. Seleccione Save.
39. Seleccione Guardar paso.
40. Seleccione Save.

Paso 3: Ejecute el plan

1. En la página de detalles del plan para cambiar de región, en la parte superior derecha, selecciona Ejecutar.
2. Introduzca los detalles de la ejecución:
    - Seleccione la región que desee activar.
    - Seleccione el modo de ejecución del plan.
    - (Opcional) Vea los pasos de ejecución.
    - Reconozca la ejecución del plan.
3. Elija Iniciar.
4. Puede ver los pasos detallados a medida que se ejecuta el plan en la página de detalles de la ejecución. Puede ver cada paso de la ejecución del plan, incluida la hora de inicio, la hora de finalización, el ARN del recurso y los mensajes de registro.

Cuando la región afectada se haya recuperado, podrá volver a ejecutar el plan (cambiando los parámetros que haya proporcionado) para activar la región original y volver a realizar las operaciones de la aplicación en la región principal original.

Operaciones de la API de cambio de región

En la siguiente tabla se enumeran las operaciones ARC que puede utilizar para el cambio de región, con enlaces a la documentación pertinente.

Acción	Uso de la consola ARC	Uso de la API ARC	API de plano de datos
Aprobar o denegar un paso de ejecución del plan	Consulte Bloque de ejecución y aprobación manual	Consulte ApprovePlanExecutionStep.	Sí
Cancelar la ejecución de un plan	Consulte Cree un plan de cambio de región	Consulte CancelPlanExecution.	Sí
Cree un plan	Consulte Cree un plan de cambio de región	Consulte CreatePlan.	No
Eliminar un plan	Consulte Trabajando con el conmutador de región	Consulte DeletePlan.	No
Obtenga un plan	Consulte Trabajando con el conmutador de región	Consulte GetPlan.	No
Obtenga el estado de evaluación del plan	Consulte Evaluación del plan	Consulte GetPlanEvaluationStatus.	Sí
Obtenga la ejecución de un plan	Consulte Paneles de control para cambiar de región	Consulte GetPlanExecution.	Sí

Acción	Uso de la consola ARC	Uso de la API ARC	API de plano de datos
Obtenga un plan en la región	Consulte Trabajando con el conmutador de región	Consulte GetPlanInRegion.	Sí
Enumere los controles de salud de un plan	Consulte Bloque de ejecución de chequeos de estado de Amazon Route 53	Consulte ListHealthChecksForPlan.	No
Enumere los eventos de ejecución del plan	Consulte Ejecute un plan de cambio de región para recuperar una aplicación	Consulte ListPlanExecutionEvents.	Sí
Enumere las ejecuciones del plan	Consulte Ejecute un plan de cambio de región para recuperar una aplicación	Consulte ListPlanExecutions.	Sí
Enumere los planes	Consulte Trabajando con el conmutador de región	Consulte ListPlans.	No
Enumere los planes en la región	Consulte Trabajando con el conmutador de región	Consulte ListPlansInRegion.	Sí
Enumerar las etiquetas de un recurso	Consulte Etiquetado para el conmutador de región ARC;	Consulte ListTagsForResource.	No
Inicie la ejecución de un plan	Consulte Ejecute un plan de cambio de región para recuperar una aplicación	Consulte StartPlanExecution.	Sí

Acción	Uso de la consola ARC	Uso de la API ARC	API de plano de datos
Etiquete un recurso	Consulte Cree un plan de cambio de región	Consulte TagResource.	No
Eliminar etiquetas de un recurso	Consulte Etiquetado para el conmutador de región ARC;	Consulte UntagResource.	No
Actualizar un plan	Consulte Cree un plan de cambio de región	Consulte UpdatePlan.	No
Actualizar la ejecución de un plan	Consulte Cree un plan de cambio de región	Consulte UpdatePlanExecution.	Sí
Actualizar un paso de ejecución del plan	Consulte Cree un plan de cambio de región	Consulte UpdatePlanExecutionStep.	Sí

Trabajando con el conmutador de región

En esta sección se proporcionan step-by-step instrucciones para trabajar con los planes de cambio de región, que puede utilizar para recuperar aplicaciones multirregionales. El cambio de región le permite crear planes tanto para los enfoques de recuperación como para active/passive los enfoques active/active de recuperación.

Para crear un plan de recuperación para su aplicación, haga lo siguiente:

1. Cree un plan de cambio de región. Un plan es una estructura con ciertos atributos, como los atributos específicos en los Regiones de AWS que se ejecuta la aplicación. Cada plan incluye uno o más flujos de trabajo.

   Si lo desea, puede crear varios planes y agrupar esos planes secundarios dentro de un plan de recuperación general.
2. Cree un flujo de trabajo para el plan. No puede ejecutar un plan sin crear primero un flujo de trabajo.
3. En el flujo de trabajo, añada uno o más pasos, cada uno de los cuales sea un bloque de ejecución.

Por ejemplo, puede agregar un bloque de ejecución para ampliar los grupos de EC2 Auto Scaling en una región de destino.

4. Después de añadir bloques de ejecución a su flujo de trabajo, es posible que se necesiten pasos adicionales, como configurar las comprobaciones de estado en Amazon Route 53. Cada sección del bloque de ejecución incluye la información de configuración que necesita. Para obtener más información, consulte Añada bloques de ejecución.
5. Para recuperar la aplicación cuando se esté ejecutando en un estado defectuoso Región de AWS, ejecute el plan.

   Puede realizar un seguimiento del progreso de la ejecución de un plan consultando la información en el panel global o en un panel regional.

En las siguientes secciones se proporciona información detallada y los pasos para crear un plan y flujos de trabajo, así como para añadir pasos de bloques de ejecución a los flujos de trabajo.

Contenido

- Cree un plan de cambio de región
- Cree flujos de trabajo de planes de cambio de región
- Añada bloques de ejecución
- Crea planes para niños
- Cree un activador para un plan de cambio de región
- Ejecute un plan de cambio de región para recuperar una aplicación

Los procedimientos de esta sección ilustran cómo trabajar con planes, flujos de trabajo, bloques de ejecución y activadores mediante el AWS Management Console. Para trabajar en su lugar con las operaciones de la API de cambio de región, consulte Operaciones de la API de cambio de región.

Cree un plan de cambio de región

Puedes crear dos tipos diferentes de planes en Region Switch: un active/active plan o un active/passive plan. Al crear un plan, especifique el tipo que se aplica a la forma en que desea gestionar la conmutación por error.

- Un enfoque activo/pasivo despliega dos réplicas de aplicaciones en dos regiones, y el tráfico se dirige únicamente a la región activa. Puede activar la réplica en la región pasiva ejecutando el plan de cambio de región.
- Un enfoque activo/activo despliega dos réplicas de aplicaciones en dos regiones, y ambas réplicas procesan el trabajo o reciben tráfico.

Para crear un plan de cambio de región

1. En la consola de cambio de región, elija Crear un plan de cambio de región con active/passive enfoque.
2. Proporcione los siguientes detalles:
   - Nombre del plan: introduzca un nombre descriptivo para su plan.
   - Enfoque multirregional: seleccione Activo/pasivo o Activo/activo. Este enfoque significa que se implementan dos réplicas de aplicaciones en dos regiones y que el tráfico se enrute únicamente a la región activa. Puede activar la réplica en la región pasiva ejecutando el plan de cambio de región.
     - Elija activa/pasiva si ha implementado dos réplicas de aplicaciones en dos regiones y el tráfico se dirige únicamente a la región activa. A continuación, puede activar la réplica en la región pasiva ejecutando el plan de cambio de región que especifica la opción activa/pasiva.
     - Elija Activa/activa si ha implementado dos réplicas de aplicaciones en dos regiones y ambas están procesando trabajo o recibiendo tráfico.
   - Regiones o regiones principales y en espera: seleccione las regiones principales y en espera para su aplicación. Para una active/active implementación, seleccione las regiones en las que se implementan las réplicas.
   - Objetivo de tiempo de recuperación (RTO): introduzca el RTO deseado. El conmutador de región lo utiliza para obtener información sobre el tiempo que tarda en ejecutarse el plan de cambio de región en comparación con el RTO deseado.
   - Función de IAM: proporcione una función de IAM para que el conmutador de región la utilice para ejecutar el plan. Para obtener más información sobre los permisos, consulte Identity and Access Management for Region Switch en ARC.
   - CloudWatch Alarma de Amazon: proporciona una alarma de estado de la aplicación que hayas creado con Amazon CloudWatch para indicar el estado de la aplicación en cada región. El conmutador de región utiliza estas alarmas de estado de las aplicaciones para ayudar a

determinar el tiempo de recuperación real después de cambiar de región para implementar la recuperación.

- Etiquetas: si lo desea, añada una o más etiquetas a su plan.

Cree flujos de trabajo de planes de cambio de región

Tras crear un plan de cambio de región, debe definir y crear flujos de trabajo que especifiquen el proceso de recuperación de su aplicación. Para cada plan, debe definir uno o más flujos de trabajo que completen la recuperación de su aplicación. En cada flujo de trabajo, agrega pasos que incluyen bloques de ejecución que definen cada acción que desea que Region Switch realice para la recuperación de la aplicación.

La cantidad de flujos de trabajo que cree depende del escenario de despliegue de la aplicación y de sus preferencias a la hora de gestionar la recuperación. Por ejemplo:

- Si su plan de cambio de región es para una active/active application deployment, you also need to create a deactivation workflow. This means that for or active/active implementación, tendrá un mínimo de dos flujos de trabajo: un flujo de trabajo de activación y un flujo de trabajo de desactivación.
- Si su plan de cambio de región es para el despliegue de una active/passive aplicación, tiene una región principal y una secundaria. Si decide tener flujos de trabajo de activación independientes para cada región, creará dos flujos de trabajo: uno para cada región.

Para crear flujos de trabajo de planificación, cambie de región.

1. En el plan de cambio de región que creó, elija Crear flujos de trabajo.
2. Seleccione una de las siguientes opciones de flujo de trabajo:
   - Cree el mismo flujo de trabajo de activación para todas las regiones: le permite utilizar el mismo flujo de trabajo de activación en todas las regiones.
   - Cree flujos de trabajo por separado para cada región: crea un flujo de trabajo de activación individual para cada región.
3. Si lo desea, proporcione una descripción para cada flujo de trabajo.
4. Defina el flujo de trabajo necesario para recuperar la aplicación. En su flujo de trabajo, agregue bloques de ejecución para definir los pasos que desea que Region Switch lleve a cabo para su recuperación. Cada bloque de ejecución define acciones, como el redireccionamiento del

tráfico de las aplicaciones o la recuperación de la base de datos en una región que se activa, y admite los recursos en otra Cuenta de AWS. Puede optar por que los bloques de ejecución se ejecuten en paralelo o secuencialmente. Para obtener información detallada sobre los bloques de ejecución específicos que puede añadir a los flujos de trabajo, consulteAñada bloques de ejecución.

5. En función de la opción de flujo de trabajo que haya seleccionado, haga lo siguiente:

   - Si ha seleccionado Crear el mismo flujo de trabajo de activación para todas las regiones, se necesitará un flujo de trabajo de activación.
   - Si ha seleccionado Crear flujos de trabajo por separado para cada región, se necesitan dos flujos de trabajo de activación.

   En el active/active caso de los planes, debe definir tanto un flujo de trabajo de activación como un flujo de trabajo de desactivación.

Añada bloques de ejecución

Agregue bloques de ejecución a los flujos de trabajo de su plan de cambio de región para realizar los pasos individuales necesarios para completar la conmutación por error o la conmutación de su aplicación. Para obtener información detallada sobre la funcionalidad y el comportamiento de cada tipo de bloque de ejecución, consulte las siguientes descripciones.

El cambio de región ejecuta una evaluación del plan inmediatamente después de crearlo o actualizarlo y, a continuación, cada 30 minutos durante el estado estable. El conmutador de región almacena información sobre la evaluación del plan en todas las regiones en las que está configurado su plan. Aquí, cada sección del bloque de ejecución incluye información sobre lo que se evalúa cuando el cambio de región ejecuta la evaluación del plan.

El conmutador de región incluye tipos de bloques de ejecución que ayudan a escalar los recursos informáticos como parte de la recuperación. Si utiliza estos bloques de ejecución en un plan, tenga en cuenta que el cambio de región no garantiza que se alcance la capacidad informática deseada. Si tiene una aplicación esencial y necesita garantizar el acceso a la capacidad, le recomendamos que reserve la capacidad. Existen estrategias que puede seguir para reservar la capacidad de cómputo en una región secundaria y, al mismo tiempo, limitar los costos. Para obtener más información, consulte Pilot light con capacidad reservada: Cómo optimizar los costes de recuperación ante desastres mediante reservas de capacidad bajo demanda.

El conmutador de región admite los siguientes bloques de ejecución.

Bloque de ejecución	Función	Configuración desordenada
Bloque de ejecución del plan del conmutador de región ARC	Organice la recuperación de varias aplicaciones en una sola ejecución especificando los planes secundarios de ejecución.	Comience los planes para niños con su configuración desordenada.
Bloque de ejecución grupal de Amazon EC2 Auto Scaling	Escale los recursos de EC2 cómputo que se encuentran en un grupo de Auto Scaling como parte de la ejecución de su plan.	Especifique el porcentaje mínimo de capacidad informática que debe coincidir en la región que vaya a activar.
Bloque de ejecución de escalado de recursos de Amazon EKS	Escale los pods de clústeres de Amazon EKS como parte de la ejecución de su plan.	N/A
Bloque de ejecución de escalado del servicio Amazon ECS	Amplíe las tareas de servicio de Amazon ECS como parte de la ejecución de su plan.	N/A
Bloque de ejecución del control de enrutamiento ARC	Añada un paso para cambiar el estado de uno o más controles de enrutamiento ARC, a fin de redirigir el tráfico de su aplicación a un objetivo Región de AWS.	N/A
Bloque de ejecución de Amazon Aurora Global Database	Realice un flujo de trabajo de recuperación para una base de datos global de Aurora.	Realice una conmutación por error en las bases de datos globales de Aurora (puede provocar la pérdida de datos).

Bloque de ejecución	Función	Configuración desordenada
Bloque de ejecución y aprobación manual	Inserte un paso de aprobación para solicitar la aprobación o cancelación de una ejecución antes de continuar.	N/A
Bloque de ejecución de Lambda de acción personalizada	Añada un paso personalizado para ejecutar una función Lambda, a fin de habilitar las acciones personalizadas.	Omita este paso.
Bloque de ejecución de chequeos de estado de Amazon Route 53	Especifica las regiones a las que se redirigirá el tráfico de la aplicación durante la conmutación por error.	N/A

Bloque de ejecución del plan del conmutador de región ARC

El bloque de ejecución del plan de cambio de región te permite organizar el orden en el que varias aplicaciones se transfieren a la región que deseas activar, haciendo referencia a otros planes de cambio de región secundarios. Gracias a esta relación padre/hijo, puede crear procesos de recuperación complejos y coordinados que gestionen varios recursos y dependencias en toda su infraestructura.

Configuración

Cuando utiliza el bloque de ejecución del plan de cambio de región, selecciona un plan de cambio de región específico que desea que se ejecute en el flujo de trabajo del plan que está creando.

Para configurar un bloque de ejecución de un plan de cambio de región, introduzca los siguientes valores:

1. Nombre del paso: introduzca un nombre.

2. Descripción del paso (opcional): introduzca una descripción del paso.
3. Plan de cambio de región: seleccione un plan para ejecutarlo en el flujo de trabajo del plan actual.

A continuación, seleccione Guardar paso.

Funcionamiento

Utilice el bloque de ejecución del plan de cambio de región para crear flujos de trabajo anidados con parent/child relaciones. Tenga en cuenta que este bloque de ejecución no admite niveles adicionales de planes secundarios y limita la cantidad de planes secundarios anidados. Los planes para niños deben apoyar a las mismas regiones que el plan principal y deben tener el mismo enfoque de recuperación que el plan para padres (es decir, activo active/active o pasivo).

Este bloque admite los modos de ejecución elegante y desgraciado. Los escenarios desgraciados iniciarán planes infantiles con su configuración desgraciada. Si el bloqueo de cambio de región se ejecutó correctamente y, a continuación, se cambió al modo de ejecución irregular, cualquier plan secundario también pasará al modo de ejecución irregular.

¿Qué se evalúa como parte de la evaluación del plan

Si compartes un plan entre cuentas y el plan ya no se comparte con la cuenta del plan principal, la evaluación del cambio de región mostrará una advertencia de que el plan no es válido.

Bloque de ejecución grupal de Amazon EC2 Auto Scaling

El bloque de ejecución grupal de EC2 Auto Scaling le permite escalar EC2 instancias como parte de su proceso de recuperación multirregional. Puede definir un porcentaje de capacidad en relación con la región de la que se va (origen y destino).

Configuración

Al configurar el bloque de ejecución grupal de EC2 Auto Scaling, ingresa el EC2 Auto Scaling ARNs para las regiones específicas asociadas a su plan. Debe introducir EC2 Auto Scaling ARNs en cada región que desee ampliar durante la ejecución del plan.

Para configurar un bloque de ejecución grupal de EC2 Auto Scaling, introduzca los siguientes valores:

1. Nombre del paso: introduzca un nombre.

2. Descripción del paso (opcional): introduzca una descripción del paso.
3. EC2 ARN del grupo de Auto Scaling para la región: Introduzca el ARN del EC2 Auto Scaling en cada región de su plan.
4. Porcentaje que coincide con la capacidad de la región activada: introduzca el porcentaje deseado del número de instancias en ejecución en el grupo de Auto Scaling que coincida con la región activada.
5. Enfoque de monitoreo de capacidad: en el menú desplegable, selecciona tu enfoque de monitoreo para tus grupos de EC2 Auto Scaling.
6. Tiempo de espera: introduzca un valor de tiempo de espera.

A continuación, selecciona Guardar paso.

Funcionamiento

Después de configurar un bloque de ejecución de EC2 Auto Scaling, el conmutador de región confirma que solo hay un grupo de Auto Scaling de origen y un grupo de Auto Scaling de destino. Si hay varios grupos de Auto Scaling, el bloque de ejecución falla durante la evaluación del plan. La capacidad objetivo se define como el número de instancias que tienen un estado establecido en`InService`. Para obtener más información, consulte Ciclo de vida de las instancias de EC2 Auto Scaling.

En función del valor que especifique (al configurar el bloque de ejecución de Auto Scaling) para un porcentaje de coincidencia, el conmutador de región calcula la nueva capacidad deseada para el grupo de Auto Scaling de destino. La nueva capacidad deseada se compara con la capacidad deseada del grupo de Auto Scaling de destino. La fórmula que utiliza Region Switch para calcular la capacidad deseada es la siguiente:`ceil(percentToMatch * Source Auto Scaling group capacity)`, donde ceil () es una función que redondea cualquier resultado fraccionario. Si la capacidad actual deseada del grupo de Auto Scaling de destino es mayor o igual a la capacidad deseada del nuevo grupo de Auto Scaling que calcula el conmutador de región, el bloque de ejecución continúa. Tenga en cuenta que el cambio de región no reduce la capacidad del grupo de Auto Scaling.

Cuando el conmutador de región ejecuta un bloque de Auto Scaling, el conmutador de región intenta ampliar la capacidad del grupo de Auto Scaling de la región objetivo para que coincida con la capacidad deseada. A continuación, el cambio de región espera hasta que se alcance la capacidad de grupo de Auto Scaling solicitada en el grupo de Auto Scaling de la región objetivo antes de que el cambio de región pase al siguiente paso del plan.

Si está utilizando un active/active enfoque, el conmutador de región utiliza la otra región configurada como origen. Es decir, si se está desactivando una región, el conmutador de región utiliza la otra región activa como fuente para igualar el porcentaje a escalar.

Este bloque admite los modos de ejecución elegantes y desgraciados. Puede configurar una ejecución irregular especificando el porcentaje mínimo de capacidad informática que debe corresponder a la región de destino antes de que el cambio de región pase al siguiente paso del plan.

¿Qué se evalúa como parte de la evaluación del plan

Cuando Region Switch evalúa su plan, Region Switch realiza varias comprobaciones críticas de la configuración y los permisos del bloque de ejecución grupal de EC2 Auto Scaling. La evaluación del cambio de región verifica que los grupos de Auto Scaling estén presentes en ambas regiones, asegura que estén correctamente configurados y sean accesibles, y anota el número de instancias en ejecución en cada región. También confirma que la capacidad máxima del grupo Auto Scaling de la región objetivo es suficiente para gestionar el porcentaje de coincidencia de escala especificado para la capacidad requerida.

El cambio de región también valida que la función de IAM del plan tenga los permisos correctos para Auto Scaling. Para obtener más información sobre los permisos necesarios para los bloques de ejecución del cambio de región, consulte. Ejemplos de políticas basadas en la identidad para el cambio de región en ARC Si se produce un error en alguna de las comprobaciones, el conmutador de región mostrará mensajes de advertencia, que podrá ver en la consola. O bien, puede recibir las advertencias de validación a través de las operaciones de la API EventBridge o mediante ellas.

Bloque de ejecución de escalado de recursos de Amazon EKS

El bloque de ejecución de escalado de recursos de EKS le permite escalar los recursos de EKS como parte de su proceso de recuperación multirregional. Al configurar el bloque de ejecución, se define un porcentaje de la capacidad que se va a escalar en relación con la capacidad de la región que se va a desactivar.

Configure los permisos de entrada de acceso a EKS

Antes de poder añadir un bloque de ejecución para el escalado de recursos de EKS, debe proporcionar a Region Switch los permisos necesarios para realizar acciones con los recursos de Kubernetes de sus clústeres de EKS. Para proporcionar acceso al conmutador de región, debe crear una entrada de acceso EKS para la función de IAM que el conmutador de región utiliza

para la ejecución del plan, mediante la siguiente política de acceso al conmutador de región: `arn:aws:eks::aws:cluster-access-policy/AmazonARCRegionSwitchScalingPolicy`

Política de acceso al EKS del conmutador regional

La siguiente información proporciona detalles sobre la política de acceso a EKS.

Nombre: `AmazonARCRegionSwitchScalingPolicy`

ARN de la política: `arn:aws:eks::aws:cluster-access-policy/AmazonARCRegionSwitchScalingPolicy`

Grupos de API de Kubernetes	Recursos de Kubernetes	Verbos de Kubernetes (permisos)
*	*/escala	obtener, actualizar
*	*/estado	introducción
autoscaling	escaladores automáticos horizontales	obtener, parchear

Cree una entrada de acceso EKS para el conmutador de región

En el siguiente ejemplo, se describe cómo crear las asociaciones de entrada y política de acceso necesarias para que Region Switch pueda tomar medidas específicas para sus recursos de Kubernetes. En este ejemplo, los permisos se aplican al espacio de nombres del clúster *`my-cluster`* de EKS para *`my-namespace1`* la función de IAM. `arn:aws:iam::555555555555:role/`*`my-role`*

Al configurar estos permisos, asegúrese de seguir estos pasos para los dos clústeres de EKS del bloque de ejecución.

Requisito previo

Antes de empezar, cambie el modo de autenticación del clúster a uno `API_AND_CONFIG_MAP` u otro`API`. Al cambiar el modo de autorización, se añade la API para las entradas de acceso. Para obtener más información, consulte Cambiar el modo de autenticación para usar entradas de acceso en la Guía del usuario de Amazon EKS.

Cree la entrada de acceso

El primer paso consiste en crear la entrada de acceso mediante un AWS CLI comando similar al siguiente:

```
aws eks create-access-entry --cluster-name my-cluster --principal-arn
        arn:aws:iam::555555555555:user/my-user --type STANDARD
```

Para obtener más información, consulte Crear entradas de acceso en la Guía del usuario de Amazon EKS.

Cree la asociación de entradas de acceso

A continuación, cree la asociación a la política de acceso del conmutador de región mediante un AWS CLI comando similar al siguiente:

```
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
```

Para obtener más información, consulte Asociar políticas de acceso a entradas de acceso en la Guía del usuario de Amazon EKS.

Asegúrese de repetir estos pasos con el segundo clúster EKS del bloque de ejecución, en la otra región, para garantizar que el conmutador de región pueda acceder a ambos clústeres.

Configuración

Para configurar el bloque de ejecución de escalado de recursos de EKS, primero asegúrese de contar con los permisos correctos. Para obtener más información, consulte Configure los permisos de entrada de acceso a EKS.

Tenga en cuenta que el conmutador de región admite actualmente los siguientes ReplicaSet recursos: apps/v1, Deployment, and apps/v 1.

A continuación, para la configuración del bloque de ejecución, introduzca los siguientes valores.

1. Nombre del paso: introduzca un nombre.
2. Descripción del paso (opcional): introduzca una descripción del paso.
3. Nombre de la aplicación: introduzca el nombre de su aplicación EKS, por ejemplo, myApplication.

4. Tipo de recurso de Kubernetes: introduzca el tipo de recurso de la aplicación, por ejemplo, Despliegue.
5. Recurso por región: para cada región, introduzca la información del clúster de EKS, incluido el ARN del clúster de EKS, el espacio de nombres del recurso, etc.
6. Porcentaje que coincida con la capacidad de la región activada: introduce el porcentaje deseado de pods en ejecución en la región de origen que coincida con la región activada.
7. Método de supervisión de la capacidad: en el menú desplegable, seleccione el enfoque de supervisión para sus recursos de EKS.
8. Tiempo de espera: introduzca un valor de tiempo de espera.

A continuación, selecciona Guardar paso.

Funcionamiento

Durante la ejecución de un plan, el conmutador de región recupera el número máximo de réplicas muestreado en las últimas 24 horas para el recurso objetivo en la región que se está activando. A continuación, calcula el recuento de réplicas deseado para el recurso de destino mediante la siguiente fórmula: `ceil(percentToMatch * Source replica count)`

Si el recuento de réplicas listas para el destino es inferior al valor deseado, Region Switch escala el valor de la réplica del recurso de destino a la capacidad deseada. Espera a que las réplicas estén listas y aprovecha el escalador automático de nodos para aumentar la capacidad de los nodos si es necesario.

Si el `hpaName` campo opcional no está vacío, Region Switch lo HorizontalPodAutoscaler parchea para evitar que se reduzca automáticamente la escala durante o después de la ejecución mediante el siguiente parche: `{"spec":{"behavior":{"scaleDown": {"selectPolicy":"Disabled"}}}}`

Asegúrese de configurar cualquier herramienta de corrección de desviaciones, como las GitOps herramientas, para que ignore el campo de réplica de los recursos del parche, así como el campo. HorizontalPodAutoscaler

¿Qué se evalúa como parte de la evaluación del plan

Cuando Region Switch evalúa su plan, Region Switch realiza varias comprobaciones del bloque de ejecución de EKS y de los permisos configurados. El conmutador de región verifica que la función de IAM del plan tenga los permisos correctos para describir los clústeres de EKS y enumerar las

políticas de entrada de acceso asociadas. El cambio de región también valida que la función de IAM esté asociada a la política de entrada de acceso correcta, de modo que el cambio de región tenga los permisos necesarios para actuar sobre los recursos de Kubernetes. Por último, el cambio de región confirma que existen los clústeres de EKS configurados y los recursos de Kubernetes.

Además, el conmutador de región comprueba que ha recopilado y almacenado correctamente los datos de supervisión necesarios (recuento de réplicas de Kubernetes) y registra el número de pods en ejecución necesarios para ejecutar el plan de conmutación de región.

Bloque de ejecución de escalado del servicio Amazon ECS

El bloque de ejecución de escalado del servicio de ECS le permite escalar su servicio de ECS en una región de destino como parte de su proceso de recuperación multirregional. Puede definir un porcentaje de capacidad en relación con la región desde la que el conmutador de región se conmuta por error o se desactiva.

Configuración

Para configurar el bloque de ejecución de escalado del servicio ECS, introduzca los siguientes valores.

1. Nombre del paso: introduzca un nombre.
2. Descripción del paso (opcional): introduzca una descripción del paso.
3. Recurso por región: para cada región, introduzca el ARN del clúster de ECS y el ARN del servicio de ECS.
4. Porcentaje que coincide con el recuento de tareas de la región de origen: introduzca el porcentaje deseado de tareas en ejecución en la región de origen que coincida con el de la región activada.
5. Método de supervisión de la capacidad: en el menú desplegable, seleccione el enfoque de supervisión para sus recursos de ECS.
6. Tiempo de espera: introduzca un valor de tiempo de espera.

A continuación, selecciona Guardar paso.

Funcionamiento

Tras configurar el bloque de ejecución en su plan, el conmutador de región confirma que solo hay un servicio ECS de origen y un servicio de destino. Si hay varios servicios, el conmutador de región muestra una advertencia para el bloque de ejecución. El conmutador de región almacena estos datos

en todas las regiones para las que esté configurado su plan. La capacidad objetivo se define como el recuento deseado establecido en su servicio de ECS.

Como active/passive enfoque, el conmutador de región calcula la nueva capacidad deseada para el servicio de ECS en la región de destino (de activación). La nueva capacidad deseada se compara con la capacidad deseada del servicio ECS de destino. La fórmula que utiliza Region Switch para calcular la capacidad deseada es la siguiente:`ceil(percentToMatch * Source Auto Scaling group capacity)`, donde ceil () es una función que redondea cualquier resultado fraccionario. Si el recuento actual deseado para el servicio ECS de destino es superior a la nueva capacidad deseada calculada para el servicio ECS, la ejecución del plan continúa. Tenga en cuenta que el cambio de región no reduce la capacidad del servicio de ECS.

Si el servicio ECS tiene activado el escalado automático de aplicaciones, el conmutador de región actualiza la capacidad mínima en el escalado automático de aplicaciones y también actualiza el recuento deseado en el servicio ECS.

Cuando el conmutador de región ejecuta un bloque de servicios de ECS, el conmutador de región intenta ampliar la capacidad de ECS de la región de destino para ajustarla a la capacidad deseada. A continuación, el conmutador de región espera hasta que se alcance la capacidad de servicio de ECS solicitada en el servicio de ECS de la región de destino antes de pasar al siguiente paso del plan. Si lo deseas, puedes configurar el paso para que se complete antes de que se complete la gestión logística. Para ello, establece un límite de tiempo de espera para que el cambio de región se complete antes de completar la gestión logística.

Si utilizas un active/active enfoque, el conmutador de región utiliza la otra región configurada como origen. Es decir, si se está desactivando una región, el conmutador de región utiliza la otra región activa como fuente para igualar el porcentaje a escalar.

¿Qué se evalúa como parte de la evaluación del plan

Cuando Region Switch evalúa su plan, Region Switch realiza varias comprobaciones de la configuración y los permisos del bloque de ejecución del servicio ECS. El cambio de región verifica que los servicios de ECS estén presentes tanto en la región de origen como en la de destino, y comprueba que la capacidad máxima establecida para el servicio de ECS de la región de destino es suficiente para gestionar el porcentaje de coincidencia especificado de la capacidad de la región de destino. El cambio de región también valida que la función de IAM del plan tenga los permisos correctos para el servicio de ECS. Para obtener más información sobre los permisos necesarios para los bloques de ejecución de los cambios de región, consulte. Ejemplos de políticas basadas en la identidad para el cambio de región en ARC

Además, el conmutador de región comprueba que se `ResourceMonitor` han recopilado y almacenado correctamente los datos de supervisión necesarios para los servicios de ECS y hace un recuento del número de tareas en ejecución.

Si alguna de las comprobaciones falla, el conmutador de región muestra mensajes de advertencia, que puede ver en la consola. O bien, puede recibir las advertencias de validación a través de las operaciones de la API EventBridge o mediante ellas.

Bloque de ejecución del control de enrutamiento ARC

Si ha configurado el control de enrutamiento de Amazon Application Recovery Controller (ARC) para su aplicación, puede añadir un bloque de ejecución del control de enrutamiento ARC para redirigir el tráfico de la aplicación. Este bloque de ejecución le permite cambiar el estado de uno o más controles de enrutamiento ARC para redirigir el tráfico de la aplicación a un destino Región de AWS. El control de enrutamiento ARC redirige el tráfico mediante comprobaciones de estado en Amazon Route 53 que se configuran con los registros DNS asociados a los controles de enrutamiento.

Configuración

Para configurar un bloque de ejecución del control de enrutamiento, introduzca los siguientes valores:

1. Nombre del paso: introduzca un nombre.
2. Descripción del paso (opcional): introduzca una descripción del paso.
3. Controles de enrutamiento deseados: Para cada región que desee activar o desactivar, introduzca el ARN del control de enrutamiento y el estado inicial del control de enrutamiento, Activado o Desactivado.
4. Tiempo de espera: introduzca un valor de tiempo de espera.

A continuación, selecciona Guardar paso.

El patrón esperado para este bloque de ejecución consiste en especificar los controles de enrutamiento y los estados iniciales que se ajusten a la forma en que se ha configurado la aplicación en concreto Regiones de AWS. Por ejemplo, si tiene un plan que le permite activar la región A y la región B para su aplicación, es posible que tenga un control de enrutamiento para la región A en el que se establece el estado en Activado y un control de enrutamiento para la región B en el que se establece el estado en Activado.

A continuación, cuando ejecute el plan y especifique que desea activar la región A, el flujo de trabajo que incluye este bloque de ejecución actualiza el control de enrutamiento especificado a Activado, lo que dirige el tráfico a la región A.

Funcionamiento

Al configurar un bloque de ejecución del control de enrutamiento ARC, puede redirigir el tráfico de la aplicación a un destino o Región de AWS, si es un active/active enfoque, impedir que el tráfico se enrute a una región que esté desactivando. Si su plan incluye varios flujos de trabajo, asegúrese de proporcionar las mismas entradas para los registros DNS de todos los bloques de ejecución del control de enrutamiento que utilice.

Este bloque no admite el modo de ejecución irregular.

¿Qué se evalúa como parte de la evaluación del plan

Cuando Region Switch evalúa su plan, Region Switch realiza varias comprobaciones de los controles de enrutamiento, la configuración del bloque de ejecución y los permisos. El conmutador de región verifica que los controles de enrutamiento especificados estén correctamente configurados y sean accesibles.

El cambio de región también valida que la función de IAM del plan tenga los permisos necesarios para acceder a los estados de control de enrutamiento y actualizarlos. Para obtener más información sobre los permisos necesarios para los bloques de ejecución de los conmutadores de región, consulte. Ejemplos de políticas basadas en la identidad para el cambio de región en ARC

Los permisos de IAM correctos son esenciales para el correcto funcionamiento del bloque de ejecución del control de enrutamiento. Si se produce un error en alguna de estas validaciones, el conmutador de región muestra advertencias sobre la existencia de problemas y proporciona mensajes de error específicos para ayudarle a resolver los problemas de permisos o configuración. Esto garantiza que su plan tenga el acceso necesario para administrar los controles de enrutamiento ARC e interactuar con ellos durante la ejecución de este paso.

Bloque de ejecución de Amazon Aurora Global Database

El bloque de ejecución de Amazon Aurora Global Database le permite realizar un flujo de trabajo de recuperación por error o conmutación para una base de datos global.

- Conmutación por error: utilice este enfoque para recuperarse de una interrupción imprevista. Con este enfoque, realiza una conmutación por error entre regiones a uno de los clústeres de bases de datos secundarios de las bases de datos globales de Aurora. El objetivo del punto de

recuperación (RPO) de este enfoque suele ser un valor distinto de cero medido en segundos. La cantidad de pérdida de datos depende del retraso en la replicación de las bases de datos globales de Aurora Regiones de AWS en el momento de la falla. Para obtener más información, consulte Recuperación de una base de datos global de Amazon Aurora tras una interrupción imprevista en la Guía del usuario de Amazon Aurora.

- Conmutación: anteriormente, esta operación se denominaba conmutación por error planificada gestionada. Utilice este enfoque para situaciones controladas, como el mantenimiento operativo y otros procedimientos operativos planificados en los que todos los clústeres de Aurora y otros servicios con los que interactúan se encuentren en buen estado. Dado que esta característica sincroniza los clústeres secundarios de base de datos con el principal antes de realizar cualquier otro cambio, el RPO es 0 (sin pérdida de datos). Para obtener más información, consulte Realizar cambios en las bases de datos globales de Amazon Aurora en la Guía del usuario de Amazon Aurora.

Configuración

Para configurar un bloque de ejecución de Aurora Global Database, introduzca los siguientes valores:

1. Nombre del paso: introduzca un nombre.
2. Descripción del paso (opcional): introduzca una descripción del paso.
3. Nombre del clúster de la base de datos global Aurora: introduzca el identificador de la base de datos global.
4. ARN del clúster para la región: introduzca el ARN del clúster que se utilizará en cada región del plan.
5. Especifique la opción para la base de datos Aurora: elija entre conmutación o conmutación por error (pérdida de datos), según lo que desee
6. Nombre del clúster de Aurora Global Database:
7. Tiempo de espera: introduzca un valor de tiempo de espera.

A continuación, selecciona Guardar paso.

Funcionamiento

Al configurar un bloque de ejecución de Aurora Global Databases, puede realizar la conmutación por error o la conmutación de bases de datos globales como parte de la recuperación de la aplicación.

Si utiliza un active/active enfoque, el conmutador de región utiliza la otra región configurada como origen. Es decir, si se está desactivando una región, el conmutador de región utiliza la otra región activa como fuente para igualar el porcentaje a escalar.

Este bloque admite los modos de ejecución elegantes y desgraciados. Una configuración incorrecta provoca una conmutación por error de Aurora Global Database, lo que podría provocar la pérdida de datos.

Para obtener más información sobre la recuperación ante desastres de Aurora Global Database, incluidas la conmutación por error y la conmutación, consulte Uso de la conmutación o la conmutación por error en las bases de datos globales de Amazon Aurora en la Guía del usuario de Amazon Aurora.

¿Qué se evalúa como parte de la evaluación del plan

Cuando el conmutador de región evalúa su plan, el conmutador de región realiza varias comprobaciones de la configuración y los permisos del bloque de ejecución de Aurora. El cambio de región verifica que lo siguiente sea correcto:

- Existe el clúster global de Aurora especificado en la configuración.
- Hay clústeres de bases de datos Aurora tanto en la región de origen como en la de destino.
- Los clústeres de bases de datos de origen y destino están en un estado que permite el cambio de base de datos global.
- Hay instancias de base de datos tanto en el clúster de origen como en el de destino
- Las versiones del motor de clústeres global para la acción de conmutación son compatibles. Esto incluye verificar que los clústeres estén en las mismas versiones principal, secundaria y de parche, con algunas excepciones que se indican en la documentación de Aurora.

El cambio de región también valida que la función de IAM del plan tenga los permisos necesarios para la conmutación por error y la conmutación de Aurora. Para obtener más información sobre los permisos necesarios para los bloques de ejecución del cambio de región, consulte. Ejemplos de políticas basadas en la identidad para el cambio de región en ARC

Los permisos de IAM correctos son esenciales para el correcto funcionamiento del bloque de ejecución de Aurora. Si se produce un error en alguna de estas validaciones, Region Switch muestra advertencias sobre la existencia de problemas y proporciona mensajes de error específicos para

ayudarle a resolver los problemas de permisos o configuración. Esto garantiza que su plan tenga el acceso necesario para gestionar la Aurora e interactuar con ella durante la ejecución de este paso.

Bloque de ejecución y aprobación manual

El bloque de ejecución de la aprobación manual permite insertar un paso de aprobación que se asocia a una función de IAM. Los usuarios con acceso al rol pueden aprobar o rechazar la ejecución de un paso, pausar el paso hasta que se conceda la aprobación o, posiblemente, impedir que el plan avance.

Para garantizar que se requiera la aprobación manual durante la ejecución del plan, debe introducir un paso de aprobación manual en una ubicación específica del flujo de trabajo y, a continuación, configurar la función de IAM para especificar quién puede aprobar el paso.

Configuración

Para configurar un bloque de ejecución de la aprobación manual, introduzca los siguientes valores:

1. Nombre del paso: introduzca un nombre.
2. Descripción del paso (opcional): introduzca una descripción del paso.
3. Función de aprobación de IAM: introduzca el ARN de una función de IAM que tenga permiso para aprobar manualmente la ejecución y continuar con el plan de cambio de región. La función de IAM debe estar dentro de la cuenta propietaria del plan.
4. Tiempo de espera: introduzca un valor de tiempo de espera.

A continuación, selecciona Guardar paso.

Funcionamiento

Al configurar un bloque de ejecución de la aprobación manual, puede solicitar una aprobación como parte de la recuperación de la aplicación. En el caso de un bloque de ejecución manual, el conmutador de región hace lo siguiente:

- Cuando el conmutador de región ejecuta un bloque de ejecución manual, detiene la ejecución y establece el estado de ejecución del plan en pendiente de aprobación.
- Cualquier persona que tenga acceso a la función definida en el bloque de ejecución puede aprobar o rechazar la ejecución del paso.
- Si aprueban la ejecución del paso, el cambio de región procederá a ejecutar el plan. Si lo rechazan, el cambio de región cancela la ejecución del plan.

Este bloque no admite el modo de ejecución irregular.

¿Qué se evalúa como parte de la evaluación del plan

El cambio de región no completa ninguna evaluación de los bloques de ejecución de la aprobación manual.

Bloque de ejecución de Lambda de acción personalizada

El bloque de ejecución de Lambda de acciones personalizadas permite añadir un paso personalizado a un plan mediante una función de Lambda.

Configuración

Para configurar un bloque de ejecución de Lambda, introduzca los siguientes valores:

1. Nombre del paso: introduzca un nombre.
2. Descripción del paso (opcional): introduzca una descripción del paso.
3. El ARN de la función Lambda que se invocará al activar o desactivar la región: especifique el ARN de la función Lambda que se va a ejecutar en este paso.
4. Región para ejecutar la función Lambda: en el menú desplegable, elija la región en la que desee ejecutar las funciones Lambda.
5. Tiempo de espera: introduzca un valor de tiempo de espera.
6. Intervalo de reintento: introduzca un intervalo de reintento para volver a ejecutar la función Lambda si no tiene éxito dentro de este intervalo.

A continuación, seleccione Guardar paso.

Funcionamiento

- Al crear un bloque de ejecución de Lambda de acciones personalizadas, debe especificar dos funciones de Lambda para que el paso se ejecute, una en cada una de las regiones del plan.
- Puede configurar la región en la que desea que se ejecute la Lambda, por ejemplo, en la región de activación o en la región de desactivación. Sin embargo, si ejecuta en la región de desactivación, pasa a depender de esa región. No te recomendamos que dependas de la región que se está desactivando.

Este bloque admite los modos de ejecución elegantes y desgraciados. En el modo de ejecución irregular, el conmutador de región omite el paso del bloque de ejecución de Lambda.

¿Qué se evalúa como parte de la evaluación del plan

Cuando Region Switch evalúa su plan, Region Switch realiza varias comprobaciones de la configuración y los permisos del bloque de ejecución de Lambda. El conmutador de región comprueba que lo siguiente es correcto:

- Existen las funciones Lambda especificadas en la configuración.
- La configuración de simultaneidad de las funciones Lambda no está limitada, incluida la verificación de lo siguiente:
  - La simultaneidad no está establecida en 0.
  - Hay al menos una ejecución simultánea disponible o existe esa simultaneidad sin reservas.

El conmutador de región realiza una ejecución en seco de la función Lambda para validar los parámetros y permisos especificados, sin ejecutar la lógica de la función real. Se incurre en los costes estándar de Lambda cuando se realiza un ensayo en seco.

El cambio de región también valida que la función de IAM del plan tenga los permisos necesarios para la ejecución de Lambda. Para obtener más información sobre los permisos necesarios para los bloques de ejecución de los cambios de región, consulte. Ejemplos de políticas basadas en la identidad para el cambio de región en ARC

Los permisos de IAM correctos son esenciales para el correcto funcionamiento del bloque de ejecución de Lambda. Si se produce un error en alguna de estas validaciones, el conmutador de región muestra advertencias sobre la existencia de problemas y proporciona mensajes de error específicos para ayudarle a resolver los problemas de permisos o configuración. Esto garantiza que su plan tenga el acceso necesario para administrar la Lambda e interactuar con ella durante la ejecución de este paso.

Bloque de ejecución de chequeos de estado de Amazon Route 53

El bloque de ejecución de comprobaciones de estado de Amazon Route 53 le permite especificar las regiones a las que se redirigirá el tráfico de su aplicación durante la conmutación por error. El bloque de ejecución crea comprobaciones de estado de Amazon Route 53, que luego se adjuntan a los registros DNS de Route 53 de tu cuenta. Cuando ejecuta su plan de cambio de región, el estado de las comprobaciones de estado de Route 53 se actualiza y el tráfico se redirige en función de su configuración de DNS.

Configuración

Para configurar un bloque de ejecución de comprobaciones de estado de Route 53, ingresa los siguientes valores:

1. Nombre del paso: introduzca un nombre.
2. Descripción del paso (opcional): introduzca una descripción del paso.
3. ID de zona alojada: el ID de zona alojada de su dominio y registros de DNS en Route 53.
4. Nombre de registro: el nombre de registro (nombre de dominio) de los registros que utilizas, con las comprobaciones de estado asociadas, para redirigir el tráfico hacia tu aplicación.
5. Identificadores de conjuntos de registros (opcionales): si es necesario, proporcione información adicional para ayudar a Region Switch a identificar el conjunto de registros que asocia a cada región para redirigir el tráfico a esa región. La información de identificación que se debe introducir, si es necesaria, es la siguiente:
   - Identificador del conjunto de registros: puede introducir el identificador del conjunto de registros o el valor/ruta al que se dirige el tráfico para el conjunto de registros.
   - Región: introduzca la región asociada al conjunto de registros que contiene la información del identificador del conjunto de registros que ingresó.
6. Seleccione Guardar paso.
7. Configure las comprobaciones de estado en Route 53.

   El conmutador de región proporciona un identificador de comprobación de estado, para cada región, para cada nombre de registro dentro de una zona alojada definida en el bloque de ejecución. Asegúrese de configurar las comprobaciones de estado de los conjuntos de registros correspondientes de su cuenta en Route 53 para que el conmutador de región pueda redirigir correctamente el tráfico de su aplicación durante la ejecución del plan. En la pestaña Comprobaciones de estado de la página de detalles del plan, puede ver las comprobaciones de estado de todos los bloques de ejecución y regiones.

Funcionamiento

Añada un bloque de ejecución de comprobaciones de estado al flujo de trabajo del cambio de región para poder redirigir el tráfico a una región secundaria (en el caso de active/passive las configuraciones) o alejarlo de una región desactivada (en el caso de active/active las configuraciones). Si añades varios flujos de trabajo a tu plan, proporciona los mismos valores de

configuración para todos los bloques de ejecución de comprobaciones de estado que utilizan los mismos registros de DNS.

En función de la información que proporciona al configurar el bloque de ejecución, el cambio de región intenta determinar el conjunto de registros correcto para cada región de su plan. Por lo general, el identificador de la zona alojada y el nombre del registro son información suficiente para determinar los conjuntos de registros y las regiones asociadas. De lo contrario, cuando el conmutador de región ejecute la evaluación automática del plan después de crear el plan, aparecerá una advertencia para informarle de que se necesita más información.

El conmutador de región envía comprobaciones de estado para cada bloque de ejecución de las comprobaciones de estado de Route 53. En el caso de los planes que utilizan un enfoque de active/passive recuperación, la comprobación de estado de la región principal comienza como correcta y la comprobación de estado de la región en espera se establece inicialmente como insalubre. En el caso de los planes que utilizan el enfoque de active/active recuperación, los controles de salud de todas las regiones comienzan en estado saludable.

Para permitir que Region Switch ejecute correctamente este bloque de ejecución para su plan, debe añadir las comprobaciones de estado a sus registros de DNS.

En el caso de un active/active plan, el paso de ejecución funciona de la siguiente manera:

- Cuando se ejecuta un flujo de trabajo desactivado en una región, la comprobación de estado se establece en mal estado y el tráfico deja de dirigirse a esa región.
- Cuando se ejecuta un flujo de trabajo activado para una región, la comprobación de estado se establece en buen estado y el tráfico se dirige a esa región.

En el caso de un active/passive plan, el paso de ejecución funciona de la siguiente manera:

- Cuando se ejecuta un flujo de trabajo de activación para una región, la comprobación de estado de esa región se establece en buen estado y el tráfico se dirige a esa región. Al mismo tiempo, el control de estado de la otra región del plan se establece en mal estado y el tráfico deja de dirigirse a esa región.

¿Qué se evalúa como parte de la evaluación del plan

Cuando Region Switch evalúa su plan, Region Switch realiza varias comprobaciones de la configuración y los permisos del bloque de ejecución de Lambda. El conmutador de región

verifica que las comprobaciones de estado estén adjuntas a los registros DNS especificados en la configuración del bloque de ejecución. Es decir, el conmutador de región verifica que los registros DNS de una región específica Región de AWS estén configurados para utilizar las comprobaciones de estado de esa región.

Crea planes para niños

Para respaldar escenarios de recuperación más complejos, puede crear planes para hijos agregándolos con bloques de ejecución de planes de cambio de región. La jerarquía está limitada a dos niveles, pero un plan principal puede incluir varios planes secundarios.

Por motivos de compatibilidad, los planes para niños deben ser compatibles con todas las regiones admitidas por el plan para padres. Además, el enfoque de recuperación, active/active o activo/pasivo, debe ser el mismo para los planes para padres e hijos.

Tenga en cuenta las siguientes maneras en las que un plan para hijos responde a los cambios que usted realice en un plan para padres y a los escenarios del plan para padres.

- Un bloque de ejecución principal se marca como completado cuando se han completado todos los planes secundarios y demás bloques de ejecución incluidos en él.
- Si algún paso falla en algún plan secundario, el bloque de ejecución del plan de cambio de región fallará en el plan principal.
- Las acciones de control que se inician en el plan principal durante el cambio de región, como una pausa, un cambio gradual o incorrecto, o una cancelación, se implementan automáticamente en el plan secundario, independientemente del paso actual del plan secundario.
- Las operaciones de Skip tienen un comportamiento especial: se omite el plan principal, pero el plan secundario seguirá ejecutándose.
- Si un plan secundario ya se está ejecutando en un bloque de cambios de región, para determinar si sigue ejecutándose, el cambio de región evalúa la compatibilidad del plan secundario con el plan principal. Si la configuración del plan secundario coincide con los requisitos del plan principal, Region Switch trata el plan secundario como si lo hubiera iniciado el plan principal.
- El paso del plan principal fallará si el plan secundario se ejecuta con parámetros de configuración incompatibles, como los siguientes:
  - El plan secundario funciona en una región diferente
  - El plan secundario ejecuta una operación de desactivación cuando el cambio de región espera que ejecute una operación de activación

- Si el plan secundario se completa correctamente durante un período en el que el plan principal está en pausa, el plan principal tendrá éxito cuando se reanude el plan principal.

Cree un activador para un plan de cambio de región

Si quieres automatizar la recuperación de tu aplicación en el cambio de región, puedes crear uno o más activadores para tu plan de cambio de región. Los activadores comienzan a ejecutar automáticamente un plan de cambio de región, en función de las condiciones de CloudWatch alarma que elijas.

Para crear un disparador para un plan de cambio de región

1. Tras crear un plan, en la página de detalles del plan, selecciona la pestaña Activadores.
2. Selecciona Administrar los desencadenantes.
3. Seleccione los flujos de trabajo para los que desee automatizar la ejecución y, a continuación, elija Agregar activador.
4. Proporcione una descripción del desencadenador.
5. Seleccione una CloudWatch alarma y, a continuación, seleccione hasta 10 CloudWatch alarmas para crear las condiciones del disparador.

   Si selecciona más de una condición, se deben cumplir todas las condiciones antes de que comience la ejecución automática del plan.

Ejecute un plan de cambio de región para recuperar una aplicación

Para recuperar una aplicación cuando una Región de AWS está dañada, ejecute un plan de cambio de región en Amazon Application Recovery Controller (ARC).

- Si su aplicación se despliega siguiendo un active/active enfoque, los flujos de trabajo de su plan desactivan la región afectada para que la otra región activa se escale adecuadamente y comience a recibir todo el tráfico de su aplicación.
- Si su aplicación se implementa con un active/passive enfoque, los flujos de trabajo de su plan desactivan la región afectada y activan la región en espera, aumentando sus recursos allí, si es necesario, y redirigiendo el tráfico de la aplicación a la región en espera.

Para realizar la recuperación de la aplicación de forma manual, ejecute su plan de cambio de región de la siguiente manera.

Otra opción es activar una ejecución automáticamente con CloudWatch las alarmas de Amazon específicas que especifiques para iniciar la ejecución de un plan. Puede especificar los desencadenantes de la ejecución del plan al crear o actualizar un plan. Para obtener más información, consulte Cree un activador para un plan de cambio de región.

Para ejecutar un plan de cambio de región

1. En el AWS Management Console, navegue hasta el Región de AWS que desee activar para su aplicación.
2. En la consola Amazon Application Recovery Controller (ARC), elija el conmutador de región y, a continuación, seleccione el plan que desee ejecutar.
3. Elija Ejecutar plan.
4. Si su plan incluye pasos de aprobación manual, apruebe cada paso cuando se le solicite.

Mientras se ejecuta un plan, puede realizar un seguimiento de su progreso en la página de detalles de la ejecución, que se abre cuando decide ejecutar un plan.

También puede ver información sobre la recuperación de aplicaciones en curso en los paneles de control del conmutador de región. En la consola de cambio de región, en el panel de navegación izquierdo, en el botón de cambio de región, selecciona una de las siguientes opciones:

- Panel global
- Ejecuciones en el nombre de la región

Ten en cuenta que, si hay deficiencias en una región, es posible que el panel global no muestre todos los datos de tu plan. Por este motivo, te recomendamos que utilices únicamente el panel de ejecuciones regionales durante los eventos operativos. El panel de ejecuciones regionales es más resistente porque utiliza el plano de datos del conmutador regional local.

Cuando se complete la ejecución del plan, podrá ver la información sobre la ejecución del plan y otros planes que haya ejecutado el cambio de región en la página de detalles del plan, en la pestaña Historial de ejecución del plan.

Paneles de control para cambiar de región

El cambio de región incluye un panel global que puede usar para observar el estado de los planes de cambio de región en su organización y en las regiones. El cambio de región también tiene un panel de ejecuciones regionales que muestra solo las ejecuciones de planes en la región en la que estás conectado actualmente AWS Management Console.

Ten en cuenta que, si hay deficiencias en una región, es posible que el panel global no muestre todos los datos de tu plan. Por este motivo, te recomendamos que utilices únicamente el panel de ejecuciones regionales durante los eventos operativos. El panel de ejecuciones regionales es más resistente porque utiliza el plano de datos del conmutador regional local.

Para abrir el panel global de cambio de región

1. Abra la consola ARC enhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. En el conmutador de región, selecciona Panel de control global.

Para abrir el panel de control regional, cambia de región

1. Abra la consola ARC enhttps://console.aws.amazon.com/route53recovery/home#/dashboard.
2. En el conmutador de región, seleccione Panel de control regional.

Soporte multicuenta en el cambio de región

En el cambio de región, puedes añadir recursos de otras cuentas a tus planes. También puedes compartir un plan de cambio de región con otras cuentas. Para obtener más información, consulte las siguientes secciones.

Recursos entre cuentas

El cambio de región permite alojar los recursos en una cuenta independiente de la cuenta que contiene el plan de cambio de región. Cuando el cambio de región ejecuta un plan, asume el rol de ejecutivo. Si el plan utiliza recursos de una cuenta diferente a la cuenta que aloja el plan, el conmutador de región utiliza el ExecutionRole para asumir el crossAccountRole acceso a esos recursos.

Cada recurso del plan de cambio de región tiene dos campos opcionales: crossAccountRole un ID externo.

- crossAccountRole: Esta función permite el acceso a los recursos de una cuenta diferente de la cuenta que aloja el plan de cambio de región. El rol solo necesita permisos para actuar sobre los recursos de su cuenta; no necesita permisos para actuar sobre los recursos de la cuenta que aloja el plan de cambio de región.
- ExternalId: Este es el ID externo de STS de la política de confianza de la cuenta que contiene el recurso que requiere una acción. Se trata de una cadena alfanumérica que es el secreto compartido entre las dos cuentas.

Compartir planes de cambio de región

Region Switch se integra con AWS Resource Access Manager (AWS RAM) para que puedas compartir planes entre todos Cuentas de AWS. Cuando compartes un plan, las cuentas que especifiques pueden ver los detalles del plan, ejecutarlo y ver las ejecuciones del plan, lo que proporciona más control y flexibilidad a las capacidades de recuperación de los distintos equipos.

Para empezar a compartir recursos entre cuentas en Region Switch, debe crear un recurso compartido en AWS RAM. El recurso compartido especifica los participantes que están autorizados a compartir el plan que pertenece a tu cuenta. Los participantes pueden ver y ejecutar el plan compartido a través de la consola, la CLI o AWS SDKs.

Importante: Cuenta de AWS Debes ser el propietario de los planes que quieres compartir. No puede compartir un plan que se haya compartido con usted. Para compartir un plan con tu organización o con una unidad organizativa AWS Organizations, debes habilitar la opción de compartir con Organizations.

Para obtener más información al respecto AWS RAM, consulte Support comparte planes entre cuentas para el cambio de región ARC.

Support comparte planes entre cuentas para el cambio de región ARC

Amazon Application Recovery Controller (ARC) se integra AWS Resource Access Manager para permitir el uso compartido de recursos. AWS RAM es un servicio que le permite compartir recursos con otros Cuentas de AWS o a través de ellos AWS Organizations. Para el cambio de región ARC, puede compartir el plan de cambio de región. (Para usar los recursos de otra cuenta de su plan, utiliza un rol de cuenta cruzada. Para obtener más información, consulteRecursos entre cuentas.)

Con AWS RAM, compartes los recursos que te pertenecen mediante la creación de un recurso compartido. Un uso compartido de recursos especifica los recursos que compartir y los consumidores con quienes compartirlos. Los participantes pueden incluir:

- Cuentas de AWS Específico dentro o fuera de la organización del propietario en AWS Organizations
- Una unidad organizativa dentro de su organización en AWS Organizations
- Toda su organización en AWS Organizations

Para obtener más información al respecto AWS RAM, consulte la Guía AWS RAM del usuario.

Si se utiliza AWS Resource Access Manager para compartir planes entre cuentas de ARC, puede utilizar un plan con varios planes diferentes Cuentas de AWS. Si opta por compartir un plan, otro plan Cuentas de AWS que especifique puede ejecutar el plan para recuperar la aplicación.

AWS RAM es un servicio que ayuda a AWS los clientes a compartir recursos de forma segura entre sí Cuentas de AWS. Con AWS RAMél, puede compartir recursos dentro de una organización o unidades organizativas (OUs) mediante funciones y usuarios de IAM. AWS Organizations AWS RAM es una forma centralizada y controlada de compartir un plan.

Al compartir un plan, puede reducir la cantidad total de planes que necesita su organización. Con un plan compartido, puede asignar el costo total de la ejecución del plan a diferentes equipos para maximizar los beneficios del ARC con un costo menor. Compartir los planes entre cuentas también puede facilitar el proceso de incorporación de varias aplicaciones a ARC, especialmente si tiene una gran cantidad de aplicaciones distribuidas en varias cuentas y equipos de operaciones.

Para empezar a compartir recursos entre cuentas en ARC, debe crear un recurso compartido en n. AWS RAM El recurso compartido especifica los participantes que están autorizados a compartir el plan que pertenece a su cuenta.

En este tema se explica cómo compartir los recursos que le pertenecen y cómo utilizar los recursos que se comparten con usted.

Contenido

- Requisitos previos para compartir planes
- Compartir un plan
- Dejar de compartir un plan compartido
- Identificar un plan compartido
- Responsabilidades y permisos de los planes compartidos
- Costos de facturación
- Cuotas

Requisitos previos para compartir planes

- Para compartir un plan, debes tenerlo incluido en tu Cuenta de AWS. Esto significa que el recurso debe asignarse o suministrarse en su cuenta. No puede compartir un plan que se haya compartido con usted.
- Para compartir un plan con tu organización o unidad organizativa AWS Organizations, debes habilitar la opción de compartir con AWS Organizations. Para obtener más información, consulte Habilitar el uso compartido con AWS Organizations en la Guía del usuario de AWS RAM .

Compartir un plan

Cuando compartes un plan, los participantes que especifiques para compartir el plan pueden verlo y, si concedes permisos adicionales, ejecutarlo.

Para compartir un plan, debe agregarlo a un recurso compartido. Un uso compartido de recursos es un recurso de AWS RAM que le permite compartir los recursos a través de Cuentas de AWS. Un uso compartido de recursos especifica los recursos que compartir y los participantes con los que compartirlos. Para compartir un plan, puede crear un nuevo recurso compartido o añadir el recurso a un recurso compartido existente. Para crear un nuevo recurso compartido, puede utilizar la AWS RAM consola o utilizar las operaciones de la AWS RAM API con la tecla AWS Command Line Interface o AWS SDKs.

Si formas parte de una organización AWS Organizations y está activado el uso compartido dentro de tu organización, los participantes de tu organización tienen acceso automático al plan compartido. De lo contrario, los participantes reciben una invitación para unirse al recurso compartido y se les concede acceso al plan compartido tras aceptar la invitación.

Puedes compartir un plan de tu propiedad mediante la AWS RAM consola o mediante las operaciones de la AWS RAM API con AWS CLI o SDKs.

Para compartir un plan de tu propiedad mediante la AWS RAM consola

Consulte Creación de un uso compartido de recursos en la Guía del usuario de AWS RAM .

Para compartir un plan de tu propiedad mediante el AWS CLI

Utilice el comando create-resource-share.

Otorgar permisos para compartir planes

Para compartir planes entre cuentas, se requieren los siguientes permisos adicionales para el director de IAM que comparte el plan mediante 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"
```

El propietario que comparte el plan debe tener los siguientes permisos. Si intentas compartir un plan AWS RAM sin tener estos permisos, aparecerá un error.

```
"arc-region-switch:PutResourcePolicy" # Permission only apis
"arc-region-switch:DeleteResourcePolicy" # Permission only apis
"arc-region-switch:GetResourcePolicy" # Permission only apis
```

Para obtener más información sobre la forma en que se AWS Resource Access Manager usa IAM, consulte Cómo se AWS Resource Access Manager usa IAM en la Guía del AWS RAM usuario.

Dejar de compartir un plan compartido

Al dejar de compartir un plan, se aplica lo siguiente a los participantes y propietarios:

- Los participantes ya no pueden ver ni ejecutar el plan no compartido.

Para dejar de compartir un plan compartido de tu propiedad, elimínalo del recurso compartido. Para ello, puede utilizar la AWS RAM consola o utilizar las operaciones de la AWS RAM API con la tecla AWS CLI o SDKs.

Para dejar de compartir un plan compartido de tu propiedad mediante la consola AWS RAM

Consulte Actualización de un recurso compartido en la Guía del usuario de AWS RAM .

Para dejar de compartir un plan compartido del que eres propietario mediante el AWS CLI

Utilice el comando disassociate-resource-share.

Identificar un plan compartido

Los propietarios y los participantes pueden identificar los planes compartidos consultando la información en AWS RAM. También pueden obtener información sobre los recursos compartidos mediante la consola ARC y AWS CLI.

En general, para obtener más información sobre los recursos que ha compartido o que se han compartido con usted, consulte la información en la Guía del AWS Resource Access Manager usuario:

- Como propietario, puede ver todos los recursos que comparte con otros usuarios mediante AWS RAM. Para obtener más información, consulte Visualización de los recursos compartidos en AWS RAM.
- Como participante, puede ver todos los recursos que se han compartido con usted utilizando AWS RAM. Para obtener más información, consulte Visualización de los recursos compartidos en AWS RAM.

Como propietario, puede determinar si está compartiendo un plan consultando la información de las operaciones de la API ARC AWS Management Console o utilizándolas AWS Command Line Interface con ellas.

Para identificar si un plan de tu propiedad es compartido mediante la consola

En la AWS Management Console página de detalles de un plan, consulta el estado del plan compartido.

Como participante, cuando se comparte un plan contigo, normalmente debes aceptar la participación para poder acceder al plan.

Responsabilidades y permisos de los planes compartidos

Permisos de los propietarios

Los participantes pueden ver o ejecutar el plan (si tienen los permisos correctos).

Permisos para los participantes

Cuando compartes un plan de tu propiedad con otros Cuentas de AWS, los participantes pueden verlo o ejecutarlo (si tienen los permisos correctos).

Cuando compartes un plan mediante el uso AWS RAM, el participante tiene, de forma predeterminada, permisos de solo lectura. Para ver una lista de permisos de solo lectura para el cambio de región, consulte. Permisos de solo lectura Los participantes necesitan permisos adicionales para ejecutar un plan de cambio de región. Los participantes que necesitan ejecutar planes necesitan permisos adicionales. Tenga en cuenta que no puede conceder permiso a un AWS RAM participante para las siguientes operaciones:

- `ApprovePlanExecutionStep`
- `UpdatePlan`

Costos de facturación

En ARC, al propietario de un plan se le facturan los costos asociados al plan. La creación de recursos alojados en un plan no supone ningún coste adicional, ni para los propietarios ni para los participantes.

Para obtener información detallada sobre precios y ejemplos, consulte los precios de Amazon Application Recovery Controller (ARC) y desplácese hacia abajo hasta Amazon Application Recovery Controller (ARC).

Cuotas

Todos los recursos creados en un plan compartido se incluyen en las cuotas del propietario del plan.

Para obtener una lista de las cuotas de los planes de cambio de región, consulteLas cuotas para el cambio de región.

Identity and Access Management for Region Switch en ARC

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a los AWS recursos. Los administradores de IAM controlan quién puede autenticarse (iniciar sesión) y quién puede autorizarse (tener permisos) para usar los recursos de ARC. La IAM es una Servicio de AWS opción que puede utilizar sin coste adicional.

Contenido

- Cómo funciona el cambio de región en ARC con IAM
- Ejemplos de políticas basadas en la identidad para el cambio de región en ARC

Cómo funciona el cambio de región en ARC con IAM

Antes de usar IAM para administrar el acceso a ARC, infórmese sobre las funciones de IAM disponibles para su uso con ARC.

Antes de usar IAM para administrar el acceso al conmutador de región en Amazon Application Recovery Controller (ARC), infórmese sobre las funciones de IAM disponibles para su uso con el conmutador de región.

Funciones de IAM que puede utilizar con el cambio de región en Amazon Application Recovery Controller (ARC)

Característica de IAM	Soporte para conmutadores de región
Políticas basadas en identidades	Sí
Políticas basadas en recursos	Sí
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política	Sí
ACLs	Sí
ABAC (etiquetas en políticas)	Sí
Credenciales temporales	Sí
Permisos de entidades principales	Sí
Roles de servicio	No
Roles vinculados al servicio	No

Para obtener una visión general y de alto nivel del funcionamiento de AWS los servicios con la mayoría de las funciones de IAM, consulte AWS los servicios que funcionan con IAM en la Guía del usuario de IAM.

Políticas basadas en la identidad para el cambio de región

Compatibilidad con las políticas basadas en identidad: sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está asociada. Para obtener más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de las políticas de JSON de IAM en la Guía del usuario de IAM.

Para ver ejemplos de políticas ARC basadas en la identidad, consulte. Ejemplos de políticas basadas en identidad en Amazon Application Recovery Controller (ARC)

Políticas basadas en recursos dentro de Region Switch

Compatibilidad con las políticas basadas en recursos: sí

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico.

Acciones políticas para el cambio de región

Compatibilidad con las acciones de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Las acciones políticas suelen tener el mismo nombre que la operación de AWS API asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Las acciones políticas en ARC for Region Switch utilizan los siguientes prefijos antes de la acción:

```
arc-region-switch
```

Para especificar varias acciones en una única instrucción, sepárelas con comas. Por ejemplo, los siguientes:

```
"Action": [
      "arc-region-switch:action1",
      "arc-region-switch:action2"
         ]
```

Puede utilizar caracteres comodín (*) para especificar varias acciones . Por ejemplo, para especificar todas las acciones que comiencen con la palabra `Describe`, incluya la siguiente acción:

```
"Action": "arc-region-switch:Describe*"
```

Para ver ejemplos de políticas ARC basadas en la identidad para el cambio de región, consulte. Ejemplos de políticas basadas en la identidad para el cambio de región en ARC

Recursos de políticas para el cambio de región

Compatibilidad con los recursos de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puedes realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puedes hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utiliza un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

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

Para ver ejemplos de políticas ARC basadas en la identidad para el cambio de región, consulte. Ejemplos de políticas basadas en la identidad para el cambio de región en ARC

Claves de condición de política para el cambio de región

Compatibilidad con claves de condición de políticas específicas del servicio: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puedes realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puedes crear expresiones condicionales que utilizan operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación `AND` lógica. Si especifica varios valores para una única clave de condición, AWS evalúa la condición mediante una `OR` operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puedes utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puedes conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para más información, consulta Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

Para ver ejemplos de políticas ARC basadas en la identidad para el cambio de región, consulte. Ejemplos de políticas basadas en la identidad para el cambio de región en ARC

Listas de control de acceso (ACLs) en el conmutador de región

Soporta ACLs: Sí

Las listas de control de acceso (ACLs) controlan qué directores (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLs son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Control de acceso basado en atributos (ABAC) con conmutador de región

Admite ABAC (etiquetas en las políticas): sí

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos. En AWS, estos atributos se denominan etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a muchos AWS recursos. El etiquetado de entidades y recursos es el primer paso de ABAC. A continuación, designa las políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso al que se intenta acceder.

ABAC es útil en entornos que crecen con rapidez y ayuda en situaciones en las que la administración de las políticas resulta engorrosa.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte Definición de permisos con la autorización de ABAC en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

El conmutador de región TODO Recovery (conmutador de región) es compatible con ABAC.

Uso de credenciales temporales con el conmutador de región

Compatibilidad con credenciales temporales: sí

Algunas Servicios de AWS no funcionan cuando inicias sesión con credenciales temporales. Para obtener información adicional, incluidas las que Servicios de AWS funcionan con credenciales temporales, consulta Cómo Servicios de AWS funcionan con IAM en la Guía del usuario de IAM.

Utiliza credenciales temporales si inicia sesión en ellas AWS Management Console mediante cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accedes AWS mediante el enlace de inicio de sesión único (SSO) de tu empresa, ese proceso crea automáticamente credenciales temporales. También crea credenciales temporales de forma

automática cuando inicia sesión en la consola como usuario y luego cambia de rol. Para obtener más información sobre el cambio de roles, consulte Cambio de un usuario a un rol de IAM (consola) en la Guía del usuario de IAM.

Puedes crear credenciales temporales manualmente mediante la AWS CLI API o. AWS A continuación, puede utilizar esas credenciales temporales para acceder AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para obtener más información, consulte Credenciales de seguridad temporales en IAM.

Permisos principales entre servicios para el cambio de región

Admite sesiones de acceso directo (FAS): sí

Cuando utilizas una entidad de IAM (usuario o rol) para realizar acciones en ella AWS, se te considera principal. Las políticas conceden permisos a una entidad principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. En este caso, debe tener permisos para realizar ambas acciones.

Funciones de servicio para el cambio de región

Compatible con roles de servicio: No

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

Funciones vinculadas al servicio para el cambio de región

Compatibilidad con roles vinculados al servicio: no

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puedes ver, pero no editar, los permisos de los roles vinculados a servicios.

Para más información sobre cómo crear o administrar roles vinculados a servicios, consulta Servicios de AWS que funcionan con IAM. Busque un servicio en la tabla que incluya `Yes` en la columna Rol vinculado a un servicio. Seleccione el vínculo Sí para ver la documentación acerca del rol vinculado a servicios para ese servicio.

Ejemplos de políticas basadas en la identidad para el cambio de región en ARC

De forma predeterminada, los usuarios y los roles no tienen permiso para crear o modificar los recursos de ARC. Tampoco pueden realizar tareas mediante la AWS Management Console, AWS Command Line Interface (AWS CLI) o la AWS API. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puedes añadir las políticas de IAM a roles y los usuarios puedes asumirlos.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM (consola) en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos por ARC, incluido el ARNs formato de cada uno de los tipos de recursos, consulte Acciones, recursos y claves de condición de Amazon Application Recovery Controller (ARC) en la Referencia de autorización de servicios.

Temas

- Prácticas recomendadas sobre las políticas
- Planifique la ejecución, la función, la política de
- Permisos de acceso completo
- Permisos de solo lectura
- Permisos de bloqueo de ejecución
- Acceso a recursos entre cuentas
- Política completa de funciones de ejecución del plan

Prácticas recomendadas sobre las políticas

Las políticas basadas en la identidad determinan si alguien puede crear, eliminar o acceder a los recursos de ARC de su cuenta. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están

disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulta las políticas administradas por AWS o las políticas administradas por AWS para funciones de tarea en la Guía de usuario de IAM.

- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulta Políticas y permisos en IAM en la Guía del usuario de IAM.
- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo AWS CloudFormation. Para obtener más información, consulta Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utiliza el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Validación de políticas con el Analizador de acceso de IAM en la Guía del usuario de IAM.
- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para exigir la MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para más información, consulte Acceso seguro a la API con MFA en la Guía del usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Planifique la ejecución, la función, la política de

Esta es la política de confianza necesaria para la función de ejecución del plan:

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

```
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "arc-region-switch.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Permisos de acceso completo

La siguiente política de IAM otorga acceso total a todos los conmutadores APIs de región:

```
{
  "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:CancelPlanExecution",
        "arc-region-switch:ListRoute53HealthChecks",
        "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": "*"
    }
  ]
}
```

Permisos de solo lectura

La siguiente política de IAM concede permisos de acceso de solo lectura para el conmutador de región:

```
{
  "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:ListPlanExecutions",
        "arc-region-switch:ListPlanExecutionEvents",
        "arc-region-switch:ListTagsForResource"
      ],
      "Resource": "*"
    }
  ]
}
```

Permisos de bloqueo de ejecución

En las siguientes secciones, se proporcionan políticas de IAM para bloques de ejecución específicos que se añaden a un plan de cambio de región.

EC2 Bloque de ejecución EC2 de Amazon Auto Scaling

Política para la función de ejecución del plan para administrar los grupos de EC2 Amazon EC2 Auto Scaling:

```
{
  "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": "*",
      "Condition": {
        "StringEquals": {
          "cloudwatch:namespace": "AWS/AutoScaling"
        }
      }
    }
  ]
}
```

Bloque de ejecución de escalado de recursos de Amazon EKS

Política para la función de ejecución del plan para administrar los clústeres de Amazon EKS:

```
{
  "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: Además de esta política de IAM, la función de ejecución del plan debe añadirse a las entradas de acceso del clúster de Amazon EKS con la política de `AmazonArcRegionSwitchScalingPolicy` acceso. Para obtener más información, consulte Configure los permisos de entrada de acceso a EKS.

Bloque de ejecución de escalado del servicio Amazon ECS

Política para la función de ejecución del plan para gestionar los servicios de Amazon ECS:

```
{
  "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": "*",
      "Condition": {
        "StringEquals": {
          "cloudwatch:namespace": "ECS/ContainerInsights"
```

```
        }
      }
    }
  ]
}
```

El enrutamiento ARC controla el bloque de ejecución

Nota: El bloque de ejecución de los controles de enrutamiento de Amazon ARC requiere que cualquier política de control de servicios (SCPs) aplicada a la función de ejecución del plan permita el acceso a las siguientes regiones para estos servicios:

- `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`

Política relativa a la función de ejecución del plan para gestionar los controles de enrutamiento de ARC:

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

Puede recuperar el ID del panel de control de enrutamiento y el ID del clúster mediante CLI. Para obtener más información, consulte Configure los componentes de control de enrutamiento.

Bloque de ejecución de Aurora Global Database

Política para la función de ejecución del plan para administrar las bases de datos globales de Aurora:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "rds:DescribeGlobalClusters",
        "rds:DescribeDBClusters"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "rds:FailoverGlobalCluster",
        "rds:SwitchoverGlobalCluster"
      ],
      "Resource": [
        "arn:aws:rds:us-east-1:123456789012: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"
      ]
    }
  ]
```

```
}
```

Bloque de ejecución y aprobación manual

Política para el rol que puede aprobar los pasos manuales:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "arc-region-switch:ApprovePlanExecutionStep"
      ],
      "Resource": "arn:aws:arc-region-switch::123456789012:plan/sample-plan:0fba5e"
    }
  ]
}
```

Bloque de ejecución de Lambda de acción personalizada

Política para que la función de ejecución del plan invoque funciones Lambda:

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

Bloque de ejecución del chequeo de estado de Route 53

Política para que la función de ejecución del plan utilice las comprobaciones de estado de Route 53:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "route53:ListResourceRecordSets"
      ],
      "Resource": [
        "arn:aws:route53:::hostedzone/Z1234567890ABCDEFGHIJ"
      ]
    }
  ]
}
```

Bloque de ejecución del plan de cambio de región

Política sobre la función de ejecución del plan para ejecutar los planes secundarios:

```
{
  "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-1:50c1a1",
        "arn:aws:arc-region-switch::123456789012:plan/child-plan-2:d1e5e1"
      ]
    }
  ]
}
```

CloudWatch alarmas para el estado de la aplicación

Política para la función de ejecución del plan de acceso a CloudWatch las alarmas relacionadas con el estado de las aplicaciones, que se utilizan para ayudar a determinar el tiempo de recuperación real:

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

Acceso a recursos entre cuentas

Si los recursos están en cuentas diferentes, necesitarás un rol multicuenta. Este es un ejemplo de política de confianza para un rol multicuenta:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:role/RegionSwitchExecutionRole"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "sts:ExternalId": "UniqueExternalId123"
        }
      }
    }
```

```
  ]
}
```

Y el permiso para que la función de ejecución del plan asuma esta función multicuenta:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::987654321098:role/RegionSwitchCrossAccountRole",
      "Condition": {
        "StringEquals": {
          "sts:ExternalId": "UniqueExternalId123"
        }
      }
    }
  ]
}
```

Política completa de funciones de ejecución del plan

Una política integral que incluya permisos para todos los bloques de ejecución sería bastante amplia. En la práctica, solo debes incluir los permisos para los bloques de ejecución que utilices en tu plan específico. A continuación se muestra un ejemplo de política de .

```
{
  "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": "*"
```

```
    },
    // Include additional statements for specific execution blocks here
  ]
}
```

Recuerde incluir solo los permisos necesarios para los bloques de ejecución específicos que utilice en su plan, para seguir el principio de privilegios mínimos.

Registro y supervisión del cambio de región en ARC

Puede usar Amazon y Amazon CloudWatch EventBridge para monitorear el cambio de región en Amazon Application Recovery Controller (ARC), para recibir alertas, analizar patrones y ayudar a solucionar problemas. AWS CloudTrail

Temas

- Registrar las llamadas a la API de cambio de región mediante AWS CloudTrail
- Uso del conmutador de región en ARC con Amazon EventBridge

Registrar las llamadas a la API de cambio de región mediante AWS CloudTrail

El conmutador de región Amazon Application Recovery Controller (ARC) está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, rol o AWS servicio en ARC. CloudTrail captura todas las llamadas a la API de ARC como eventos. Las llamadas capturadas incluyen llamadas desde la consola ARC y llamadas en código a las operaciones de la API ARC.

Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos de ARC. Si no configura una ruta, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos.

Con la información recopilada por CloudTrail, puede determinar la solicitud que se realizó a ARC, la dirección IP desde la que se realizó la solicitud, quién la hizo, cuándo se realizó y detalles adicionales.

Para obtener más información CloudTrail, consulte la Guía AWS CloudTrail del usuario.

Información sobre ARC en CloudTrail

CloudTrail está habilitada en tu cuenta Cuenta de AWS al crear la cuenta. Cuando se produce una actividad en ARC, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS

servicio en el historial de eventos. Puede ver, buscar y descargar eventos recientes en su Cuenta de AWS. Para obtener más información, consulte Trabajar con el historial de CloudTrail eventos.

Para tener un registro continuo de tus eventos Cuenta de AWS, incluidos los eventos de ARC, crea una ruta. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las Regiones de AWS. La ruta registra los eventos de todas las regiones de la AWS partición y envía los archivos de registro al bucket de Amazon S3 que especifique. Además, puede configurar otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para más información, consulte los siguientes temas:

- Introducción a la creación de registros de seguimiento
- CloudTrail servicios e integraciones compatibles
- Configuración de las notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de CloudTrail registro de varias regiones y recibir archivos de CloudTrail registro de varias cuentas

Todas las acciones de ARC se registran CloudTrail y se documentan en el ENLACE DE REFERENCIA DE LA API, por determinar. Por ejemplo, las llamadas a TBD y TBD las acciones generan entradas en los archivos de CloudTrail registro. TBD

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con credenciales de usuario root o AWS Identity and Access Management (IAM).
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro AWS servicio.

Para obtener más información, consulte el elemento userIdentity de CloudTrail .

Visualización de los eventos de cambio de región en el historial de eventos

CloudTrail te permite ver los eventos recientes en el historial de eventos. La mayoría de los eventos relacionados con las solicitudes de API de cambio de región tienen lugar en la región en la que

trabajas con un plan de cambio de región, por ejemplo, cuando creas un plan o ejecutas un plan. Sin embargo, algunas acciones de cambio de región que se ejecutan en la consola ARC se realizan mediante operaciones de API del plan de control, en lugar de operaciones del plano de datos. En el caso de las operaciones del plano de control, se visualizan los eventos en el este de EE. UU. (Virginia del Norte). Para obtener información sobre qué llamadas a la API son operaciones del plano de control, consulte Operaciones de la API de cambio de región.

Descripción de las entradas de los archivos de registro ARC

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

En el siguiente ejemplo, se muestra una entrada de CloudTrail registro que demuestra la `StartPlanExecution` acción del cambio de región.


```
{
    "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"
}
```


Uso del conmutador de región en ARC con Amazon EventBridge

Con Amazon EventBridge, puede configurar reglas basadas en eventos que supervisen los recursos del conmutador de región en Amazon Application Recovery Controller (ARC) y, a continuación, iniciar acciones específicas que utilicen otros AWS servicios. Por ejemplo, puede establecer una regla para el envío de notificaciones por correo electrónico mediante la señalización de un tema de Amazon SNS cada vez que se complete la ejecución de un plan de cambio de región.

Puedes crear reglas en Amazon EventBridge para actuar en los siguientes eventos de cambio de región ARC:

- Ejecución del plan de cambio de región. El evento especifica que se ha ejecutado (ejecutado) un plan de cambio de región.
- Evaluación del plan de cambio de región. El evento especifica que se ha completado la evaluación del plan de cambio de región.

Para capturar eventos de ARC específicos que le interesen, defina patrones específicos de eventos que EventBridge pueda utilizar para detectarlos. Los patrones de eventos de tienen la misma estructura que los eventos con los que coinciden. El patrón cita los campos para los que se desea encontrar coincidencias y proporciona los valores que está buscando.

Los eventos se emiten en la medida de lo posible. En circunstancias operativas normales, se envían desde ARC a prácticamente EventBridge en tiempo real. Sin embargo, pueden surgir situaciones que retrasen o impidan la entrega de un evento.

Para obtener información sobre cómo funcionan EventBridge las reglas con los patrones de eventos, consulte Eventos y patrones de eventos en EventBridge.

Supervise un recurso de cambio de región con EventBridge

Con él EventBridge, puede crear reglas que definan las acciones que se deben tomar cuando ARC emita eventos para los recursos del cambio de región.

Para escribir o copiar y pegar un patrón de eventos en la EventBridge consola, en la consola, seleccione la opción Introducir mi propia opción. Para ayudarle a determinar los patrones de eventos que podrían serle útiles, en este tema se incluyen ejemplos de patrones de cambio de región.

Para crear una regla para un evento de recurso, realice lo siguiente:

1. Abre la EventBridge consola de Amazon en https://console.aws.amazon.com/events/.
2. Región de AWS Para crear la regla, elige la región en la que creaste el plan para el que deseas monitorear los eventos.
3. Seleccione Creación de regla.
4. Ingrese un Name (Nombre) para la regla y opcionalmente, una descripción.
5. Para Bus de eventos, deje el valor predeterminado, predeterminado.
6. Elija Siguiente.
7. En el paso Crear un patrón de eventos, en Origen del evento, deje el valor predeterminado, Eventos de AWS .

8. En Ejemplo de evento, elija Introducir el mío.
9. Para Ejemplos de eventos, escriba o copie y pegue un patrón de eventos. Para ver ejemplos, consulta la siguiente sección.

Ejemplo de patrones de cambio de región

Los patrones de eventos de tienen la misma estructura que los eventos con los que coinciden. El patrón cita los campos para los que se desea encontrar coincidencias y proporciona los valores que está buscando.

Puede copiar y pegar los patrones de eventos de esta sección EventBridge para crear reglas que pueda usar para monitorear las acciones y los recursos de ARC.

Los siguientes patrones de eventos proporcionan ejemplos que puede utilizar EventBridge para la función de cambio de región de ARC.

- Seleccione todos los eventos de la opción Cambiar región por PlanExecution.

```
{
    "source": [ "aws.arc-region-switch" ],
    "detail-type": [ "ARC Region switch Plan Execution" ]
}
```

- Selecciona todos los eventos de la opción Cambiar región por PlanEvaluation.

```
    {
    "source": [ "aws.arc-region-switch" ],
    "detail-type": [ "ARC Region Switch Plan Evaluation" ]
    }
```

El siguiente es un ejemplo de un evento ARC para la ejecución de un plan de cambio de región:

```
{
   "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
   }
}
```

El siguiente es un ejemplo de un evento ARC para la ejecución escalonada de un plan de cambio de región:

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

El siguiente es un ejemplo de un evento ARC para una advertencia de evaluación de un plan de cambio de región.

Para la evaluación de un plan de cambio de región, se emite un evento cuando se devuelve una advertencia. Si la advertencia no se borra, solo se emite un evento para la advertencia una vez cada 24 horas. Cuando se borra el evento, no se emitirán más eventos para esa advertencia.

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

Especifique un grupo de CloudWatch registros para usarlo como destino

Al crear una EventBridge regla, debe especificar el destino al que se envían los eventos que coinciden con la regla. Para obtener una lista de los objetivos disponibles EventBridge, consulte Objetivos disponibles en la EventBridge consola. Uno de los destinos que puedes añadir a una EventBridge regla es un grupo de CloudWatch registros de Amazon. En esta sección se describen los requisitos para añadir grupos de CloudWatch registros como objetivos y se proporciona un procedimiento para añadir un grupo de registros al crear una regla.

Para agregar un grupo de CloudWatch registros como destino, puede realizar una de las siguientes acciones:

- Cree un nuevo grupo de registros
- Elija un grupo de registros existente

Si especifica un nuevo grupo de registros mediante la consola al crear una regla, crea EventBridge automáticamente el grupo de registros. Asegúrese de que el grupo de registros que utilice como destino para la EventBridge regla comience por`/aws/events`. Si desea elegir un grupo de registros existente, tenga en cuenta que solo los grupos de registros que comiencen por `/aws/events` aparecen como opciones en el menú desplegable. Para obtener más información, consulta Crear un nuevo grupo de registros en la Guía del CloudWatch usuario de Amazon.

Si crea o usa un grupo de CloudWatch registros para usarlo como destino mediante CloudWatch operaciones fuera de la consola, asegúrese de configurar los permisos correctamente. Si usa la consola para agregar un grupo de registros a una EventBridge regla, la política basada en recursos del grupo de registros se actualiza automáticamente. Sin embargo, si usa el SDK AWS Command Line Interface o un AWS SDK para especificar un grupo de registros, debe actualizar la política basada en recursos para el grupo de registros. El siguiente ejemplo de política ilustra los permisos que debe definir en una política basada en recursos para el grupo de registros:

```
{
  "Statement": [
    {
      "Action": [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "events.amazonaws.com",
          "delivery.logs.amazonaws.com"
        ]
      },
      "Resource": "arn:aws:logs:region:account:log-group:/aws/events/*:*",
      "Sid": "TrustEventsToStoreLogEvent"
    }
  ],
  "Version": "2012-10-17"
}
```

No puede configurar una política basada en recursos para un grupo de registros mediante la consola. Para añadir los permisos necesarios a una política basada en recursos, utilice la operación de API. CloudWatch PutResourcePolicy A continuación, puede utilizar el comando describe-resource-policiesCLI para comprobar que la política se ha aplicado correctamente.

Para crear una regla para un evento de recurso y especificar un objetivo de grupo de CloudWatch registros

1. Abre la EventBridge consola de Amazon en https://console.aws.amazon.com/events/.
2. Elige en Región de AWS qué quieres crear la regla.
3. Seleccione Crear regla y, a continuación, introduzca cualquier información sobre esa regla, como el patrón de eventos o los detalles de la programación.

   Para obtener más información sobre la creación de EventBridge reglas de preparación, consulte Supervisar un recurso de verificación de preparación con EventBridge.
4. En la página Seleccione el destino, elija CloudWatchcomo objetivo.
5. Elija un grupo de CloudWatch registros en el menú desplegable.

Las cuotas para el cambio de región

El cambio de región en Amazon Application Recovery Controller (ARC) está sujeto a las siguientes cuotas.

Entidad	Cuota
Número de planes por cuenta	10
Número de bloques de ejecución por plan	100
Número de bloques de ejecución del plan de cambio de región por plan	25
Número de CloudWatch alarmas por condición de activación	10

Ejemplos de código para Application Recovery Controller mediante AWS SDKs

Los siguientes ejemplos de código muestran cómo utilizar Application Recovery Controller con un kit de desarrollo de AWS software (SDK).

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulteUso de este servicio con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Ejemplos de código

- Ejemplos básicos del uso de Application Recovery Controller AWS SDKs
  - Acciones para Application Recovery Controller mediante AWS SDKs
    - GetRoutingControlStateUtilízalo con un AWS SDK
    - UpdateRoutingControlStateÚselo con un AWS SDK

Ejemplos básicos del uso de Application Recovery Controller AWS SDKs

Los siguientes ejemplos de código muestran cómo utilizar los aspectos básicos de Amazon Route 53 Application Recovery Controller con AWS SDKs.

Ejemplos

- Acciones para Application Recovery Controller mediante AWS SDKs
  - GetRoutingControlStateUtilízalo con un AWS SDK
  - UpdateRoutingControlStateÚselo con un AWS SDK

Acciones para Application Recovery Controller mediante AWS SDKs

Los siguientes ejemplos de código muestran cómo realizar acciones individuales de Application Recovery Controller con AWS SDKs. Cada ejemplo incluye un enlace a GitHub, donde puede encontrar instrucciones para configurar y ejecutar el código.

Los siguientes ejemplos incluyen solo las acciones que se utilizan con mayor frecuencia. Para ver una lista completa, consulte la Referencia de la API del controlador de recuperación de aplicaciones de Amazon Route 53.

Ejemplos

- GetRoutingControlStateUtilízalo con un AWS SDK
- UpdateRoutingControlStateÚselo con un AWS SDK

`GetRoutingControlState`Utilízalo con un AWS SDK

En los siguientes ejemplos de código, se muestra cómo utilizar `GetRoutingControlState`.

Java

SDK para Java 2.x

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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;
    }
```

- Para obtener más información sobre la API, consulta GetRoutingControlStatela Referencia AWS SDK for Java 2.x de la API.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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
```

- Para obtener más información sobre la API, consulta GetRoutingControlStatela AWS Referencia de API de SDK for Python (Boto3).

Para obtener una lista completa de las guías para desarrolladores del AWS SDK y ejemplos de código, consulte. Uso de este servicio con un AWS SDK En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

`UpdateRoutingControlState`Úselo con un AWS SDK

En los siguientes ejemplos de código, se muestra cómo utilizar `UpdateRoutingControlState`.

Java

SDK para Java 2.x

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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;
    }
```

- Para obtener más información sobre la API, consulta UpdateRoutingControlStatela Referencia AWS SDK for Java 2.x de la API.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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)
```

- Para obtener más información sobre la API, consulta UpdateRoutingControlStatela AWS Referencia de API de SDK for Python (Boto3).

Para obtener una lista completa de las guías para desarrolladores del AWS SDK y ejemplos de código, consulte. Uso de este servicio con un AWS SDK En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Seguridad en Amazon Application Recovery Controller

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de los centros de datos y las arquitecturas de red diseñados para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre AWS usted y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la Nube de AWS. AWS también le proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los AWS programas de de . Para obtener información sobre los programas de conformidad que se aplican a Amazon Application Recovery Controller, consulte AWS Servicios incluidos en el ámbito del programa de conformidad AWS .
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. También eres responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y la normativa aplicables.

Esta documentación le ayuda a entender cómo aplicar el modelo de responsabilidad compartida al utilizar ARC. Los siguientes temas muestran cómo configurar ARC para cumplir sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger sus recursos de ARC.

Temas

- Protección de datos en Amazon Application Recovery Controller
- Identity and Access Management para Amazon Application Recovery Controller (ARC)
- Registro y supervisión en ARC
- Validación de conformidad para Amazon Application Recovery Controller
- Resiliencia en Amazon Application Recovery Controller
- Seguridad de la infraestructura en Amazon Application Recovery Controller

Protección de datos en Amazon Application Recovery Controller

El modelo de se aplica a protección de datos en Amazon Application Recovery Controller. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global en la que se ejecutan todos los Nube de AWS. Eres responsable de mantener el control sobre el contenido alojado en esta infraestructura. También eres responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulta las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulta la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS .

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utiliza la autenticación multifactor (MFA) en cada cuenta.
- Se utiliza SSL/TLS para comunicarse con AWS los recursos. Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con AWS CloudTrail. Para obtener información sobre el uso de CloudTrail senderos para capturar AWS actividades, consulte Cómo trabajar con CloudTrail senderos en la Guía del AWS CloudTrail usuario.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utiliza servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-3 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulta Estándar de procesamiento de la información federal (FIPS) 140-3.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja con ARC u otro tipo de aplicaciones Servicios de AWS mediante la consola, la API o. AWS CLI AWS SDKs Cualquier dato que ingrese

en etiquetas o campos de texto de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya la información de las credenciales en la URL para validar la solicitud para ese servidor.

Cifrado en reposo

La información de configuración del cliente se almacena en tablas globales de Amazon DynamoDB propiedad del servicio y se cifra en reposo.

Los conjuntos de datos que contienen el estado de las celdas de un clúster ARC se escriben en un volumen de Amazon EBS para su copia de seguridad. ARC utiliza el cifrado predeterminado de Amazon EBS mientras los datos están en reposo.

Cifrado en tránsito

Las solicitudes y respuestas de los clientes (relacionadas con la configuración de ARC, las consultas sobre el estado de preparación, las actualizaciones del estado de las celdas, etc.) se cifran mediante TLS durante el transporte por todo el servicio.

Identity and Access Management para Amazon Application Recovery Controller (ARC)

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a los AWS recursos. Los administradores de IAM controlan quién puede autenticarse (iniciar sesión) y quién puede autorizarse (tener permisos) para usar los recursos de ARC. La IAM es una Servicio de AWS opción que puede utilizar sin coste adicional.

Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo que se realice en ARC.

Usuario del servicio: si utiliza el servicio ARC para realizar su trabajo, el administrador le proporcionará las credenciales y los permisos que necesita. A medida que vaya utilizando más funciones de ARC para realizar su trabajo, es posible que necesite permisos adicionales. Entender

cómo se administra el acceso puede ayudarle a solicitar los permisos correctos al administrador. Si no puede acceder a una función de ARC, consulteSolución de problemas de identidad y acceso a Amazon Application Recovery Controller (ARC).

Administrador de servicios: si está a cargo de los recursos de ARC en su empresa, probablemente tenga acceso total a ARC. Su trabajo consiste en determinar a qué funciones y recursos de ARC deben acceder los usuarios del servicio. Luego, debe enviar solicitudes a su gestionador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo su empresa puede utilizar IAM con ARC, consulteCómo funcionan las capacidades de Amazon Application Recovery Controller (ARC) con IAM.

Administrador de IAM: si es administrador de IAM, puede que desee obtener más información sobre cómo redactar políticas para administrar el acceso a ARC. Para ver ejemplos de políticas de ARC basadas en la identidad que puede utilizar en IAM, consulte. Ejemplos de políticas basadas en identidad en Amazon Application Recovery Controller (ARC)

Autenticación con identidades

La autenticación es la forma de iniciar sesión AWS con sus credenciales de identidad. Debe estar autenticado (con quien haya iniciado sesión AWS) como usuario de IAM o asumiendo una función de IAM. Usuario raíz de la cuenta de AWS

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (IAM Identity Center), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, su gestionador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accedes AWS mediante la federación, asumes un rol de forma indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en el portal AWS Management Console o en el de AWS acceso. Para obtener más información sobre cómo iniciar sesión AWS, consulte Cómo iniciar sesión Cuenta de AWS en su Guía del AWS Sign-In usuario.

Si accede AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus credenciales. Si no utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener más información sobre la firma de solicitudes, consulte AWS Signature Versión 4 para solicitudes API en la Guía del usuario de IAM.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, le AWS recomienda que utilice la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Autenticación multifactor en la Guía del usuario de AWS IAM Identity Center y Autenticación multifactor AWS en IAM en la Guía del usuario de IAM.

Cuenta de AWS usuario root

Al crear una Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todos Servicios de AWS los recursos de la cuenta. Esta identidad se denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizaste para crear la cuenta. Recomendamos encarecidamente que no utiliza el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulta Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos, incluidos los que requieren acceso de administrador, que utilicen la federación con un proveedor de identidades para acceder Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio de usuarios de su empresa, un proveedor de identidades web AWS Directory Service, el directorio del Centro de Identidad o cualquier usuario al que acceda Servicios de AWS mediante las credenciales proporcionadas a través de una fuente de identidad. Cuando las identidades federadas acceden Cuentas de AWS, asumen funciones y las funciones proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utiliza AWS IAM Identity Center. Puede crear usuarios y grupos en el Centro de identidades de IAM, o puede conectarse y sincronizarse con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus Cuentas de AWS aplicaciones. Para obtener más información, consulta ¿Qué es el Centro de identidades de IAM? en la Guía del usuario de AWS IAM Identity Center .

Usuarios y grupos de IAM

Un usuario de IAM es una identidad propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como

contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para más información, consulte Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración en la Guía del usuario de IAM.

Un grupo de IAM es una identidad que especifica un conjunto de usuarios de IAM. No puedes iniciar sesión como grupo. Puedes usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos para grandes conjuntos de usuarios. Por ejemplo, puede asignar un nombre a un grupo IAMAdminsy concederle permisos para administrar los recursos de IAM.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales de larga duración permanentes; no obstante, los roles proporcionan credenciales temporales. Para obtener más información, consulte Casos de uso para usuarios de IAM en la Guía del usuario de IAM.

Roles de IAM

Un rol de IAM es una identidad dentro de usted Cuenta de AWS que tiene permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una persona determinada. Para asumir temporalmente un rol de IAM en el AWS Management Console, puede cambiar de un rol de usuario a uno de IAM (consola). Puedes asumir un rol llamando a una operación de AWS API AWS CLI o usando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulta Métodos para asumir un rol en la Guía del usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuario federado: para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información acerca de roles de federación, consulte Crear un rol para un proveedor de identidad de terceros (federación) en la Guía de usuario de IAM. Si utiliza el IAM Identity Center, debe configurar un conjunto de permisos. IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué pueden acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulta Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center .
- Permisos de usuario de IAM temporales: un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.

- Acceso entre cuentas: puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunas Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para obtener información acerca de la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulta Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.
- Acceso entre servicios: algunos Servicios de AWS utilizan funciones en otros Servicios de AWS. Por ejemplo, cuando realizas una llamada en un servicio, es habitual que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.
  - Sesiones de acceso directo (FAS): cuando utilizas un usuario o un rol de IAM para realizar acciones en AWS ellas, se te considera principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. El FAS utiliza los permisos del principal que llama Servicio de AWS y los solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.
  - Rol de servicio: un rol de servicio es un rol de IAM que adopta un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.
  - Función vinculada al servicio: una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.
- Aplicaciones que se ejecutan en Amazon EC2: puedes usar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una EC2 instancia y realizan AWS CLI solicitudes a la AWS API. Esto es preferible a almacenar las claves de acceso en la EC2 instancia. Para asignar un AWS rol a una EC2 instancia y ponerlo a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene

el rol y permite que los programas que se ejecutan en la EC2 instancia obtengan credenciales temporales. Para obtener más información, consulte Usar un rol de IAM para conceder permisos a las aplicaciones que se ejecutan en EC2 instancias de Amazon en la Guía del usuario de IAM.

Administración de acceso mediante políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando un director (usuario, usuario raíz o sesión de rol) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulte Información general de políticas JSON en la Guía del usuario de IAM.

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utiliza para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con esa política puede obtener información sobre el rol de la API AWS Management Console AWS CLI, la o la AWS API.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios,

grupos y roles de su Cuenta de AWS empresa. Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para obtener más información sobre cómo elegir una política administrada o una política insertada, consulte Elegir entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

Listas de control de acceso () ACLs

Las listas de control de acceso (ACLs) controlan qué responsables (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLs son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Amazon S3 y Amazon VPC son ejemplos de servicios compatibles. AWS WAF ACLs Para obtener más información ACLs, consulte la descripción general de la lista de control de acceso (ACL) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite tipos de políticas adicionales y menos comunes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- Límites de permisos: un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM (usuario o rol de IAM). Puedes establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en

el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.

- Políticas de control de servicios (SCPs): SCPs son políticas de JSON que especifican los permisos máximos para una organización o unidad organizativa (OU). AWS Organizations AWS Organizations es un servicio para agrupar y gestionar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilitas todas las funciones de una organización, puedes aplicar políticas de control de servicios (SCPs) a una o a todas tus cuentas. El SCP limita los permisos de las entidades en las cuentas de los miembros, incluidas las de cada una Usuario raíz de la cuenta de AWS. Para obtener más información sobre Organizations SCPs, consulte las políticas de control de servicios en la Guía del AWS Organizations usuario.
- Políticas de control de recursos (RCPs): RCPs son políticas de JSON que puedes usar para establecer los permisos máximos disponibles para los recursos de tus cuentas sin actualizar las políticas de IAM asociadas a cada recurso que poseas. El RCP limita los permisos de los recursos en las cuentas de los miembros y puede afectar a los permisos efectivos de las identidades, incluidos los permisos Usuario raíz de la cuenta de AWS, independientemente de si pertenecen a su organización. Para obtener más información sobre Organizations e RCPs incluir una lista de Servicios de AWS ese apoyo RCPs, consulte Políticas de control de recursos (RCPs) en la Guía del AWS Organizations usuario.
- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo se AWS determina si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del usuario de IAM.

Cómo funcionan las capacidades de Amazon Application Recovery Controller (ARC) con IAM

Para obtener información sobre cómo funciona cada función de Amazon Application Recovery Controller (ARC) con IAM, consulte los siguientes temas:

- IAM para cambio zonal
- IAM para cambio automático zonal
- IAM para el control de enrutamiento
- IAM para comprobar la preparación
- IAM para cambio de región

Ejemplos de políticas basadas en identidad en Amazon Application Recovery Controller (ARC)

Para ver ejemplos de políticas basadas en la identidad para cada capacidad de Amazon Application Recovery Controller (ARC), consulte los siguientes temas en los AWS Identity and Access Management capítulos correspondientes a cada capacidad:

- Ejemplos de políticas basadas en la identidad para el cambio automático zonal en ARC
- Ejemplos de políticas basadas en la identidad para el cambio zonal en ARC
- Ejemplos de políticas basadas en la identidad para el control de enrutamiento en ARC
- Ejemplos de políticas basadas en la identidad para comprobar la preparación en ARC

AWS políticas gestionadas para Amazon Application Recovery Controller (ARC)

Para obtener información sobre las políticas AWS administradas para las capacidades de ARC con políticas administradas, incluida una política administrada para un rol vinculado a un servicio, consulte los siguientes temas:

- Políticas gestionadas para el cambio automático zonal
- Políticas gestionadas para el control de enrutamiento
- Políticas gestionadas para la comprobación de la preparación

Actualizaciones de las políticas AWS gestionadas de Amazon Application Recovery Controller (ARC)

Consulte los detalles sobre las actualizaciones de las políticas AWS administradas para las capacidades de ARC desde que este servicio comenzó a rastrear estos cambios. Para recibir alertas automáticas sobre los cambios en esta página, suscríbase a la fuente RSS de la página del historial de documentos de ARC.

Cambio	Descripción	Fecha
AWSZonalAutoshiftPracticeRunSLRPolicy política gestionada: política actualizada	Agrega la declaración de política `AutoshiftPracticeCheckPermissions` con los permisos y `autoscaling:DescribeAutoScalingGroups` `ec2:DescribeInstances` `elasticloadbalancing:DescribeTargetHealth` , `elasticloadbalancing:DescribeTargetHealth` para respaldar las comprobaciones de capacidad equilibradas. Para obtener más información, consulte Cómo funcionan el cambio automático de zona y las ejecuciones de práctica.	30 de junio de 2025
AWSServiceRoleForPercPracticePolicy— Nueva política	ARC agregó una nueva función vinculada al servicio para el cambio automático y las sesiones de práctica. ARC utiliza los permisos habilitados por la función	30 de noviembre de 2023

Cambio	Descripción	Fecha
	vinculada al servicio para monitorear las alarmas de CloudWatch Amazon proporcionadas por el AWS Health Dashboard cliente y los eventos de los clientes para las ejecuciones de práctica y para iniciar las ejecuciones de práctica. Para obtener más información sobre el nuevo rol vinculado a servicios, consulte Permisos de rol vinculados al servicio para AWSService RoleForZonalAutoshiftPracticeRun.	
AmazonRoute53 — Política actualizada RecoveryControlConfigReadOnlyAccess	Añade permisos para`GetResourcePolicy` , a fin de permitir la devolución de detalles sobre las políticas de AWS Resource Access Manager recursos para los recursos compartidos.	18 de octubre de 2023

Cambio	Descripción	Fecha

Route53RecoveryReadinessServiceRolePolicy: política actualizada	ARC agregó nuevos permisos para consultar información sobre las EC2 instancias de Amazon.
	
	ARC utiliza los siguientes permisos para respaldar el sondeo de EC2 las instancias de Amazon, ejecutar comprobaciones de disponibilidad y determinar el estado de preparación de las instancias.
	
	`ec2:DescribeVpnGateways`
	
	`ec2:DescribeCustomerGateways`
		17 de febrero de 2023

Route53RecoveryReadinessServiceRolePolicy: política actualizada	ARC agregó un nuevo permiso para consultar información sobre las funciones de Lambda. ARC utiliza el siguiente permiso para consultar información sobre las funciones de Lambda a fin de ejecutar comprobaciones de disponibilidad y determinar el estado de preparación de las funciones. `lambda:ListProvisionedConcurrencyConfigs`	31 de agosto de 2022

Cambio	Descripción	Fecha
AmazonRoute53 RecoveryControlConfigFullAccess — Política actualizada	Se eliminaron los permisos de Amazon Route 53 de la política y se agregó una nota en la que se enumeran los permisos opcionales.	26 de mayo de 2022
AmazonRoute53 RecoveryControlConfigFullAccess — Política actualizada	Se agregaron a la política los permisos de Amazon Route 53 que faltaban y que eran obligatorios.	15 de abril de 2022
AmazonRoute53 RecoveryClusterReadOnlyAccess — Política actualizada	ARC agregó un nuevo permiso,`route53-recovery-cluster:ListRoutingControls` , para permitir el control de enrutamiento de listados ARNs con alta disponibilidad.	15 de marzo de 2022
AmazonRoute53 RecoveryControlConfigReadOnlyAccess — Política actualizada	ARC agregó un nuevo permiso`route53-recovery-control-config:ListTagsForResources` ,, para permitir incluir etiquetas en un recurso.	20 de diciembre de 2021

Cambio	Descripción	Fecha
Route53RecoveryReadinessServiceRolePolicy: política actualizada	ARC agregó un nuevo permiso para consultar información sobre Amazon API Gateway. ARC utiliza el permiso,`apigateway:GET` , para consultar información sobre API Gateway a fin de ejecutar comprobaciones de disponibilidad y determinar el estado de preparación.	28 de octubre de 2021
AmazonRoute53 RecoveryReadinessReadOnlyAccess — Se agregaron nuevos permisos	ARC agregó dos nuevos permisos a AmazonRoute53 RecoveryReadinessReadOnlyAccess: ARC utiliza `route53-recovery-readiness:GetArchitectureRecommendations` y `route53-recovery-readiness:GetCellReadinessSummary` permite el acceso de solo lectura a estas acciones para trabajar con la preparación para la recuperación.	15 de octubre de 2021

Cambio	Descripción	Fecha

Route53 RecoveryReadinessServiceRolePolicy: política actualizada	ARC agregó nuevos permisos para consultar informaci ón sobre las funciones de Lambda.
	
	ARC utiliza los siguiente s permisos para consultar información sobre las funciones de Lambda para ejecutar comprobaciones de disponibilidad y determinar el estado de preparación de esas funciones.
	
	`lambda:GetFunction Concurrency`
	
	`lambda:GetFunction Configuration`
	
	`lambda:GetProvisio nedConcurrencyConf ig`
	
	`lambda:ListAliases`
	
	`lambda:ListVersion sByFunction`
	
	`lambda:ListEventSo urceMappings`
	
	`lambda:ListFunctions`
		8 de octubre de 2021

Cambio	Descripción	Fecha
Route53 RecoveryReadinessServiceRolePolicy: se agregaron nuevas políticas administradas	ARC agregó las siguientes políticas administradas nuevas: AmazonRoute53 RecoveryReadinessFullAccess AmazonRoute53 RecoveryReadinessReadOnlyAccess AmazonRoute53 RecoveryClusterFullAccess AmazonRoute53 RecoveryClusterReadOnlyAccess AmazonRoute53 RecoveryControlConfigFullAccess AmazonRoute53 RecoveryControlConfigReadOnlyAccess	18 de agosto de 2021
ARC comenzó a rastrear los cambios	ARC comenzó a realizar un seguimiento de los cambios en sus políticas AWS gestionadas.	27 de julio de 2021

Solución de problemas de identidad y acceso a Amazon Application Recovery Controller (ARC)

Utilice la siguiente información como ayuda para diagnosticar y solucionar problemas comunes que pueden surgir al trabajar con Amazon Application Recovery Controller (ARC) e IAM.

Temas

- No estoy autorizado a realizar ninguna acción en ARC
- No estoy autorizado a realizar lo siguiente: PassRole

- Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de ARC

No estoy autorizado a realizar ninguna acción en ARC

Si AWS Management Console le indica que no está autorizado a realizar una acción, debe ponerse en contacto con su administrador para obtener ayuda. El administrador es la persona que le proporcionó las credenciales.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM `mateojackson` intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio *`my-example-widget`*, pero no tiene los permisos ficticios `route53-recovery-readiness:`*`GetWidget`*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 route53-recovery-readiness:GetWidget on resource: my-example-widget
```

En este caso, Mateo pide a su administrador que actualice sus políticas de forma que pueda obtener acceso al recurso *`my-example-widget`* mediante la acción `route53-recovery-readiness:`*`GetWidget`*.

No estoy autorizado a realizar lo siguiente: PassRole

Si recibes un mensaje de error que indica que no estás autorizado a realizar la `iam:PassRole` acción, debes actualizar tus políticas para que puedas transferir una función a ARC.

Algunas Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada al servicio. Para ello, debe tener permisos para transferir el rol al servicio.

El siguiente ejemplo de error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en ARC. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

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

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su AWS administrador. El gestionador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de ARC

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que respaldan políticas basadas en recursos o listas de control de acceso (ACLs), puede usar esas políticas para permitir que las personas accedan a sus recursos.

Para obtener más información, consulte lo siguiente:

- Para saber si ARC admite estas funciones, consulte. Cómo funcionan las capacidades de Amazon Application Recovery Controller (ARC) con IAM
- Para obtener información sobre cómo proporcionar acceso a los recursos de su Cuentas de AWS propiedad, consulte Proporcionar acceso a un usuario de IAM en otro usuario de su propiedad Cuenta de AWS en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulta Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para conocer sobre la diferencia entre las políticas basadas en roles y en recursos para el acceso entre cuentas, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Registro y supervisión en ARC

La supervisión es una parte importante del mantenimiento de la disponibilidad y el rendimiento de ARC y sus AWS soluciones. Debe recopilar los datos de supervisión de todas las partes de la AWS solución para poder depurar más fácilmente una falla multipunto en caso de que se produzca. AWS proporciona varias herramientas para supervisar los recursos y la actividad de ARC y responder a posibles incidentes, por ejemplo, AWS CloudTrail y Amazon CloudWatch.

Para obtener información sobre la supervisión de cada capacidad de ARC, consulte los siguientes temas:

- Registro y supervisión del cambio zonal
- Registro y supervisión del cambio automático zonal
- Registro y supervisión para el control de enrutamiento
- Registro y supervisión del cambio de región
- Registro y supervisión para comprobar la disponibilidad

Validación de conformidad para Amazon Application Recovery Controller

Los auditores externos evalúan la seguridad y la conformidad de Amazon Application Recovery Controller como parte de varios programas de AWS conformidad. Esto incluye SOC, PCI, HIPAA y otros.

Para saber si un programa de conformidad Servicio de AWS se encuentra dentro del ámbito de aplicación de un programa de conformidad específico, consulte Servicios de AWS Alcance por programa de de conformidad y elija el programa de conformidad que le interese. Para obtener información general, consulte Programas de AWS cumplimiento > Programas AWS .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact .

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- Cumplimiento de seguridad y gobernanza: en estas guías se explican las consideraciones de arquitectura y se proporcionan pasos para implementar las características de seguridad y cumplimiento.
- Referencia de servicios válidos de HIPAA: muestra una lista con los servicios válidos de HIPAA. No todos Servicios de AWS cumplen con los requisitos de la HIPAA.
- AWS Recursos de de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.

- AWS Guías de cumplimiento para clientes: comprenda el modelo de responsabilidad compartida desde el punto de vista del cumplimiento. Las guías resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad del Sector de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).
- Evaluación de los recursos con reglas en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- AWS Security Hub— Esto Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la Referencia de controles de Security Hub.
- Amazon GuardDuty: Servicio de AWS detecta posibles amenazas para sus cargas de trabajo Cuentas de AWS, contenedores y datos mediante la supervisión de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a cumplir con varios requisitos de conformidad, como el PCI DSS, al cumplir con los requisitos de detección de intrusiones exigidos por ciertos marcos de cumplimiento.
- AWS Audit Manager— Esto le Servicio de AWS ayuda a auditar continuamente su AWS uso para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

Resiliencia en Amazon Application Recovery Controller

La infraestructura AWS global se basa en distintas zonas Regiones de AWS de disponibilidad. Regiones de AWS proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de uno o varios centros de datos.

Para obtener más información sobre las zonas de disponibilidad Regiones de AWS y las zonas de disponibilidad, consulte Infraestructura global.AWS

Además de la infraestructura AWS global, ARC ofrece varias funciones para ayudarlo a satisfacer sus necesidades de respaldo y resiliencia de datos.

Seguridad de la infraestructura en Amazon Application Recovery Controller

Como servicio gestionado, está protegido por la seguridad de la red AWS global. Para obtener información sobre los servicios AWS de seguridad y cómo se AWS protege la infraestructura, consulte Seguridad AWS en la nube. Para diseñar su AWS entorno utilizando las mejores prácticas de seguridad de la infraestructura, consulte Protección de infraestructuras en un marco de buena AWS arquitectura basado en el pilar de la seguridad.

Las llamadas a la API AWS publicadas se utilizan para acceder a ARC a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad principal de IAM. También puedes utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Historial de documentos de la Guía para desarrolladores de Amazon Application Recovery Controller (ARC)

En las siguientes entradas se describen los cambios importantes realizados en la documentación de Amazon Application Recovery Controller (ARC).

- Versión: más actualizada
- Última actualización de la documentación: 1 de agosto de 2025

Cambio	Descripción	Fecha
Nuevo servicio de cambio de región	El cambio de región permite a los clientes organizar los pasos específicos, compatibl es con varias cuentas, que son necesarios para operar su aplicación multirregional desde otra. Región de AWS Para obtener más información, consulte Cambio de región en ARC.	1 de agosto de 2025
Mejoras en las carreras de práctica	Ahora puede iniciar sesiones de práctica bajo demanda en ARC. Además, las prácticas ahora incluyen comprobac iones de capacidad suficient e AZs en otros lugares de la Región. Para obtener más información, consulte Cómo funciona.	30 de junio de 2025
Actualiza una política administrada	Actualiza la política `AWSZonalAutoshiftP`	30 de junio de 2025

Cambio	Descripción	Fecha
	racticeRunSLRPolicy gestionada añadiendo la declaración de política AutoshiftPracticeCheckPermissions con los permisos autoscaling:DescribeAutoScalingGroups ec2:DescribeInstances elasticloadbalancing:DescribeTargetHealth , y elasticloadbalancing:DescribeTargetHealth para respaldar las comprobaciones de capacidad equilibradas. Para obtener más información, consulte la política AWSZonal AutoshiftPracticeRun SLRPolicy gestionada.	
Actualizaciones de los tipos de excepciones para el cambio automático zonal	Ahora puede interactuar con el cambio automático zonal en función de cada recurso. Para obtener más información, consulte Cómo funciona.	21 de abril de 2025

Cambio	Descripción	Fecha
Pruebe el cambio automático zonal ARC con AWS FIS	Puede utilizarla AWS FIS para comprobar cómo el cambio automático zonal ARC recupera automáticamente su aplicación durante una interrupción del suministro eléctrico en Arizona Para obtener más informaci ón, consulte Probar el cambio automático zonal con. AWS FIS	26 de marzo de 2025
ARC ahora admite IPv6 puntos finales para los controles de enrutamiento y el cambio zonal.	ARC ahora admite IPv6 puntos finales para los controles de enrutamiento y el cambio zonal. Para obtener más informaci ón, consulte Configurar los componentes de control de enrutamiento.	21 de noviembre de 2024
Capacidad de cambio zonal para grupos de Amazon EC2 Auto Scaling	ARC ahora admite el cambio zonal para los grupos de Amazon EC2 Auto Scaling. Para obtener más información, consulte Support for Amazon EC2 Auto Scaling groups.	18 de noviembre de 2024

Cambio	Descripción	Fecha
Capacidad de cambio zonal para Amazon EKS	Puede iniciar un cambio zonal para un clúster de Amazon EKS o puede AWS permitir que lo haga por usted activando el cambio automático zonal. Este cambio actualiza el flujo de tráfico de east-to-west red de su clúster para que solo se consideren en buen estado los puntos finales de red de los pods que se ejecutan en nodos de trabajo. AZs Para obtener más información, consulte Support for Amazon Elastic Kubernetes Service.	22 de octubre de 2024
Capacidad de cambio zonal para balanceadores de carga de red	ARC ahora admite el cambio zonal para los balanceadores de carga de red con configuraciones activadas o inhabilitadas entre zonas. Para obtener más información, consulte Support for Network Load Balancers.	11 de octubre de 2024

Cambio	Descripción	Fecha
Notificaciones de observadores de Autoshift	Con las notificaciones de observadores de cambios automáticos, puedes configurar el cambio automático zonal para que te notifique, a través de Amazon EventBridge, cada vez que se AWS inicie un cambio automático para alejar el tráfico de una zona de disponibilidad potencialmente afectada. No tiene que configurar ningún recurso específico con el cambio automático zonal para habilitar estas notificaciones independientes. Para obtener más información, consulta Cómo usar el cambio automático zonal con Amazon EventBridge.	12 de julio de 2024

Cambio	Descripción	Fecha
Reorganización de los documentos por cada capacidad	Reorganiza el contenido de la guía para desarrolladores para agruparlo en guías de subdesarrollo. Es decir, ahora hay secciones independientes que contienen información completa sobre cada capacidad de ARC: cambio zonal y cambio automático zonal para la recuperación en zonas de disponibilidad múltiples, y control de enrutamiento y verificación de disponibilidad para la recuperación en varias regiones. Para obtener más información, consulte Qué es Amazon Application Recovery Controller (ARC).	30 de abril de 2024

Cambio	Descripción	Fecha
Añade la capacidad de cambio automático de zona	Añade una nueva función a ARC, en virtud de la cual usted autoriza AWS a transferir el tráfico de recursos de una aplicación desde una zona de disponibilidad, en su nombre, a fin de reducir el tiempo de recuperación durante los eventos. Para obtener más información, consulte Cambio automático zonal en Amazon Application Recovery Controller (ARC).	30 de noviembre de 2023
Añade un nuevo rol vinculado a un servicio	Añade una nueva función vinculada al servicio, para las prácticas de cambio AWSServiceRoleForZonalAutoshiftPracticeRunautomático zonal. Para obtener más información, consulte Permisos de roles vinculados a servicios para AWSServiceRoleForZonalAutoshiftPracticeRun.	30 de noviembre de 2023

Cambio	Descripción	Fecha
Se agrega soporte entre cuentas para los clústeres	Incorpora compatibilidad con varias cuentas para los clústeres de ARC AWS Resource Access Manager, de forma que puede utilizar un clúster de forma fácil y segura para alojar paneles de control y controles de enrutamiento propiedad de varias cuentas diferentes. AWS Para obtener más información, consulte Support cross-account for clusters in ARC.	18 de octubre de 2023
Actualiza una política administrada	Actualiza la política `AmazonRoute53RecoveryControlConfigReadOnly` gestionada para `GetResourcePolicy` añadir permisos y permitir la devolución de detalles sobre las políticas de AWS Resource Access Manager recursos para los recursos compartidos. Para obtener más información, consulte Políticas administradas de AWS.	19 de septiembre de 2023

Cambio	Descripción	Fecha
Actualización del rol vinculado al servicio	Se agregaron nuevos permisos `ec2:DescribeVpnGateways` y `ec2:DescribeCustomerGateways` , a la función vinculada al servicio de ARC, para admitir el sondeo de instancias de Amazon EC2 . Para obtener más información, consulte Uso de roles vinculados a servicios para ARC.	17 de febrero de 2023
Versión de GA para el cambio zonal	Es compatible con la versión general del cambio zonal para ARC, que incluye el control de acceso basado en atributos (ABAC) para los recursos gestionados que están registrados en ARC para el cambio zonal. Para obtener más información, consulte Control de acceso basado en atributos (ABAC) con ARC.	10 de enero de 2023

Cambio	Descripción	Fecha
Se agregó un nuevo cambio zonal Multi-AZ	Se agregó contenido que describe un nuevo servicio en ARC, el cambio zonal, para aplicaciones Multi-AZ. Puede iniciar un cambio zonal para mover temporalmente el tráfico de un recurso de balanceador de carga fuera de una zona de disponibilidad. Para obtener más informaci ón, consulte Cambio zonal en ARC.	28 de noviembre de 2022
Actualización del rol vinculado al servicio	Se agregó un nuevo permiso,`lambda:Li stProvisionedConcu rrencyConfigs` , a la función vinculada al servicio para que ARC consulte información sobre las funciones de Lambda. Para obtener más informaci ón, consulte Uso de roles vinculados a servicios para ARC.	31 de agosto de 2022

Cambio	Descripción	Fecha
Actualización de la política administrada de	Se actualizó la política `AmazonRoute53RecoveryControlConfigFullAccess` administrada para eliminar los permisos de Amazon Route 53 e incluirlos como opcionales. Para obtener más información, consulte las políticas AWS administradas de Amazon Application Recovery Controller (ARC).	26 de mayo de 2022
Actualización de la política administrada de	Se actualizó la política `AmazonRoute53RecoveryControlConfigFullAccess` administrada para incluir los permisos de Amazon Route 53 necesarios. Para obtener más información, consulte las políticas AWS administradas de Amazon Application Recovery Controller (ARC).	15 de abril de 2022

Cambio	Descripción	Fecha
Se agregó un ejemplo de CLI para la nueva API de controles de enrutamiento de listas	Se agregaron ejemplos de comandos CLI y recomendaciones de mejores prácticas para la nueva operación de la API de controles de enrutamiento de listas incluida en la extremadamente confiable API de plano de datos ARC. Para obtener más información, consulte Listar y actualizar los controles y estados de enrutamiento.	31 de marzo de 2022
Se ha agregado compatibilidad con las normas de seguridad	Se ha añadido la compatibilidad con normas de seguridad incompatibles, lo que te permite eludir las medidas de control de rutas que se aplican con las normas de seguridad que has configurado. Es posible que sea necesario anular las normas de seguridad, por ejemplo, en el caso de que se rompa un cristal durante una conmutación por error para la recuperación en caso de desastre. Para obtener más información, consulte Anular las normas de seguridad para redirigir el tráfico.	2 de marzo de 2022

Cambio	Descripción	Fecha
Se agregó soporte de etiquetado adicional	Se agregó soporte para etiquetar recursos adicionales en ARC, incluidos clústeres, paneles de control, controles de enrutamiento y reglas de seguridad. Para obtener más informaci ón, consulte Etiquetado en Amazon Application Recovery Controller (ARC).	20 de diciembre de 2021
Actualización de la política administrada de	Se ha actualizado `AmazonRou te53RecoveryContro lConfigReadOnly` la política de administración para agregar permiso para enumerar las etiquetas de un recurso. Para obtener más informaci ón, consulte las políticas AWS administradas de Amazon Application Recovery Controlle r (ARC)	20 de diciembre de 2021

Cambio	Descripción	Fecha
Se agregó soporte para alertas en tiempo real con EventBridge	Se agregó compatibilidad con EventBridge, lo que significa que ahora puede agregar reglas para recibir alertas y actuar en función de los cambios de estado de preparación para el ARC, por ejemplo, cuando un estado cambia de LISTO a NO LISTO. Para obtener más informaci ón, consulte Uso de ARC con Amazon EventBridge.	20 de diciembre de 2021
Se agregaron ejemplos de códigos de estado de control de enrutamiento	Se agregaron ejemplos de código para ilustrar cómo probar los puntos finales del clúster en secuencia cuando se utilizan las operaciones de la API para obtener o actualiza r los estados del control de enrutamiento. Para obtener más informaci ón, consulte los ejemplos de API para Amazon Application Recovery Controller (ARC).	16 de noviembre de 2021

Cambio	Descripción	Fecha
Ha agregado una política nueva que concede permisos de solo lectura	Ha añadido dos nuevos permisos a la política `AmazonRoute53RecoveryReadinessReadOnlyAccess` : `route53-recovery-readiness:GetArchitectureRecommendations` y `route53-recovery-readiness:GetCellReadinessSummary` . Para obtener más información, consulte las políticas AWS administradas de Amazon Application Recovery Controller (ARC).	9 de noviembre de 2021
Ha añadido compatibilidad con el tipo de recurso Amazon API Gateway	Se agregó un nuevo tipo de recurso, Amazon API Gateway, y se actualizaron los permisos de los roles vinculados al servicio ARC para que ARC pueda auditar API Gateway con comprobaciones de disponibilidad. Para obtener más información, consulte Reglas de preparación y tipos de recursos compatibles y Uso de roles vinculados a servicios para ARC.	28 de octubre de 2021

Cambio	Descripción	Fecha
Se agregó soporte para el tipo de recurso de funciones Lambda	Se agregó un nuevo tipo de recurso, las funciones de Lambda, y se actualizaron los permisos de los roles vinculados al servicio ARC para que ARC pueda auditar las funciones de Lambda con comprobaciones de disponibilidad. Para obtener más información, consulte Reglas de preparación y tipos de recursos compatibles y Uso de roles vinculados a servicios para ARC.	8 de octubre de 2021
Se agregaron enlaces CloudFormation y plantillas de Terraform	Se han añadido enlaces a plantillas Terraform descargables AWS CloudFormation y de Hashicorp para ayudarle a empezar a utilizar Arc rápidamente. Para obtener más información, consulte Preparación para la recuperación con una nueva aplicación.	13 de septiembre de 2021

Cambio	Descripción	Fecha
Nuevas políticas administradas añadidas	Se agregaron las siguientes políticas AWS administradas para ARC:`AmazonRoute53RecoveryReadinessFullAccess` ,,`AmazonRoute53RecoveryReadinessReadOnlyAccess` , `AmazonRoute53RecoveryClusterFullAccess` y. `AmazonRoute53RecoveryClusterReadOnlyAccess` `AmazonRoute53RecoveryControlConfigFullAccess` `AmazonRoute53RecoveryControlConfigReadOnlyAccess` Para obtener más información, consulte las políticas AWS administradas de Amazon Application Recovery Controller (ARC).	18 de agosto de 2021

Cambio	Descripción	Fecha
Comenzó a rastrear las políticas AWS administradas para Amazon Application Recovery Controller (ARC)	Se realizará un seguimiento de las actualizaciones de las políticas administradas a partir de la fecha de lanzamiento inicial. Para obtener más informaci ón, consulte las políticas AWS administradas de Amazon Application Recovery Controlle r (ARC).	27 de julio de 2021
Versión inicial de Amazon Application Recovery Controlle r (ARC)	ARC mejora la disponibi lidad de las aplicaciones mediante la coordinación centralizada de las conmutaci ones por error dentro de una AWS región o entre varias regiones. ARC proporciona comprobaciones de preparaci ón para garantizar que sus aplicaciones estén escaladas para gestionar el tráfico de conmutación por error y estén configuradas para evitar los fallos. También proporciona un control de enrutamiento extremadamente confiable para que pueda recuperar las aplicaciones redirigie ndo el tráfico, por ejemplo, entre zonas o regiones de disponibilidad. Para obtener más información, consulte ¿Qué es ARC? .	27 de julio de 2021

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.